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) d.lgs. N. 50/2016

LOTTO 1

ID SIGEF 2296

SCHEMA DI ACCORDO QUADRO

PER L'AFFIDAMENTO SERVIZI DI SICUREZZA DA REMOTO 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 23/02/2022 (nel seguito per brevità anche "**Consip S.p.A**.")

E

- **Telecom Italia S.p.A.**, sede legale in Milano, Via Gaetano Negri n. 1, capitale sociale Euro 11.677.002.855,10=, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. 00488410010, P. IVA 00488410010, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti:
- **Almaviva – The Italian Innovation Company S.p.A.** con sede legale in Roma, Via di Casal Boccone n.188, capitale sociale Euro 154.899.065,00=, iscritta al Registro delle Imprese di Roma al n. 08450891000, P. IVA 08450891000;
- **KPMG Advisory S.p.A**., con sede legale in Milano, Via Vittor Pisani n. 27, capitale sociale Euro 8.696.950,00=, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. 04662680158, P. IVA 04662680158;
- **Netgroup S.p.A. (già Netgroup S.r.l.)**, con sede legale in Marigliano (NA) Via Pontecitra n. 23, capitale sociale Euro 1.050.000,00=, iscritta al Registro delle Imprese di Napoli al n. 03008301214, P. IVA 03008301214;
- **Reevo S.p.A**., con sede legale in Milano, Via Dante n. 4, capitale sociale Euro 556.479,60=, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. 03888200965, P. IVA 03888200965

giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott. Sandra De Franchis repertorio n. 17737 raccolta n. 8646 del 3 marzo 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 1 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 Lotto 1), 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 Zurich ed avente n. PC8MMS4U per un importo di Euro 68.000,00=(sessantottomila/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*;*

che risulta allo stato pendente il termine per proporre appello avverso la sentenza del TAR Lazio n. 10766/22 pubblicata in data 28 luglio 2022 resa nel giudizio R.G. 3738/22, promosso dall'impresa Leonardo S.p.A. in proprio e nella veste di mandataria del costituendo RTI con IBM Italia S.p.A., Sistemi Informativi S.r.l., Engineering Ingegneria Informatica S.p.A., Aruba PEC S.p.A., Sferanet s.r.l. e SMI Technologies and Consulting S.r.l. nella veste di mandataria contro Consip S.p.A e Accenture S.p.A. anche nella qualità di mandataria del costituendo RTI con Fincantieri Nextech S.p.A., Fastweb S.p.A., DEAS - Difesa e Analisi Sistemi S.p.A. e Telecom Italia S.p.A. anche nella qualità di mandataria del costituendo RTI con Netgroup S.p.A. (già Netgroup S.r.l.), Reevo S.p.A., KPMG Advisory S.p.A., Almaviva The Italian Innovation Company S.p.A. per l'annullamento del provvedimento di aggiudicazione definitiva non efficace comunicato da Consip il 24/02/2022.

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 sicurezza da remoto, in base ai criteri, le modalità ed i termini indicati nel presente Accordo Quadro e nel paragrafo 6.4 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 1), l'Allegato **"G"** (Disposizioni per la Governance), l'Allegato **"H"** (Regolamento degli organismi di coordinamento e controllo)l'Allegato "**I**" (Contratto di Avvalimento Trust), l'Allegato "**L"** (Contratto di Avvalimento Noovle).
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 sicurezza da remoto (Lotto 1 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 187.200.000,00 = (centoottantasettemilioniduecentomila), IVA esclusa (attribuzione della quota massima 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 risultato secondo 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 sicurezza da remoto descritti nel Capitolato Tecnico Speciale Lotto 1 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 Lotto 1) 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 6.4 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.
7. Ai sensi di quanto stabilito all'art. 89, comma 9, del D. Lgs. n. 50/2016, le Amministrazioni contraenti eseguono in corso d'esecuzione del Contratto Esecutivo le verifiche sostanziali circa l'effettivo possesso dei requisiti e delle risorse oggetto dell'avvalimento da parte dell'impresa ausiliaria, nonché l'effettivo impiego delle risorse medesime nell'esecuzione dell'appalto. A tal fine l'Amministrazione contraente accerta in corso d'opera che le prestazioni oggetto del Contratto esecutivo sono svolte direttamente dalle risorse umane e strumentali dell'impresa ausiliaria che il Fornitore utilizza in adempimento degli obblighi derivanti dal contratto di avvalimento.

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 6.4 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 6.4.2. del Capitolato Tecnico Generale, informare Amministrazione e Consip, spiegando le ragioni del rifiuto.
3. All'esito della procedura di cui al paragrafo 6.4 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 e agli allegati "**G**" ed "**H**".
15. Ai sensi dell'art. 47 comma 3, della L. n. 108/2021, il Fornitore è tenuto a consegnare alla **Consip** 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, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta. La suddetta relazione dovrà essere tramessa, altresì, alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.

    La relazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della stessa alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, dovrà essere consegnata alla Consip, **entro 6 mesi dalla stipula** dell'Accordo Quadro.

    La violazione del succitato obbligo determina, ai sensi dell'art. 47, comma 6, della L. n. 108/2021 l'applicazione della penale di cui al successivo articolo "Penali", nonché l'impossibilità di partecipare per un periodo di dodici mesi ad ulteriori procedure di affidamento afferenti gli investimenti pubblici.

16. 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".
17. Le relazioni di cui ai precedenti commi 15 e 16, saranno pubblicate, 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 e ISO 27001) ai fini della partecipazione, entro il termine perentorio di 15 (quindici) giorni lavorativi decorrenti dall'evento modificativo.

    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.
2. 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.

3. Nel caso di esito positivo della verifica di conformità relativamente ai servizi di sicurezza da remoto la data del relativo verbale verrà considerata quale "Data di accettazione".
4. 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.
5. 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.
6. 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.
7. 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.
8. 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. 000000002853, intestato al Fornitore Almaviva – The Italian Innovation Company S.p.A. presso Banca Nazionale del Lavoro, Codice IBAN IT33M0100503205000000002853;
    - n. 046357085991, intestato al Fornitore Almaviva – The Italian Innovation Company S.p.A. presso

Banca Intesa San Paolo, Codice IBAN IT 20 V 03069 05108 046357085991;

- n. 000056762475, intestato al Fornitore Almaviva – The Italian Innovation Company S.p.A. presso Banca Crédit Agricole Cariparma, Codice IBAN IT 09 Z 06230 03202 000056762475;
- n. 000110120174, intestato al Fornitore Almaviva – The Italian Innovation Company S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT 12 I 02008 05364 000110120174;
- n. 000063339087, intestato al Fornitore Almaviva – The Italian Innovation Company S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT 89 T 01030 01630 000063339087;
- n. 000000019233, intestato al Fornitore KPMG Advisory S.p.A. presso Banco BPM S.p.A., Codice IBAN IT59W0503401741000000019233;
- n. 000000016300, intestato al Fornitore KPMG Advisory S.p.A. presso Banco BPM S.p.A., Codice IBAN IT42I0503401741000000016300;
- n. 000000362700, intestato al Fornitore KPMG Advisory S.p.A. presso Banco di Desio e della Brianza, Codice IBAN IT54F0344001603000000362700;
- n. 000000016530, intestato al Fornitore KPMG Advisory S.p.A. presso Banca Nazionale del Lavoro, Codice IBAN IT61E0100501612000000016530;
- n. 000103123277, intestato al Fornitore KPMG Advisory S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT57W0200805364000103123277;
- n. 0000043923521, intestato al Fornitore KPMG Advisory S.p.A. presso Banca Credit Agricole Cariparma, Codice IBAN IT12G0623001630000043923521;
- n. 100000071675, intestato al Fornitore KPMG Advisory S.p.A. presso Banca Intesa San Paolo, Codice IBAN IT87S0306909400100000071675;
- n. 100000005056, intestato al Fornitore Netgroup S.p.A. (già Netgroup S.r.l.) presso Banca Intesa San Paolo, Codice IBAN IT27C0306940023100000005056;
- n. 000102664649, intestato al Fornitore Reevo S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT62N0200820400000102664649;
- n. 000006032857, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT63I0103001600000006032857;
- n. 000006032950, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT50C0103001600000006032950;
- n. 000004630563, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT13O0103002400000004630563;
- n. 000001911184, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT55L0103002000000001911184;
- n. 000009172439, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT37J0103003200000009172439;
- n. 000009172532, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT24D0103003200000009172532;
- n. 000003690065, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT46U0103002800000003690065;
- n. 000006272808, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT68K0103003400000006272808;
- n. 000001468917, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT80Z0103004600000001468917;

- n. 100000124206, intestato al Fornitore Telecom Italia S.p.A. presso Banca Intesa San Paolo, Codice IBAN IT72J0306909209100000124206;
- n. 000003248480, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT14N0103001000000003248480;
- n. 100000001962, intestato al Fornitore Telecom Italia S.p.A. presso Banca Intesa San Paolo, Codice IBAN IT76M0306909612100000001962;
- n. 100000001830, intestato al Fornitore Telecom Italia S.p.A. presso Banca Intesa San Paolo, Codice IBAN IT07B0306909612100000001830;
- n. 100000019995, intestato al Fornitore Telecom Italia S.p.A. presso Banca Intesa San Paolo, Codice IBAN IT79C0306902118100000019995;
- n. 000003050681, intestato al Fornitore Telecom Italia S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT26S0200809440000003050681;
- n. 000007764065, intestato al Fornitore Telecom Italia S.p.A. presso Banca Monte dei Paschi di Siena, Codice IBAN IT83F0103002800000007764065;
- n. 000005256355, intestato al Fornitore Telecom Italia S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT31H0200809440000005256355;
- n. 000005504328, intestato al Fornitore Telecom Italia S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT63Z0200809440000005504328;
- n. 000500009559, intestato al Fornitore Telecom Italia S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT08K0200809440000500009559;
- n. 000004646489, intestato al Fornitore Telecom Italia S.p.A. presso Banca Unicredit S.p.A., Codice IBAN IT53A0200809440000004646489;
- n. 100000019462, intestato al Fornitore Telecom Italia S.p.A. presso Banca Intesa San Paolo, Codice IBAN IT17S0306905020100000019462;
- n. 000000010015, intestato al Fornitore Telecom Italia S.p.A. presso Banca Nazionale del Lavoro, Codice IBAN IT25I0100501600000000010015;
- n. 000014157275, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT95E0760101600000014157275;
- n. 000013187133, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT38N0760101000000013187133;
- n. 000012162293, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT94W0760102400000012162293;
- n. 000012725453, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT47H0760102000000012725453;
- n. 000000381004, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT07E0760103200000000381004;
- n. 000012432548, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT50C0760102800000012432548;
- n. 000015633837, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT90L0760103400000015633837;
- n. 000012820940, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT95F0760104600000012820940;
- n. 000089119630, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN

IT43U0760103200000089119630;

- n. 000009556633, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT41N0760101600000009556633;
- n. 000009556688, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT72E0760101600000009556688;
- n. 000009556606, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT79K0760101600000009556606;
- n. 000009556562, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT42T0760101600000009556562;
- n. 000009556759, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT79A0760101600000009556759;
- n. 000009556704, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT48J0760101600000009556704;
- n. 000086444007, intestato al Fornitore Telecom Italia S.p.A. presso Poste Italiane, Codice IBAN IT15M0760103200000086444007.

Il Fornitore dichiara che i predetti conti operano nel rispetto della Legge 13 agosto 2010 n. 136 e s.m.i.

16. Il Fornitore, nel caso in cui 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 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 Lotto 1 (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 Lotto 1 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 Lotto 1 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 del 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 del 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. Nel caso in cui, come previsto nell'atto di nomina allegato all'Accordo Quadro, all'esito delle verifiche, ispezioni e audit e assessment compiute dall'Amministrazione o da terzi autorizzati, le misure di sicurezza adottate dal 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 del trattamento/Sub Responsabile una penale pari all'**1 per mille** del corrispettivo del singolo Contratto esecutivo per ogni giorno necessario 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.
8. 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.
9. Penali relative a contratti esecutivi PNRR. In caso di mancato adempimento all'obbligazione 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 15, per un importo

complessivo non superiore al 20% del valore dell'Accordo Quadro. Si applica la delibera ANAC n. 122 del 16 marzo 2022 per la parte relativa alle Comunicazioni da inserire casellario informatico.

10. Penali relative a contratti esecutivi PNRR. In caso di mancato adempimento anche ad una sola delle obbligazioni di cui al precedente art. 7, comma 16 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 15, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro. Si applica la delibera ANAC n. 122 del 16 marzo 2022 per la parte relativa alle Comunicazioni da inserire casellario informatico.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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 09/03/2022 dalla Zurich avente n. PC8MMS4U di importo pari ad Euro 68.000,00=(sessantottomila/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 6.4 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 Capitolato Tecnico Speciale Lotto 1, 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 15 e 16;
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. Gaspare Monastero.
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 Lotto 1.
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 Operation Center
- Next Generation Firewall
- Web Application Firewall
- Gestione continua delle vulnerabilità di sicurezza
- Threat Intelligence & Vulnerability Data Feed
- Protezione navigazione Internet e Posta elettronica
- Protezione end point
- Certificati SSL
- Formazione e security awareness
- Gestione dell'identità e l'accesso utente
- Firma digitale remota
- Sigillo elettronico
- Timbro elettronico
- Validazione temporale elettronica qualificata
- Servizi specialistici

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).
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.
6. 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 CONTENZIOSO TAR LAZIO ROMA

Atteso che la stipula del presente contratto avviene in pendenza del termine per proporre appello avverso la sentenza n. 10766/2022 pubblicata in data 28 luglio 2022 con la quale il TAR Lazio Roma definitivamente pronunciandosi sul ricorso iscritto al n di RG 3738/2022 promosso dal RTI Leonardo lo ha respinto dichiarando la piena legittimità dell'aggiudicazione definitiva della procedura disposta dalla Consip S.p.A. in favore del RTI TIM, le parti convengono che qualora all'esito degli eventuali giudizi instaurati a seguito della proposizione dell'appello ovvero di impugnative di qualsiasi natura, dovesse essere imposto il riesame e/o l'annullamento dell'aggiudicazione definitiva e/o della gara e da ciò scaturisse, anche in autotutela, 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 e delle Amministrazioni contraenti, fatto sempre salvo verso queste ultime il diritto al pagamento dei corrispettivi per le prestazioni eseguite a regola d'arte nelle more della pronuncia giurisdizionale resa in qualunque grado di giudizio. 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), Art. 30 (Clausola finale), Articolo 31 (Pendenza contenzioso TAR Lazio Roma**)**.

Roma, lì ___ ___

IL FORNITORE

Roma, 07/10/2021

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

LOTTO 1

RELAZIONE TECNICA

Indice

Indice delle Figure

Indice delle Tabelle

1. PREMESSA

Il Raggruppamento Temporaneo di Impresa (RTI) ritiene di poter offrire alle Pubbliche Amministrazioni (PA) contraenti una soluzione completa e di elevatissimo livello, garantita dalla fornitura di prodotti innovativi best in class, dalla professionalità e competenze delle risorse disponibili e da una consolidata capacità metodologica ed organizzativa delle aziende raggruppande. Le soluzioni proposte rispondono ai requisiti stabiliti dal Capitolato Tecnico di gara, che si intendono tutti rispettati e accettati compreso quanto specificato nelle risposte alle domande di chiarimento.
Il costituendo RTI è composto da **TIM** quale mandataria, **AlmavivA, KPMG, Netgroup** e **ReeVo** quali mandanti.

2. PRESENTAZIONE E DESCRIZIONE OFFERENTE

Di seguito si riportano i dati identificativi dei soggetti muniti dei necessari poteri che sottoscrivono l'offerta.

[redacted]	Riferimenti: [redacted]
	cale: [redacted]
	Documento: [redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Tabella 1 – Dati identificativi dei soggetti muniti di poteri di firma

Di seguito si riportano le descrizioni delle aziende.

TIM – Gruppo leader in Italia e in Brasile nel settore ICT, sviluppa infrastrutture fisse, mobili, cloud e datacenter e offre servizi e prodotti per le comunicazioni e l'intrattenimento, ponendosi all'avanguardia delle tecnologie digitali. Il gruppo si avvale di factory specializzate che offrono soluzioni digitali integrate per cittadini, imprese e PA: **Noovle** è la cloud company di TIM, **Olivetti** è il polo digitale con focus sullo sviluppo di soluzioni IoT, **Telsy** opera nel settore della Cyber Security e **Sparkle** implementa infrastrutture e servizi internazionali. Nello sviluppo del business il gruppo ha fatto propri gli obiettivi di tutela dell'ambiente e di inclusione sociale. In particolare, il progetto Operazione Risorgimento Digitale promuove la diffusione di competenze digitali utili per lo sviluppo del Paese, mentre Fondazione TIM sostiene progetti di alto interesse sociale. Al 31 Dicembre 2020 l'organico complessivo dell'azienda è di 52.333 dipendenti di cui 42.667 in Italia. I principali dati economico-finanziari relativi al 2020 sono: ✓**investimenti industriali** per 3,4 miliardi di euro, ✓**ricavi** per 15,8 miliardi di euro ed ✓**EBITDA** di 6,7 miliardi di euro. TIM vanta una pluriennale esperienza maturata sulla gestione di convenzioni e accordi quadro nella PA: ✓**Reti Locali**; ✓**Videosorveglianza**; ✓**Telefonia Mobile**; ✓**Centrali Telefoniche**; ✓**Contratto Quadro SPC Cloud Lotto 1**.

KPMG – Da oltre 60 anni in Italia, il Network KPMG è ricompreso tra le più importanti piattaforme di servizi professionali attive nel nostro Paese. Il Network è presente in Italia con **4 entità**, **25 uffici** e **4.370 persone**. Tale capillarità territoriale consente di cogliere in maniera immediata le opportunità e le esigenze delle economie del territorio, interpretando nel modo più autentico la struttura portante dell'economia nazionale. La struttura Information Risk Management di KPMG offre una rara combinazione, di competenze tecnologiche e di una profonda conoscenza del mercato, con professionisti che aiutano le aziende a proteggere il business da eventuali attacchi, stando al ritmo e alla velocità con cui operano i cyber criminali.

NETGROUP – Azienda leader nell'innovazione e nella trasformazione digitale in ambito ICT, opera da oltre 25 anni sul mercato italiano della Pubblica Amministrazione e dell'Industria. La competenza sulle tematiche ICT, una vision improntata alla ricerca dell'innovazione, nonché la forte focalizzazione sui temi trasversalmente legati alla security, guidano Netgroup in un processo di aggiornamento continuo del know-how, con particolare riferimento all'ambito Cyber Security, mediante l'acquisizione di competenze e partnership tecnico/commerciali con i più innovativi esponenti del settore, per il continuo potenziamento del portafoglio di servizi e prodotti offerti. I servizi Cyber Security sono oggi erogati per primarie realtà nazionali e internazionali in ambito PA e Industria. I valori guida cui l'azienda si ispira sono: capacità tecnologiche e orientamento all'**innovazione**; metodologie di lavoro **agile**; **flessibilità** organizzativa; sistemi di **qualità** (ISO 9001), di gestione del **servizio** (ISO 20000), di gestione della **sicurezza delle informazioni** (ISO 27001) e di gestione **ambientale** (ISO 14001); **skill e competenze** elevate in ambito security**; infrastrutture organizzative e logistiche** disponibili su tutto il territorio nazionale; **complementarità delle competenze**.

ALMAVIVA – Ha progettato, realizzato e gestito alcuni dei più significativi sistemi per la PA, per Banche e Assicurazioni, Agricoltura, Trasporti e Logistica, Sanità. La professionalità delle risorse AlmavivA è attestata dalle numerose certificazioni di sicurezza vendor independent e sulle principali tecnologie di mercato oltre che sulla conduzione dei progetti (ITIL v4, PMI, IFPUG, Prince2, Cobit5, Togaf). Tutti i servizi sono certificati ISO 9001:2015, ISO 27001:2013, ISO 20000, ISO 22301, ISO 50001 e AQAP 2110/AQAP 160, ISO/IEC 25010:2011, ISO/IEC TS 25011: 2017, UNI ISO/IEC 25012:2014, ISO/IEC 25022:2016, ISO/IEC 25023:2016, UNI CEI ISO/IEC 25024:2016. AlmavivA adotta nuove modalità di ingaggio e valorizzazione delle risorse, che prevedono un rapporto strategico, sistemico e integrato con le migliori Università, i progetti di ricerca più sfidanti, le Academy e gli Hackaton su tutto il territorio nazionale. Il **Centro di Competenza Sicurezza ICT di AlmavivA** è una struttura dedicata e specializzata nell'erogazione di servizi di gestione e servizi professionali specialistici in ambito Sicurezza informatica. Il SOC assicura una continua prevenzione dei rischi e delle minacce che possono pregiudicare la qualità dei servizi erogati ai clienti e garantisce il mantenimento di un elevato livello di Sicurezza con un approccio **security e privacy "by-design" e "by-default"**.

AlmavivA è mandataria del RTI aggiudicatario del **Contratto Quadro per i servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni.** In questo ambito, nel contesto dell'erogazione dei servizi contrattuali, assicura attraverso il proprio SOC la **sicurezza del Centro Servizi, certificato ISO27001,** svolgendo le attività di installazione, setup, delivery e conduzione delle soluzioni di sicurezza per la **protezione di portali web di primaria importanza in ambito nazionale ed internazionale** quali ad esempio: il sito della presidenza italiana del G20 del 2020, il sito Italia Expo Dubai 2020, il portale istituzionale dell'AIFA, il sito dell'Agenzia Nazionale del Turismo Italia.it, il Portale del Nuovo preventivatore IVASS.

REEVO – PMI innovativa fondata nel 2003, è il cloud provider italiano focalizzato sui servizi di Cyber Security e archiviazione che consente alle aziende e alle Amministrazioni di proteggere e custodire il vero patrimonio aziendale rappresentato dai dati. Reevo, oltre a custodire i dati attraverso risorse e piattaforme tecnologiche, analizza le minacce, le vulnerabilità e i rischi dei servizi del cloud e delle reti clienti al fine di proteggerli da attacchi esterni ed interni. Infine, Reevo dispone di Centri di Competenza distribuiti sul territorio nazionale specializzati nella ricerca di soluzioni innovative specializzate sulla Cyber Security.

3. STRUTTURA ORGANIZZATIVA

3.1. MODALITÀ ORGANIZZATIVE *PER LA GESTIONE DELL'ACCORDO QUADRO E DEI CONTRATTI ESECUTIVI*

Il RTI intende adottare un **approccio unitario** *e* **integrato** al governo e all'esecuzione della fornitura, in grado di far corrispondere le potenzialità dei nuovi servizi con le esigenze delle Amministrazioni e di *accompagnare* queste ultime all'utilizzo efficiente dei nuovi servizi. La costituzione del RTI consente alle aziende raggruppande di **sfruttare i rispettivi punti di forza** nell'ambito di un **modello operativo unico**, che prevede funzioni di **governo centrale** della fornitura, per la gestione dell'Accordo Quadro (AQ) e per il supporto a Consip/AgID, e funzioni di governo dei Contratti Esecutivi (CE) stipulati con le singole PA. Nell'ambito del modello organizzativo proposto, particolare rilevanza è assunta dal **Comitato di Governance RTI**, costituito dai responsabili di tutte le aziende raggruppande, cui spetta il ruolo di *uniformare gli approcci e le modalità operative* delle diverse aziende, garantendo l'adozione di un modello operativo comune nell'erogazione dei servizi e assicurando il monitoraggio continuo delle performance dei servizi e del livello di soddisfazione delle PA.

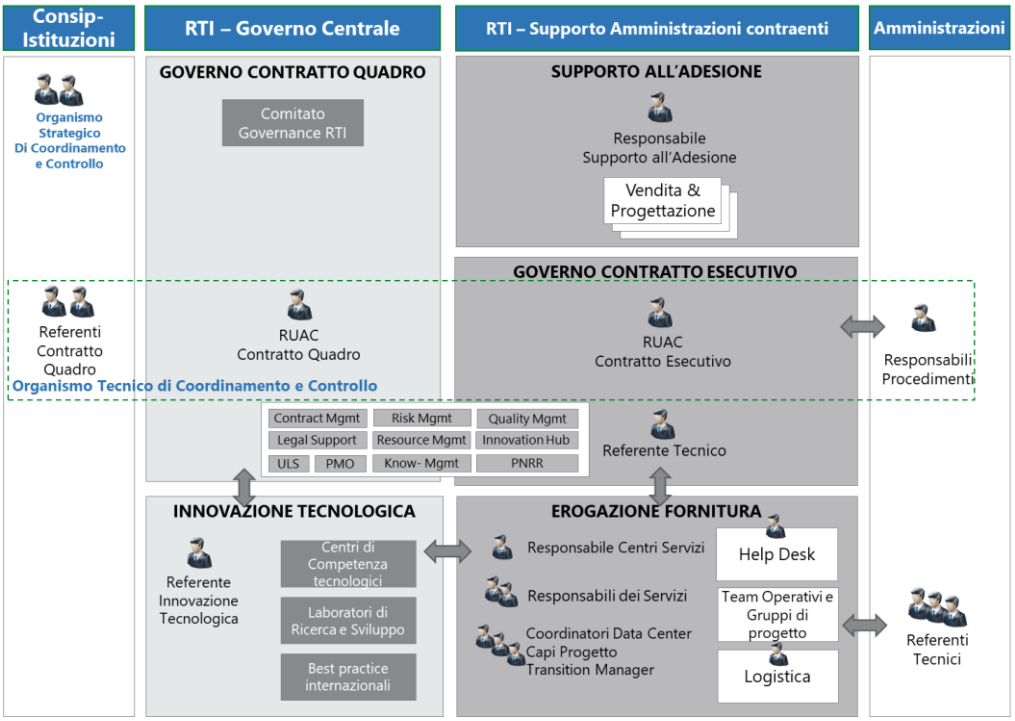

Figura 1 – Figure di riferimento nel modello organizzativo

Governo dei contratti

In conformità con i requisiti di Capitolato, il modello proposto prevede un **Responsabile Unico delle Attività Contrattuali** (**RUAC**), in relazione diretta con Consip/AgID, per le tematiche legate all'AQ, che sarà il Rappresentante del RTI nell'Organismo Tecnico di Coordinamento e Controllo. Nel modello è inoltre presente un **Responsabile Unico delle Attività Contrattuali** per ogni Contratto Esecutivo che gestisce i rapporti con la PA contraente e garantisce supporto all'Organismo Tecnico di Coordinamento e Controllo. I RUAC sono supportati dalle funzioni di staff, descritte di seguito:

Ruolo	Responsabilità
Contract Management	Funzione di supporto per tutti gli aspetti dei contratti e della loro corretta esecuzione. Svolge attività di verifica della copertura contrattuale e delle performance e fornisce supporto anche alle strutture di produzione nell'interpretazione delle clausole contrattuali.
Risk Management	Supporta l'intera organizzazione del RTI in tutti gli aspetti di valutazione del rischio. Effettua periodicamente un'analisi dei rischi sugli aspetti operativi dei servizi forniti e valuta le necessarie azioni di mitigazione.
Quality Management	Produce i Piani di Qualità Generale dell'AQ e Specifici di contratto e li modifica a fronte delle richieste di Consip/AgID/Amministrazioni contraenti. Esegue e coordina le verifiche di qualità secondo i piani approvati. Supporta Consip nelle verifiche ispettive sulla fornitura. Supporta i RUAC nelle analisi dei dati relativi a SLA, rilievi e penali e concorda azioni di mitigazione con le strutture operative.
Regulatory Support	Riferimento per gli aspetti legati alla valutazione e risoluzione di potenziali problemi di carattere legale introdotti dall'adozione dei servizi di sicurezza, tipicamente: leggi internazionali (Unione Europea), regolamenti comunitari, normative e giurisprudenza sulle tematiche dei servizi.
Resource Management	Identifica con le strutture operative delle aziende raggruppande i requisiti della fornitura in termini di risorse e profili professionali, coordinando le attività di selezione e di skill inventory. Collabora con i responsabili delle diverse unità di produzione per la definizione e l'aggiornamento continuo del Piano delle Risorse e dei Piani di Formazione.
Program Management Office (PMO)	Collabora con i RUAC per rappresentare in un quadro di riferimento unico l'andamento della fornitura in termini di volumi e di impegni (Piani Operativi). Fornisce consulenza e supporto al RUAC dei Contratti Esecutivi per le attività amministrative della fornitura (es. budget, fatturazione).
Unità Locale di Sicurezza (ULS)	Riferimento unico per tutti gli aspetti legati alla sicurezza. Recepisce le politiche di sicurezza di Consip/AgID e delle PA, identifica le misure che implementano tali politiche, diffonde tali misure lungo la filiera operativa e ne monitora l'applicazione. È owner della documentazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) secondo lo standard ISO 27001. Produce i Piani della Sicurezza per i diversi Centri Servizi e successive modifiche.
Funzione di Knowledge AQ & Content Management del Portale	Struttura a supporto del RUAC di AQ e dei RUAC di CE, che assicura: ✓la valorizzazione, diffusione, replicabilità e riuso delle lesson learned, success stories e best practice acquisite nell'AQ e nella pluriennale esperienza del RTI in materia di Risk Management, Cyber Security, Security Awareness, Sicurezza Informatica, etc.; ✓gestione editoriale dei contenuti e aggiornamento del Portale della Fornitura.

Funzione di "Innovation Hub"	Struttura a supporto del RUAC di AQ e dei RUAC di CE, ha funzione di coordinamento del processo "Innovation management" (cfr. cap.17), affianca le PA nella qualificazione dei "bisogni di innovazione". Inoltre, individua e ingaggia, in fase di attivazione, sul singolo CE le strutture dell'Ecosistema dell'Innovazione del RTI più idonee, per assicurare la migliore risposta in termini di soluzioni innovative e a valore aggiunto incrementando la consapevolezza delle PA in materia di Sicurezza (es. competence center, tech-labs, incubatori e acceleratori di innovazione).
Funzione di "Funding Innovation e PNRR"	Struttura a supporto del RUAC di AQ e dei RUAC di CE, affianca le PA che intendono aderire all'AQ nella valutazione delle fonti di finanziamento dei progetti e investimenti da effettuare in materia di innovazione di processi di gestione della sicurezza (es. PNRR, fondi comunitari e nazionali, venture capital pubblico-privato).

Tabella 2 – Funzioni di staff

Supporto all'adesione

Il RTI intende promuovere l'adesione ai servizi attraverso attività condotte sia centralmente sia sul territorio, organizzate in fasi. A sostegno delle campagne di comunicazione, e come canale informativo on-line, il RTI utilizzerà l'Area Comunicazione del *Portale della Fornitura* (cfr. cap.16), allo scopo di: ✓creare e diffondere materiale informativo; ✓facilitare il contatto diretto con le PA sul territorio attraverso strumenti di pianificazione; ✓pubblicare materiale multimediale illustrativo sulle modalità di adesione all'iniziativa.

Il supporto all'adesione è affidato alle forze di Vendita e Progettazione del RTI la cui capillare diffusione sul territorio consente di raggiungere la totalità delle PA.

Nella figura a lato sono evidenziate le fasi del supporto all'adesione, all'interno del processo complessivo di contrattualizzazione, e le macro-attività previste. La singola PA sarà pertanto in grado di individuare, con il supporto del RTI, gli indicatori di digitalizzazione più idonei al monitoraggio del raggiungimento degli obiettivi definiti nel Piano triennale e conseguentemente definire il Piano dei Fabbisogni.

Figura 2 – Fasi del Supporto all'Adesione

Innovazione tecnologica

Il RTI ritiene che abbia una particolare rilevanza il costante aggiornamento tecnologico per mantenere il sistema di sicurezza delle PA allineato alle evoluzioni continue delle minacce. Pertanto, nel modello organizzativo proposto, il RTI prevede la figura di un **Referente per l'Innovazione Tecnologica** che, nella sua funzione, avrà la responsabilità di informare periodicamente Consip e le PA contraenti sull'evoluzione tecnologica dei servizi, ed eventualmente supportare le valutazioni dei comitati di coordinamento e controllo tecnico e strategico (cfr. cap.17).

Inoltre, il RTI propone un **Ecosistema dell'Innovazione** a supporto dei Team operativi, articolato come segue:

- **Global Competence Center** interni al RTI: Centri che mettono a disposizione dei team di intervento conoscenze specialistiche, metodologie, soluzioni e tool innovativi, per migliorare qualità ed efficacia dei Servizi;
- **Tech-labs, Innovation Lab e Centri di ricerca e sviluppo**: Laboratori e centri di innovazione di ricerca e sviluppo di soluzioni innovative/prototipali per la trasformazione digitale della PA. Sono strutture interne al RTI e/o costituite in partnership con grandi centri di ricerca e poli universitari nazionali e internazionali;
- **Osservatori tematici, normativi e di Cyber Security Innovation** interni al RTI: presidiano su scala globale la frontiera dell'innovazione su temi di interesse della Fornitura (es. PNRR, Cyber Security in ambito pubblico, etc.);
- **Incubatori e acceleratori di innovazione** interni al RTI e/o con i quali le aziende del RTI collaborano stabilmente (es. partnership con incubatori di innovazione, università, etc.) che sostengono e accelerano la crescita di start-up e PMI innovative, con strumenti ad hoc (es. spazi fisici e digitali di co-working, business matching e networking, accesso a nuovi mercati e alla finanza agevolata). Tali strutture rappresentano un canale privilegiato per individuare e ingaggiare in tempo reale operatori specializzati per contribuire direttamente all'innovazione delle PA aderenti all'AQ in materia di Cyber Security;
- **Partnership IT**: Strutture interne al RTI che gestiscono e sviluppano collaborazioni con vendor di soluzioni tecnologiche leader di mercato che rappresentano piattaforme abilitanti all'adozione dei programmi di trasformazione della PA in materia di "gestione della sicurezza".

Erogazione dei servizi

Il modello organizzativo proposto dal RTI per l'erogazione dei servizi ha l'obiettivo di: ✓**individuare punti di responsabilità chiari e precisi**; ✓distribuire l'esecuzione dei servizi sui diversi gruppi di lavoro in modo da ottenere la **massima efficienza nell'operatività**; ✓presidiare i processi di servizio per monitorare e favorire l'applicazione delle best practice *e* dei requisiti di qualità.

La struttura di erogazione dei servizi prevede le seguenti figure-chiave:

- **Referente Tecnico** per ciascuna PA, che riporta al RUAC del CE, assume la responsabilità tecnica dell'esecuzione di tutti i servizi. Questa figura racchiude in sé le competenze di Service Management (ITIL), di Project Management (PMI/PMBoK) e di gestione della sicurezza (ISACA CISM). Il Responsabile Tecnico si interfaccia con i Referenti della PA per tutte le problematiche di natura tecnica afferenti al CE. Costituisce il punto di riferimento anche per gli aspetti organizzativi inerenti all'allocazione delle risorse dei Servizi Specialistici con il supporto della funzione di Resource Management.
- **Responsabile dei Centri Servizi** che assume la responsabilità dei servizi forniti da remoto dal Centro Servizi Virtuale del RTI.

In figura è rappresentato il modello organizzativo generale per l'erogazione dei CE che introduce le seguenti figure:

- **Transition Manager**: Pianifica e conduce il progetto di presa in carico dei servizi da parte delle strutture operative del RTI per le attività necessarie alla transizione. Concorda con i Responsabili dei singoli servizi le tempistiche e ne traccia l'avanzamento. Riferisce al Referente Tecnico e al RUAC del CE sullo stato delle attività, e si interfaccia direttamente con le funzioni tecniche dell'Amministrazione nelle sessioni di pianificazione e di stato avanzamento della transizione. Coordina le attività di phase out di fine fornitura;
- **Responsabili Servizi:** Uno per ciascun servizio o gruppo di servizi affini. Garantiscono la regolare erogazione del servizio coordinando le attività delle risorse assegnate al proprio gruppo di lavoro. In particolare, il Responsabile SOC coordina il team dedicato a supportare la gestione di incidenti e attacchi ostili in ambito dei servizi di sicurezza; supervisiona il processo di gestione degli incidenti, intervenendo direttamente nella gestione delle escalation verso l'Amministrazione nei casi particolarmente critici o complessi;

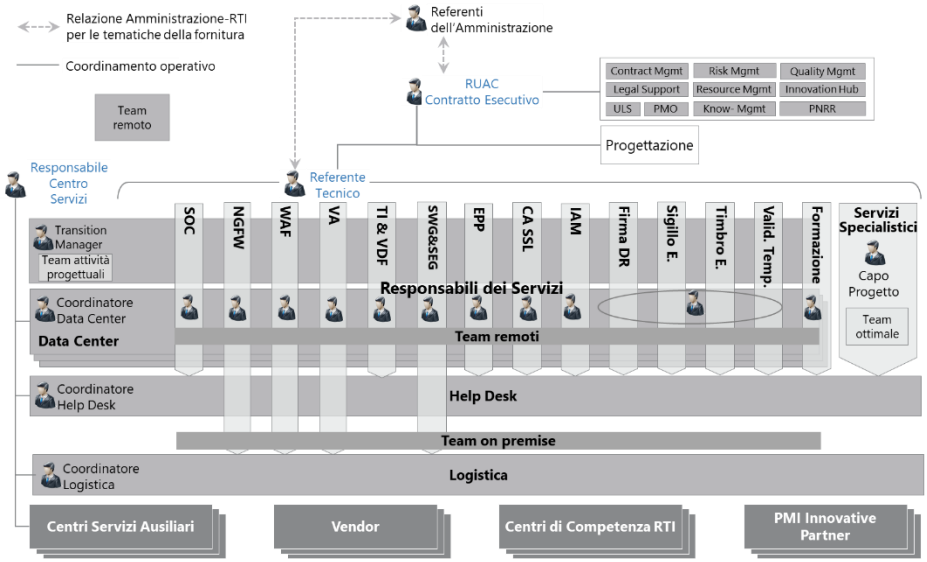

Figura 3 – Modello generale di erogazione dei servizi

- **Coordinatori Data Center**: Uno per ciascun Data Center (DC) utilizzato dal RTI per la fornitura (cfr. cap. 4), rispondono funzionalmente al Responsabile del Centro Servizi. Ogni coordinatore ha la responsabilità diretta del DC nel suo complesso: sicurezza, logistica, disponibilità degli spazi, funzionamento degli impianti, personale;
- **Coordinatore Help Desk**: Garantisce il buon funzionamento del servizio di Help Desk. Ha la responsabilità diretta del funzionamento degli strumenti, del personale, dei turni di lavoro.
- **Coordinatore Logistica**: Coordina e monitora le attività di stoccaggio e movimentazione dei materiali fra i centri logistici del RTI e la consegna dei materiali presso i punti di raccolta dei magazzini, sia in caso di nuove installazioni sia per il replacement degli apparati in caso di malfunzionamenti, supportando i tecnici preposti alla manutenzione al fine di garantire il soddisfacimento degli SLA.

Il modello è completato dalle entità di supporto, qui riepilogate: ✓**Centri Servizi Ausiliari**: Sono i Security Operation Center, i Network Operation Center e gli IT Operation Center previsti nell'organizzazione preposta all'erogazione dei servizi (cfr. cap. 4); ✓**Vendor**: Sono le aziende che producono le componenti tecnologiche HW-SW utilizzate nell'architettura di riferimento, e in particolare le strutture di supporto specifiche per i prodotti usati. Sono coinvolte nella risoluzione di problemi riscontrati sui prodotti, o in analisi e studi di fattibilità su nuovi modelli di servizio che richiedono funzionalità particolari; ✓**Centri di Competenza del RTI**: Forniscono risorse e competenze specialistiche su tematiche tecnologiche e di settore. Forniscono risorse aggiuntive da impiegare nella fornitura dei servizi per gestire eventuali picchi di lavoro; ✓**PMI Innovative/Partner**: Ecosistema di PMI innovative integrate nelle attività del RTI ed aziende terze comprese nel network di subfornitori delle aziende raggruppande, forniscono risorse specializzate a completamento di quelle messe in campo dal RTI.

3.2. DISTRIBUZIONE DELLE RESPONSABILITÀ FRA LE AZIENDE RAGGRUPPANDE

Il RTI mette a disposizione della PA capacità operative e soluzioni ampiamente consolidate presso primari clienti pubblici e privati che coprono tutti i servizi del presente AQ. Inoltre, il RTI vanta un notevole background relativamente alle procedure amministrative e ai processi interni della PA e ciò assicura la capacità di gestire forniture complesse e personalizzate in base ai diversi scenari, organizzativi e tecnologici, presenti nelle diverse Amministrazioni.

Organizzazione generale della fornitura

Le aziende raggruppande saranno organizzate secondo un modello univoco che comprende: ✓le strutture di *Account* che hanno la responsabilità dell'esecuzione dei contratti; ✓i *Centri di Competenza*, dove viene definito e implementato il portafoglio dei servizi; ✓le strutture di *Vendita* e *Prevendita*, che diffondono i servizi sul mercato; ✓i centri di *Delivery ed Operation*, che eseguono tutte le attività di attivazione ed erogazione dei servizi.
Le aziende raggruppande metteranno a disposizione del RTI le capacità delle proprie strutture per assicurare il successo della fornitura in tutte le sue componenti:

Area della fornitura	Struttura RTI	Caratteristiche
Governo AQ	Gestione Convenzioni	Struttura dedicata alla gestione del ciclo di vita delle convenzioni/AQ stipulati con Consip e ai relativi adempimenti contrattuali
Governo Contratti Esecutivi	Strutture RTI di Account	Organizzazioni dedicate alla gestione dei contratti di servizio nel settore pubblico, con focalizzazioni su PAC (incluso il settore Interforze) e su PAL
Supporto all'Adesione	Strutture RTI di Vendita e Progettazione	Strutture distribuite sul territorio (Nord-Ovest, Nord-Est, Centro, Sud) dedicate allo sviluppo del business.

Area della fornitura	Struttura RTI	Caratteristiche
Innovazione Tecnologica	Centri di Competenza RTI sulla Cyber Security	Startup Innovative e Centri di ricerca e sviluppo per la sperimentazione e la messa a punto di nuove tecnologie.
Erogazione Servizi	Strutture RTI di Delivery, Assurance ed Operation	Strutture distribuite, coinvolte nell'erogazione dei servizi oggetto di fornitura.

Tabella 3 – Strutture coinvolte nella fornitura

Sarà responsabilità del **Comitato di Governance RTI**: ✓nominare le **figure chiave** per il governo della fornitura, identificando i professionisti più qualificati per i ruoli di RUAC di AQ, RUAC di CE, Referente per l'Innovazione Tecnologica, Responsabile del Centro Servizi, Responsabili Tecnici; ✓assicurare il coinvolgimento dei **Centri di Competenza** nazionali e internazionali che si occupano delle tematiche di interesse per la fornitura; ✓assicurare la **disponibilità delle risorse** (Centro Servizi, Help Desk, Team Ottimali) necessarie all'erogazione dei servizi; ✓supervisionare l'andamento generale dell'iniziativa, il **livello di soddisfazione** delle Amministrazioni contraenti e valutare possibili evoluzioni.

Distribuzione delle responsabilità

Nella definizione del modello organizzativo per il governo e l'erogazione dei servizi, la decisione di costituire un RTI così composto nasce dalla volontà delle aziende raggruppande di sfruttare i rispettivi punti di forza in una logica di: ✓**complementarietà** nella ripartizione dei servizi con assegnazione di **ruoli e responsabilità** chiare e precise; ✓**flessibilità** nell'erogazione dei servizi grazie alla presenza di un Centro Servizi Virtuale unico, distribuito ed integrato tra le aziende del RTI in grado di erogare tutti i servizi della fornitura.

La complementarietà può essere declinata in termini di competenze tecniche ed organizzative ed in particolare la **complementarietà** di natura **organizzativa** garantisce: ✓una **governance solida,** sia a livello di Accordo Quadro sia di Contratti Esecutivi, grazie al ruolo di coordinamento svolto dalla mandataria TIM con il supporto delle mandanti, e all'adozione del **framework ITIL; ✓affidabilità**, **solidità** e **stabilità** grazie ad una presenza duratura e qualificata nel tempo delle risorse interne sugli ambiti oggetto del presente AQ.

La **complementarietà** in termini di **competenze tecniche**, si esprime nella capacità di garantire conoscenze adeguate su tutti gli ambiti di gara attraverso la sinergia delle esperienze e delle competenze acquisite: ✓**TIM e AlmavivA** possiedono infrastrutture abilitanti per l'erogazione dei servizi di Cyber Security, processi consolidati e risorse competenti per la loro gestione; ✓**KPMG** e **Netgroup** erogano principalmente servizi di formazione e di supporto specialistico grazie alla disponibilità di personale certificato negli ambiti di servizio proposti e grazie agli accordi di collaborazione con istituti nazionali ed internazionali di formazione nell'ambito specifico della Cyber Security; ✓**ReeVo** fornisce un forte impulso innovativo negli ambiti di servizio applicabili.

La complementarietà delle competenze tecniche è garantita inoltre dalla copertura delle **partnership** con tutti i principali attori sul mercato della Cyber Security e dalla presenza dei **centri di competenza** all'interno dell'**Ecosistema dell'Innovazione** che costituiranno un polo integrato cui potranno attingere le strutture operative impegnate nell'erogazione dei servizi.

In tabella si riportano le certificazioni possedute dalle aziende del RTI:

Certificazioni vendor independent	TIM	ALMAVIVA	NETGROUP	KPMG	REEVO
Togaf 9			✓		
ITIL v3/4	✓	✓	✓	✓	✓
ISO 27001 Lead Auditor	✓	✓	✓	✓	✓
ISO 27001 Foundation			✓		
ISO 22301 Auditor		✓		✓	
ISO 27017					✓
ISO 27018					✓
ISO 27701					✓
ISAE 3402 Type2					✓
SSAE 18 Type2					✓
Certified Information Security Manager (CISM)	✓	✓	✓	✓	
Certified Information Systems Security Professional (CISSP)	✓	✓		✓	
Certified Information Privacy Professional / Europe (CIPP/E)			✓		
Certified Etical Hacker (CEH)	✓	✓		✓	
Cyber Security X Fundamentals (CSX-F)	✓	✓		✓	
Certified of Cloud Security Knowledge (CCSK)	✓	✓	✓		
Certified Information System Auditor (CISA)	✓	✓	✓	✓	
Certified in Risk and Information Systems Control (CRISC)		✓		✓	
Offensive Security Certified Professional (OSCP)		✓			
OSSTMM Professional Security Tester (OPST)		✓			

eLearnSecurity Certified Professional Penetration Tester (eCPPT Gold)		✓			
CompTIA Security+		✓			
CompTIA Cybersecurity Analyst (CySA+)		✓			
Advanced Cloud Security Auditing Course		✓			
Associate Business Continuity Professional		✓			
CDPSE Data Privacy Solutions Engineer		✓			
Certified Cyber Threat Intelligence Analyst		✓			
COBIT 5 Assessor		✓			
COBIT 5 Foundation		✓			✓
CSSLP - Certified Secure Software Lifecycle Professional		✓			
eJPT - Security Junior Penetration Tester		✓			
e-Security Administration v5		✓			
e-Security Agent building v5		✓			
e-Security Analysis v5		✓			
eWPT - Security Web Application Penetration Tester v1.0		✓			
GIAC Response and Industrial Defense - GRID		✓			
GIAC Certified Incident Handler (GCIH)	✓				
Certified Intrusion Analyst (GCIA)	✓				
GIAC Penetration Tester (GPEN)	✓				

Certificazioni vendor	TIM	AlmavivA	NETGROUP	KPMG	REEVO
Splunk	✓	✓			
IBM	✓	✓	✓		✓
Oracle	✓	✓	✓		
Fortinet	✓	✓	✓		
Checkpoint	✓	✓	✓		
PaloAlto	✓	✓			
CISCO	✓	✓	✓		✓
FireEye		✓	✓		
CrowdStrike		✓			
Forcepoint	✓	✓	✓		✓
Citrix	✓	✓	✓		✓
Skybox		✓			✓
McAfee	✓		✓		
Kaspersky	✓	✓	✓		
Broadcom (Symantec/CA)	✓	✓			
Cyberark		✓		✓	
RSA		✓	✓	✓	
Rapid7					
Tenable		✓			
TrendMicro	✓	✓	✓		
Microsoft	✓	✓	✓	✓	✓
Wallix		✓			
Symantec		✓			
CA(Computer Associate)		✓			
PenTera		✓			
Qualys		✓			

Verisign		✓			
Informatica		✓			
Google	✓	✓	✓		
AWS	✓	✓	✓		✓
Forescout					✓
Darktrace					✓
Watchguard					✓
Sophos					✓

Tabella 4 - Certificazioni del RTI

Il RTI, anche grazie alla ridondanza di competenze, è in grado di assicurare massima **flessibilità** per far fronte sempre e comunque a cambiamenti nel contesto normativo, organizzativo, tecnologico e funzionale di Consip e/o delle PA e per rispondere ad esigenze particolari e di picco che possano presentarsi nell'arco della durata contrattuale. Per questo motivo la ripartizione delle attività tra le Aziende del costituendo RTI tiene conto delle specifiche specializzazioni aziendali, ma prevede, anche, un coinvolgimento multiplo sui diversi servizi per facilitare la rimodulazione e l'adattamento dell'organizzazione all'interno del RTI stesso in determinati momenti di criticità. La ripartizione delle attività di ciascun CE tra le Aziende in RTI avverrà sulla base dei seguenti criteri:✓Ambito di servizio richiesto;✓Competenze specialistiche sulle tecnologie oggetto dei servizi previsti;✓Conoscenza pregressa dell'organizzazione e dei processi operativi delle Amministrazioni.
Per quanto attiene gli ambiti e l'erogazione dei servizi, nella tabella seguente si indicano le aziende coinvolte. Il comitato di Governance del RTI definirà, sulla base delle specificità del singolo contratto, l'effettiva ripartizione dei singoli servizi tra le aziende del RTI e definirà il Responsabile del Contratto Esecutivo.

Servizio / Azienda	Governance AQ	Governance CE	Innovazione	HD	L1.S1	L1.S2	L1.S3	L1.S4	L1.S5	L1.S6	L1.S7	L1.S8	L1.S9	L1.S10	L1.S11	L1.S12	L1.S13	L1.S14	L1.S15
TIM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AlmavivA		✓	✓				✓	✓	✓		✓		✓	✓					✓
KPMG			✓					✓	✓				✓						✓
Netgroup			✓		✓								✓						✓
ReeVo			✓																✓

Tabella 5 – Ripartizione dei servizi/ambiti

3.3. RISORSE E STRUTTURE AGGIUNTIVI PROPOSTI E MODALITÀ DI INTERAZIONE CON L'AMMINISTRAZIONE

Con riferimento al modello organizzativo descritto nei precedenti paragrafi, si evidenziano i **ruoli e le strutture aggiuntive** a supporto delle figure di responsabilità richieste espressamente nel Capitolato.

Ruoli Aggiuntivi	Strutture aggiuntive
Referente Innovazione Tecnologica; Responsabile Supporto all'Adesione; Responsabile Centro Servizi; Coordinatori Data Center; Coordinatore Help Desk; Responsabile Logistica; Responsabile per ogni servizio; Capi Progetto; Transition Manager	Contract Management; Risk Management; Quality Management; Regulatory Support; Resource Management; Program Management Office (PMO); Unità Locale di Sicurezza (ULS); Knowledge AQ & Content Management; Innovation Hub e PNRR

Tabella 6 – Ruoli e Strutture aggiuntive proposte dal RTI

Risorse aggiuntive

Oltre ai ruoli ed alle strutture sopra riportate il RTI rende disponibile il supporto dei propri centri di competenza e delle relative risorse che partecipano a laboratori oltre che a collaborazioni con il mondo accademico ed enti di ricerca.
In particolare, TIM ha avviato il programma **UniversiTIM** con lo scopo di creare un ecosistema con il mondo accademico finalizzato ad una collaborazione strutturata e organizzata negli stream della ricerca.
TIM collabora con l'Agenzia Europea dedicata alla Cyber Security (**ENISA**) sui seguenti ambiti: ✓**Threat Intelligence Platform**: sperimentazione con un apposito Pilot di metodi innovativi per l'individuazione e la gestione delle minacce tipiche del mondo Telco; ✓Meccanismi di protezione da attacchi di tipo **Distributed Denial of Service** (**DDoS**): sperimentazione di strumenti innovativi sviluppati all'interno del progetto per la definizione e condivisione di specifiche "firme" di attacco che possano essere utilizzate per istruire, anche in modo automatico, gli strumenti di protezione da tali attacchi (es. firewall); ✓Analisi delle minacce emergenti, in particolare rispetto ai nuovi scenari introdotti dal 5G.
La collaborazione di TIM con il Politecnico di Torino sul tema del **Quantum Computing** (**QC**) è focalizzata sullo studio di modelli di algoritmi di **Artificial Intelligence** e **Machine Learning** e analizza il tema della **Quantum Communication** nella sua molteplicità, con particolare attenzione al livello applicativo per la **crittografia quantistica**.

AlmavivA è partner principale dell'**Osservatorio Cyber Security & Data Protection** del Politecnico di Milano all'interno di diversi gruppi di lavoro, con particolare attenzione a trend di mercato e use case aziendali in ambito Privacy, ai modelli organizzativi e alle nuove competenze, all'offerta tecnologica, alla filiera di soluzioni e servizi di Sicurezza ICT, alle modalità di gestione del rischio cyber e ai temi di conformità normativa.

AlmavivA dispone di **laboratori**: ✓sull'applicazione di soluzioni di Web Application Firewall, in cui si approfondiscono con particolare attenzione gli aspetti applicativi della protezione dei servizi WEB esposti in rete in funzione della costante evoluzione delle minacce cibernetiche; ✓per il Mobile Security Assessment che permette, tramite dispositivi dedicati fisici con framework di sviluppo, l'emulazione di dispositivi mobili con sistema sia Android sia iOS, virtualizzando dunque l'accesso al sistema operativo senza le limitazioni imposte dai produttori.

TIM, AlmavivA e Netgroup fanno parte del **Centro di Competenza nazionale ad alta specializzazione per la Cyber Security CYBER 4.0**, finanziato dal Ministero dello Sviluppo Economico. Tale centro è espressione di un partenariato pubblico e privato, interdisciplinare e multi-attoriale, che copre un ampio spettro di competenze e favorisce lo sviluppo di una rete di collaborazioni qualificate e mira a sviluppare la competitività del sistema Paese offrendo, in particolare, alla Pubblica Amministrazione servizi di formazione e finanziando progetti di ricerca e innovazione per innalzare il livello di protezione dal rischio di attacchi cyber a sistemi, processi e asset strategici nazionali. Il RTI è anche impegnato nel selezionare, accelerando e co-creando idee, prodotti e servizi innovativi provenienti dal mondo delle startup. Ad esempio, il **TIM WCAP** (**Working Capital**) distribuito su cinque hub territoriali (Milano, Bologna, Roma, Napoli e Catania), favorisce una contaminazione tra le **startup**, i **produttori di tecnologia**, i principali **Atenei** ed i **Centri di Ricerca** italiani.

Modello di relazione con le Amministrazioni contraenti

Le figure di riferimento del RTI interagiscono con i referenti della PA contraente sulla base dei rispettivi ruoli e responsabilità. Il modello prevede un *numero ben delimitato di interfacce*, ciascuna in possesso delle conoscenze e dell'autorità specifica per il ruolo, allo scopo di **massimizzare l'efficienza** *e* **l'efficacia del governo della fornitura**.

Come rappresentato in figura, l'interazione fra RTI e PA passa principalmente per quattro figure o funzioni:

- **RUAC del CE** – per gli aspetti generali della fornitura e specificamente per gli aspetti contrattuali e amministrativi;
- **Responsabile Tecnico** – per tutto quanto riguarda l'andamento dei servizi e delle attività progettuali;
- **Capo Progetto** – per gli aspetti specifici riguardanti le attività dei servizi specialistici;
- **Help Desk** – per l'assistenza informativa, amministrativa e tecnica.

A questi si aggiunge l'interazione fra il **Transition Manager** del RTI e i Referenti dell'Amministrazione durante i soli periodi di presa in carico dei servizi e di phase out. Tutti i ruoli, le strutture e le risorse aggiuntive proposte dal RTI potranno essere coinvolti, per il tramite del Referente Tecnico, nei casi in cui le PA contraenti necessitino di un supporto su una tematica particolarmente complessa.

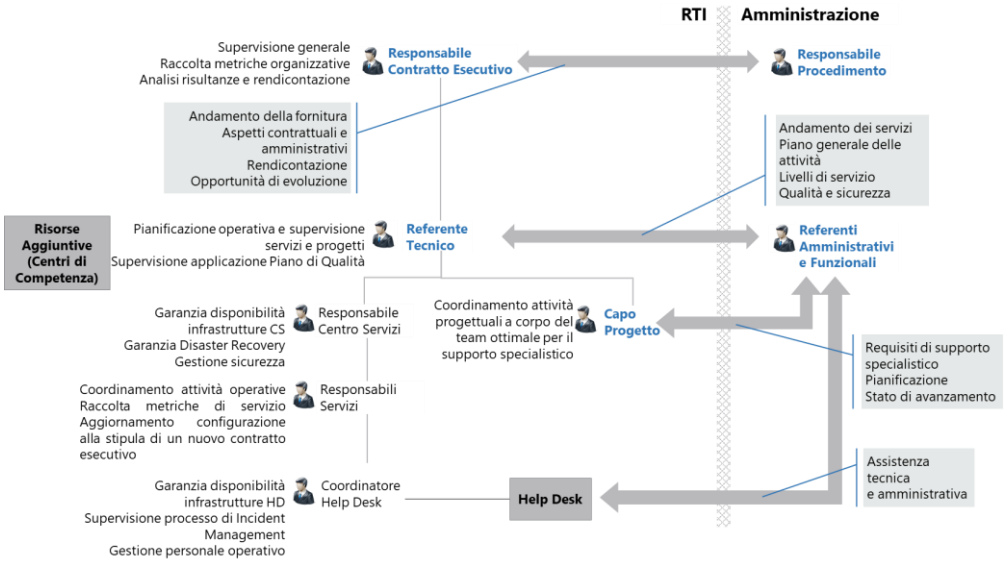

Figura 4 – Modello di relazione

4. PROPOSTA PROGETTUALE PER I "CENTRI SERVIZI"

Il RTI metterà a disposizione una soluzione organizzativa basata su un **Centro Servizi Virtuale**, distribuito su più **Data Center** (DC) e **Control Room** (CR), attivo e presidiato in modalità continuativa (H24x7) da personale qualificato e certificato e in grado di gestire i servizi contrattualizzati dalle Amministrazioni nell'ambito dell'AQ.

4.1. CARATTERISTICHE TECNOLOGICHE E MODALITÀ OPERATIVE DI FUNZIONAMENTO DEI CENTRI SERVIZI

Il Centro Servizi Virtuale è distribuito sul territorio nazionale ed organizzato sulle seguenti componenti:

- **Data Center,** dotati d'infrastrutture hardware/software con elevatissimi livelli di affidabilità, disponibilità e sicurezza dove sono ospitate le piattaforme per l'erogazione e la gestione dei servizi previsti nell'AQ;
- **Control Room,** costituite da personale altamente specializzato distribuito su più sedi per garantire la massima affidabilità e flessibilità nella gestione dei servizi previsti.

Dispone, inoltre, di una **piattaforma strumentale altamente integrata** che abilita i processi in maniera agile e ne garantisce la continuità operativa, attraverso i meccanismi di protezione dei DC e le tecnologie adottate a supporto dei processi di Disaster Recovery, e di **un'organizzazione di risorse capaci ed interconnesse digitalmente** in grado di sostenere il servizio anche in condizioni di picco o di indisponibilità di una o più CR grazie a tecniche di shadowing, multidisciplinarietà, training on the job, etc. La molteplicità di DC di cui dispone il RTI testimonia l'esperienza e la consolidata capacità operativa delle aziende raggruppande. Ricordando la modalità "managed" di erogazione dei servizi e la loro criticità, la soluzione scelta per il Centro Servizi è disegnata complessivamente sui 6 poli geografici riportati in tabella ed è in grado di offrire la massima flessibilità operativa e solidità all'intera fornitura. Al fine di garantire le Amministrazioni da eventuali picchi di lavoro, il RTI ha previsto di distribuire ogni servizio tra 2 DC Primari (Acilia e Casal Boccone) e 2 secondari di DR (Rozzano e Milano) ad eccezione dei servizi di Firma Digitale Remota, Sigillo Elettronico, Timbro Elettronico e Validazione Temporale Elettronica

Qualificata che sono erogati dalla sola mandataria attraverso l'utilizzo di un sito Primario (Pomezia) e un sito Secondario per la continuità operativa (Roma Oriolo) dedicati e certificati per i servizi fiduciari.

Nella tabella che segue è indicata l'ubicazione geografica dei DC che saranno utilizzati e l'azienda responsabile del loro funzionamento operativo.

Il modello di erogazione dei servizi prevede un'infrastruttura di erogazione dedicata alla PA all'interno di ciascuno dei DC, sia Primari che Secondari. **Tutti i Data Center sono certificati ISO/IEC 27001**.

Il monitoraggio e la gestione dei servizi richiesti in AQ sono erogati attraverso personale qualificato e certificato dislocato presso le seguenti Control Room (CR) del RTI:

- **Control Room Sud** distribuita sulle sedi di Bari - Piazzale Mater Ecclesiae 5 - e di Taranto – via Campania 11;
- **Control Room Centro** sulla sede di Roma – via di Scalo Prenestino 15.

Azienda	Città	Indirizzo
TIM	*Acilia*	Via di Macchia Palocco, 223 (RM)
	Rozzano	Viale Toscana, 3/5 (MI)
	Pomezia	SS148 Pontina km.29,100 (RM)
	Roma Oriolo	Via Oriolo Romano, 257 (RM)
ALMAVIVA	*Roma Casal Boccone*	Via di Casal Boccone, 188 (RM)
	Milano	Via dei Missaglia, 97 - ed. B4 (MI)

Tabella 7 – DC a disposizione del RTI

Tali CR operano ripartendosi le attività in funzione del carico di lavoro e delle specifiche competenze richieste in sede di ciascun contratto esecutivo. La scelta di separare fisicamente le CR dai Data Center è funzionale alla necessità di garantire la continuità operativa, disaccoppiando le infrastrutture a supporto dagli operatori che le gestiscono/utilizzano, minimizzando così gli impatti di eventuali fault di una delle sedi. Inoltre, i siti sono connessi fra loro attraverso la **VDCN** di TIM (Virtual Data Center Network), rete di trasmissione dati IP/MPLS ad altissima velocità (10 Gbps scalabili a multipli di 10) che abilita sia la connettività per l'erogazione dei servizi sia l'allineamento fra i DC del RTI. L'infrastruttura di routing ha una capacità di forwarding di 100 Gbps e rende tutto il modello di servizio *un unico grande centro "virtuale" di erogazione.* In conclusione, la soluzione consente di ottimizzare sia il traffico fra i sistemi, sia il traffico di gestione, specializzando l'erogazione di servizi in funzione della distribuzione delle risorse rispondendo pienamente ed efficacemente a possibili situazioni di indisponibilità e garantendo la *totale continuità del servizio*. Tutti i DC messi a disposizione dal RTI sono già collegati sia ad Internet, tramite due differenti Service Provider afferenti a due POP attraverso percorsi differenziati, sia alla rete **SPC**, il che li rende, dal punto di vista della rete, immediatamente disponibili ad erogare i servizi del presente AQ alle PA.

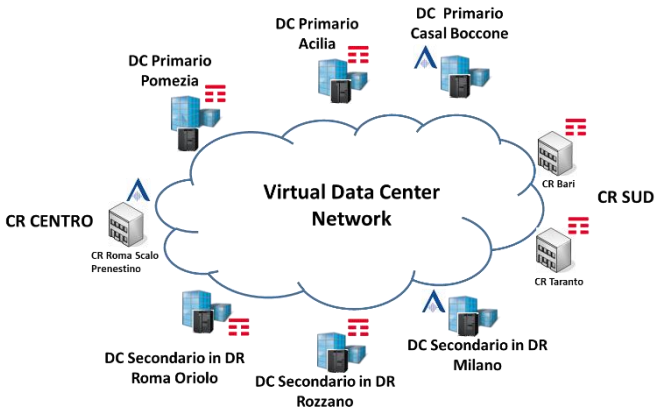

Figura 5 – Architettura Centro Servizi Virtuale

I Centri Servizi ausiliari

Il modello di servizio previsto dal RTI viene completato dai Centri Servizi ausiliari dislocati sul territorio italiano e focalizzati sulla gestione delle piattaforme tecnologiche e ai servizi infrastrutturali (backup, monitoraggio, disaster recovery, etc.) interne alle aziende del RTI. I Centri Servizi ausiliari disponibili sono:

- **Information Technology Operation Center (ITOC)** per la gestione sistemistica delle piattaforme e dei servizi infrastrutturali;
- **Network Operation Center (NOC)** per le attività di supervisione proattiva/reattiva della connettività dei DC;
- **Security Operation Center (SOC)** per le attività specialistiche volte ad assicurare una corretta gestione delle configurazioni dei sistemi di sicurezza fisica e logica dei DC e delle CR del RTI;
- **Data Center Services (DCS)** per le attività di monitoraggio, gestione e configurazione delle infrastrutture dei DC.

4.1.1. Sicurezza del Centro Servizi

Di seguito vengono descritte le misure di sicurezza distinte per ambito specifico (fisico, logico ed organizzativo) che il RTI intende mettere a disposizione dell'Amministrazione.

Sicurezza Fisica

Sistemi per il controllo accessi: presenti in tutti gli ambienti e strutture critiche con adeguato livello di sicurezza. Il RTI fornisce sia tecniche di Anti pass-back, che prevengono potenziali abusi nell'utilizzo dei badge personali, sia di Anti piggy-backing, che evitano l'accesso fraudolento mediante accodamento al passaggio di un utente autorizzato. Oltre al sistema di riconoscimento tradizionale, mediante un badge personale, il RTI prevede l'inserimento di un badge biometrico, attraverso un Badge MIFARE® contenente l'impronta digitale dell'assegnatario. Inoltre, il RTI garantisce l'**antintrusione** mediante un muro di cinta sormontato da barre di acciaio, con accessi carrai controllati da un servizio di guardiania armata del Comprensorio che opera h24, 7 giorni su 7 e da un sistema antintrusione perimetrale a microonde e raggi infrarossi. In aggiunta, il RTI prevede un sistema di videosorveglianza evoluto controllato dal servizio di guardiania operante H24 7/7. In particolare, il DC di Acilia, certificato Tier IV, è dotato di un sistema di sicurezza perimetrale con rilevamento automatico delle intrusioni, geolocalizzazione e tracking degli intrusi con Radar Navtech e telecamere termiche intelligenti Sightlogix integrate con la piattaforma di Video Management. Tale piattaforma è in grado di garantire la sicurezza su aree molto ampie, in qualsiasi condizione ambientale, e di rilevare una persona fino a 1000m di raggio, un veicolo fino a 2000m di raggio e di fornirne la posizione GPS seguendone i movimenti su una mappa con tracking automatico.

Rack: Gli apparati sono alloggiati in rack normalmente accessibili attraverso l'utilizzo di chiavi. In alcuni casi è prevista la messa in sicurezza dei rack (o delle **Cage**), attraverso l'impiego di sistemi biometrici di controllo accessi. È possibile inoltre allestire **Suite** delimitate da pareti grigliate accessibili tramite badge al solo personale autorizzato.

Continuità elettrica: il RTI garantisce la disponibilità di stazioni di trasformazione dell'energia elettrica dedicate alimentate da un consorzio di fornitori, da quadri elettrici ridondati, da gruppi di continuità (in ridondanza N+1) che entrano a regime in meno di un minuto in caso di black-out e da batterie di backup per la gestione del transitorio fino all'attivazione dei gruppi di continuità. Gli impianti elettrici (fino alla singola presa di alimentazione del rack) sono presidiati H24 per 365 giorni l'anno e controllati tramite un **Building Management System centralizzato**.

Rilevatori antifumo e antincendio: sono presenti, in tutti gli ambienti, rilevatori antifumo e antincendio con attivazione automatica dei relativi impianti di spegnimento degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. La rilevazione fumi è garantita da un impianto con sensori ottici posizionati sottopavimento, in ambiente e nel controsoffitto. Sono presenti anche mezzi estinguenti mobili e un impianto fisso ad idranti, ed un sistema di ricircolo dell'aria primaria che si aziona automaticamente in caso di allarme incendio.

Antiallagamento: sono presenti sonde in grado di rivelare la presenza di liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua e pompe elettriche in grado di convogliare e scaricare all'esterno perdite di acqua.

Sicurezza Logica

Ad ogni Amministrazione contraente, il RTI garantisce l'isolamento e la protezione dei dati. Le tematiche di gestione del rischio e della compliance vengono indirizzate attraverso:

- processi di Gestione della Sicurezza, che saranno descritti in dettaglio nel relativo Piano;
- corretta gestione dei profili di accesso di tipo amministrativo assegnati da specifica struttura organizzativa separata da quelle deputate alla gestione tecnica dei sistemi, in conformità al Provvedimento del Garante Privacy 1.6.2006;
- rispetto degli obblighi di legge previsti dal Testo Unico in materia di privacy – D.Lgs. 196/03;
- conformità agli standard internazionali di sicurezza e alle best practice richiamate anche dall'ISO27001 in materia di User Access Management;
- framework documentale interno per la descrizione di policy e linee guida di riferimento; nello specifico tutte le aziende del RTI utilizzano un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme allo standard ISO/IEC 27001, per assicurare la protezione, l'affidabilità, la riservatezza e l'integrità delle informazioni delle Amministrazioni, il patrimonio intellettuale, le attività e le informazioni affidate da terzi.
- conformità alle linee guida di riferimento emanate dagli enti internazionali che si occupano di sicurezza informatica, quali ad esempio il National Institute of Standards and Technology (NIST), la European Union Agency for Network and Information Security (ENISA).

I processi rispettano i principi generali stabiliti da tali norme, quali l'univocità degli identificativi personali, il minimo privilegio secondo le funzioni svolte, la tracciabilità delle operazioni, la separazione dei ruoli a livello funzionale o individuale, la riservatezza delle informazioni, la protezione di dati e sistemi attraverso meccanismi di segregazione a più livelli. In particolare, gli accessi ai sistemi da parte del personale tecnico vengono tracciati attraverso un sistema di Security Log Management e conservati secondo quanto previsto dalle normative correnti in materia di sicurezza.

Sicurezza Organizzativa

Al fine di garantire un'organizzazione dei Centri Servizi sicura ed efficace, il RTI prevede la condivisione di **Procedure di escalation a fronte di eventi di fault o anomalie** con impatto rilevante sull'operatività del DC. Una volta innescata la procedura di escalation, i responsabili operativi impegnati nella risoluzione del problema mantengono costantemente aggiornati i livelli superiori coinvolti. Le informazioni pervenute sono analizzate al fine di stabilire se il livello di criticità raggiunto è tale da richiedere il coinvolgimento dei Responsabili dei Centri Servizi. Sono previste anche **Procedure di backup & restore** specifiche per le piattaforme applicative installate presso i DC a supporto dell'erogazione dei servizi di AQ. Il RTI prevede, infine, un **Piano di Disaster Recovery.** Per questo motivo, il RTI ha individuato DC Secondari distanti più di 200Km dai Primari nei quali replicare infrastrutture e dati necessari a garantire la continuità operativa anche a fronte di eventi disastrosi che colpiscano una significativa area geografica. Il suddetto piano prevede:

- tecniche di ridondanza delle infrastrutture IT (connettività, sistemi elaborativi e sistemi di storage duplicati con tecniche di clusterizzazione, mirroring, virtualizzazione, etc.) che garantiscono un alto grado di resilienza all'insorgere di guasti;
- backup dei dati delle PA sia su infrastrutture di storage poste in ambienti separati dei DC con garanzia di elevata protezione fisica, sia su copie di sicurezza trasferite su altri DC del RTI sempre all'interno del territorio comunitario;
- replica asincrona tra gli storage dei siti di produzione e di DR.

4.2. CARATTERISTICHE INFRASTRUTTURALI E LOGISTICHE A SUPPORTO DELL'IMPATTO AMBIENTALE

Caratteristiche logistiche e infrastrutturali

I DC proposti dal RTI per la fornitura sono tutti **Tier III** ad eccezione del DC TIM di Acilia classificato **Tier IV**. Complessivamente dispongono di migliaia di metri quadri di sale sistemi e sale TLC. Le sale sistemi sono predisposte in modo modulare e consentono sia l'hosting "intensivo" dei sistemi sia la configurazione rapida di spazio ad-hoc. Sono presenti inoltre aree magazzino, sale ignifughe (Lampertz) per la conservazione di dati sensibili ed ambienti predisposti ad ufficio. In particolare, il DC di Acilia garantisce una disponibilità del 99,995% equivalente a 26 minuti di fermo ammissibili all'anno.

Soluzioni a supporto dell'impatto ambientale

I DC proposti dal RTI sono stati progettati, realizzati e gestiti ponendo attenzione ad aspetti ambientali che non si riducono alla sola efficienza energetica ma anche ad aspetti puramente volti al rispetto e alla tutela ambientale. TIM, così come tutto il RTI, ha un ruolo fondamentale nel contribuire allo sviluppo sostenibile ovvero al processo di cambiamento tale per cui lo sfruttamento delle risorse, la direzione degli investimenti, l'orientamento dello sviluppo tecnologico e i cambiamenti istituzionali siano orientati ad eliminare o a ridurre al minimo, ove ciò sia attuabile, gli impatti negativi sull'ecosistema generati dalle proprie attività. TIM si è dotata di un **Sistema di Gestione Ambientale** conforme alla norma **UNI EN ISO 14001** ottenendo la relativa certificazione. TIM ha inoltre ottenuto la certificazione del **Sistema di Gestione dell'Energia** in conformità con la norma **UNI EN 50001**. Nel 1996 TIM è stata uno dei fondatori del Corporate Responsibility Charter dell'ETNO; nel 2002 ha sottoscritto il Global Compact delle Nazioni Unite, che invita ad adottare un approccio responsabile favorendo lo sviluppo e la diffusione di tecnologie ecosostenibili; nel 2009 è stata tra i fondatori dell'iniziativa JAC (Joint Audit Cooperation) attraverso cui viene valutata la performance di sostenibilità dei fornitori strategici mediante audit di terze parti; nel 2015 ha aderito all'organizzazione

internazionale Global e-Sustainability Initiative che rappresenta il riferimento in merito alla sostenibilità nel settore specifico dell'ICT. Nel rispetto di tali impegni i DC di TIM sono gestiti nel segno dell'efficienza energetica e della sostenibilità ambientale che si traduce in: ✓sostituzione degli apparati più datati con nuovi meno energivori; ✓l'utilizzo di Evaporative Free Cooling, che garantisce una maggiore resilienza operativa; ✓DC costruiti e gestiti secondo principi "green" con le più avanzate tecniche di raffreddamento, ma anche soffitti e mura in grado di gestire al meglio la temperatura; ✓l'impiego di batterie agli ioni di litio al posto di quelle al piombo; ✓l'impiego di luci LED a basso consumo energetico etc. In particolare, all'interno del DC di Acilia, certificato Tier IV, l'impianto di refrigerazione è affiancato da un innovativo **sistema green** che immette all'interno aria fresca e disperde nel sottosuolo, a 30 mt di profondità, il calore in eccesso prodotto mediante un sofisticato impianto geotermico (**dispersori geotermici**), ed inoltre i servizi di alimentazione ausiliari del DC sono alimentati ad energia solare. Tali accorgimenti tecnologici innovativi consentono al DC di Acilia di raggiungere un livello di efficienza energetica PUE (**Power Usage Effectiveness**) pari a **1,3** riducendo significativamente la quantità di emissioni di gas. TIM pone grande attenzione anche all'aspetto ambientale di tutela del territorio su cui vengono realizzati i propri DC: dai sistemi di raccolta delle acque pluviali, al materiale drenante per il suolo su cui vengono costruiti, dalle vernici mangia-smog e battericide, a sistemi di illuminazione intelligenti, fino all'adozione di piccole famiglie di animali autoctoni per limitare l'impatto delle costruzioni sull'ambiente. I Data Center AlmavivA possiedono caratteristiche infrastrutturali che garantiscono elevati livelli di affidabilità, disponibilità e sicurezza dei servizi erogati, sono certificati ISO 27001, ISO 22301 per la Business Continuity, ISO 50001 per l'Efficienza Energetica e ISO 14001 per la Sostenibilità Ambientale.

Particolare attenzione è dedicata alla sostenibilità ambientale, perseguita attraverso l'accurato e costante controllo dei consumi elettrici, monitorati con l'indice di efficienza energetica **PUE** (**Power Usage Effectiveness**) paria **1,3**, e la riduzione delle emissioni di gas serra, attraverso l'utilizzo ad esempio di tecnologie di estinzione incendi innovative, il tutto monitorato con l'indicatore di sostenibilità **CUE** (**Carbon Usage Effectiveness**). La gestione efficiente dell'energia è testimoniata dalla certificazione ISO 50001 delle due sedi di Roma e della sede di Milano Missaglia.

4.3. HELP DESK – CARATTERISTICHE ORGANIZZATIVE, METODOLOGICHE, TECNICHE, DIMENSIONALI E FORMATIVE

La soluzione proposta dal RTI per il servizio di Help Desk (HD) deriva dall'esperienza maturata nel recente passato nella gestione di convenzioni e contratti quadro con AgID e Consip. Tutti gli aspetti del servizio, sia organizzativi sia tecnici, soddisfano i requisiti di gara e tengono conto delle best practice operative nel trattamento dei tipici casi d'uso nella PA.

Aspetti organizzativi e metodologici

Il servizio di Help Desk, erogato secondo la metodologia ITIL, è strutturato in modo da indirizzare adeguatamente le richieste di ogni singola Amministrazione contraente in modo specifico e contestualizzato. L'Help Desk è accessibile attraverso un'infrastruttura multicanale, in grado di gestire i contatti in modo unificato e omogeneo. I diversi canali di accesso disponibili sono integrati in un modello unico di trattamento, in cui le segnalazioni vengono indirizzate a diversi gruppi specializzati di operatori utilizzando politiche "intelligenti" di instradamento.

Il supporto fornito dall'HD si articola su due livelli logici, entrambi in grado di soddisfare:

1. richieste di tipo *informativo*, provenienti da PA che non hanno ancora aderito ai servizi dell'AQ;
2. richieste di tipo *amministrativo*, provenienti da PA già contraenti, su aspetti legati alla conduzione del contratto;
3. richieste di tipo *tecnico*, provenienti da PA contraenti che abbiano la necessità di avere sia un supporto sull'utilizzo dei servizi dell'AQ, sia di segnalare malfunzionamenti o eventuali incidenti di sicurezza.

Le richieste di tipo 1 sono disponibili a tutte le PA, mentre quelle di tipo 2 e 3 richiedono un *PIN di riconoscimento*, assegnato alle PA alla stipula del contratto.

L'**HD di 1° livello**: ✓assicura la comunicazione tempestiva ed efficace con i referenti delle PA; ✓riceve, registra le chiamate/e-mail dei referenti e comunica il codice identificativo del ticket; ✓assiste le PA per ciò che riguarda le attività propedeutiche alla sottoscrizione dei contratti; ✓classifica la richiesta fornendo direttamente una soluzione per i problemi non complessi o smista la richiesta al 2° livello; ✓controlla lo stato di avanzamento del ticket e informa il referente PA; ✓produce ed analizza le statistiche sugli interventi, per identificare i fabbisogni e definire azioni di prevenzione dei problemi.

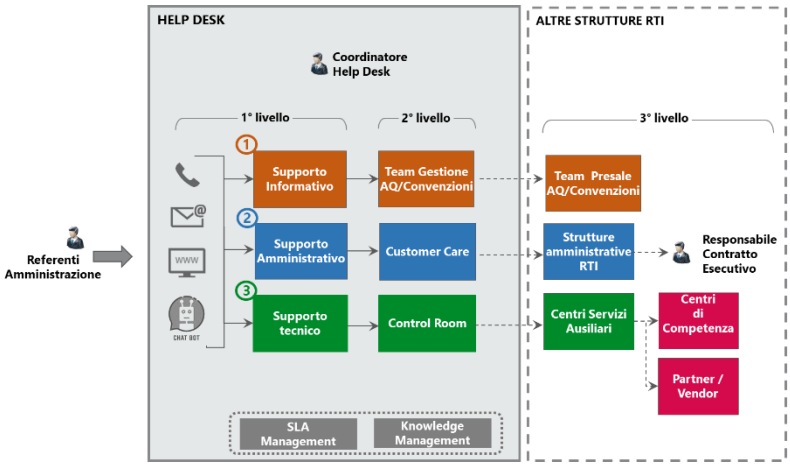

Figura 6 - Schema organizzativo generale dell'Help Desk

Le funzioni di ***2° livello*** dell'**HD** sono svolte da:

- **Team Gestione AQ/Convenzioni** che fornisce informazioni sull'AQ prima dell'adesione e supporto per compilare il Piano dei Fabbisogni;
- **Customer Care** che fornisce supporto su aspetti amministrativi dei contratti esecutivi stipulati;
- **Control Room** che fornisce assistenza ai referenti tecnici delle PA sulle segnalazioni di fault sui servizi acquisiti.

La struttura è completata da una funzione di **Knowledge Management**, che si fa carico di alimentare la Knowledge Base del servizio sulla base delle segnalazioni dei team operativi di supporto, secondo i meccanismi organizzativi e operativi descritti di seguito e da una funzione di **SLA Management** che monitora la qualità del servizio erogato rispetto ai livelli di servizio contrattualizzati, individuando situazioni potenzialmente critiche e identificando le azioni correttive intese ad assicurare che gli SLA vengano soddisfatti. Gli orari e le modalità di erogazione del servizio sono rispondenti ai requisiti di Capitolato.

Caratteristiche tecniche: infrastruttura tecnologica, modalità di accesso, strumenti a supporto

La soluzione infrastrutturale proposta dal RTI, per fornire il servizio di HD, è basata su un modello di servizio di tipo Hosted Contact Center (HCC) che utilizza le stesse funzionalità di Accoglienza e Routing Operatore dei Contact Center che TIM utilizza per fornire servizi di accoglienza ai propri Clienti. Le principali caratteristiche dell'infrastruttura sono: ✓**Scalabilità** che consente di inserire rapidamente nuove postazioni operatore che necessitano solo di un

PC e un telefono; ✓**Interoperabilità** che consente di integrare i diversi moduli che compongono l'infrastruttura anche con sistemi esterni grazie alla disponibilità di librerie e interfacce standard; ✓**Affidabilità**: garantita dalla replica delle componenti dell'infrastruttura per consentire la normale esecuzione del servizio in caso di fault.

L'infrastruttura di servizio si divide in 3 principali macro-blocchi:

- **Canali di accesso al servizio** di HD schematizzati nella figura 6:
  - **canale telefonico**, attraverso numero verde dedicato, con tre post-selezioni gestite tramite IVR per avere subito accesso all'operatore di 1° livello con le competenze richieste;
  - **canale e-mail** attraverso la configurazione di una casella e-mail dedicata e riservata all'AQ*;*
  - **canale web**, corrispondente alla funzionalità di self-ticketing accessibile attraverso il Portale della Fornitura, (cfr. Cap.16).

  Come **funzionalità aggiuntiva**, allo scopo di incrementare l'efficacia e l'efficienza dei servizi di HD per le PA contraenti, il RTI potrà rendere disponibile dal Portale della Fornitura, come ulteriore canale di accesso, una **ChatBot** che utilizza algoritmi di intelligenza artificiale per sostenere un dialogo strutturato con l'utente. Tale strumento si è dimostrato estremamente efficace in contesti analoghi come chiave di accesso per un'interazione rapida ed immediata degli utenti con il servizio di HD. La ChatBot incorpora funzioni di Machine Learning, dunque apprende dalle interazioni con gli utenti e dai comportamenti di quest'ultimi per fornire risposte rapide e precise, automatizzando quindi una serie di attività e offrendo un primo livello di assistenza.
- **Funzionalità Automatiche di Accoglienza (IVR)**, permette velocità e flessibilità nel disegno, messa in esercizio e gestione degli alberi di navigazione e dei contenuti vocali;
- **Motore di Routing Multicanale**, basato su tecnologia **Genesys**, che abilita il routing dei contatti in modalità Blending, ovvero combinando in automatico la distribuzione dei canali di accesso sincroni (Voce, Chatbot) con i canali asincroni (Mail, Web) in modo tale che l'operatore possa gestire contemporaneamente, ad esempio, sia il canale voce sia il canale mail.

Lo strumento principale utilizzato dagli operatori a supporto del servizio di HD è la **piattaforma ITSM BMC Remedy** che consente di definire i diversi processi ITIL secondo meccanismi di workflow, che ingaggiano le varie funzioni operative dell'organizzazione a seconda del trattamento richiesto, con meccanismi di escalation sui vari livelli in presenza di situazioni critiche. La piattaforma BMC Remedy: ✓supporta tutti i processi di acquisizione e gestione delle richieste e degli incidenti; ✓**consente la gestione centralizzata degli asset IT** e delle relative informazioni tecniche ed amministrative attraverso il modulo della suite BMC di **Asset & Configuration Management** e sulla base delle informazioni contenute nell'**Atrium CMDB**; ✓implementa la base di conoscenza della fornitura attraverso modalità multiple di classificazione e indicizzazione dei contenuti; ✓consente ai referenti di inserire richieste verso l'HD utilizzando il tool di **self ticketing** accessibile dal Portale della Fornitura anche per verificare lo stato delle richieste pendenti; ✓consente di distribuire, grazie al motore di workflow interno, le attività lungo l'organizzazione e monitorarne l'esecuzione, per massimizzare l'efficienza del processo.

Dimensionamento dei gruppi di supporto

Il gruppo di lavoro preposto al servizio di HD (1° e 2° livello) sarà **dimensionato in modo dinamico**, in funzione del numero delle PA contraenti e del volume complessivo dei servizi sottoscritti. Le ipotesi dimensionali utilizzate si basano sulle numerose esperienze maturate dal RTI in analoghi servizi di HD gestiti in altri Accordi Quadro/Convenzioni; mensilmente, tale dimensionamento sarà rivisto dal Responsabile dell'HD in funzione dei seguenti parametri:

- Profili di traffico:
  1. Numero di contatti al mese: ✓**60%** da canali sincroni (telefono, chatbot); ✓**40%** da canali asincroni (e-mail, web).
  2. Distribuzione percentuale dei contatti sui tre gruppi di supporto: ✓Informativo **5%**, ✓Amministrativo: **25%**, ✓Tecnico: **70%**.
  3. Distribuzione del traffico sulle diverse fasce orarie: ✓**89%** Lun-Ven dalle ore 08:30 alle ore 17:30; ✓**7%** Sabato dalle ore 08:30 alle ore 13:30; ✓**4%** Lun-Ven dalle ore 17:30 alle ore 08:30, il Sabato dalle ore 13:30 alle ore 24:00, la domenica e nei giorni festivi.
- Parametri di Servizio:
  1. Tempo massimo di attesa netto per il servizio telefonico: **60 secondi nel 95%** dei casi (cfr. indicatore di qualità HDCG);
  2. Tempo di presa in carico di una singola richiesta: **10 minuti nel 95%** dei casi, (cfr. indicatore di qualità HDPC);
  3. Tempo di risoluzione delle richieste da parte dell'HD: in funzione della priorità assegnate, **4 ore nel 98%**, **8 ore nel 96%**, **12 ore nel 94%** dei casi (cfr. indicatore di qualità HDTR);
  4. Numero di chiamate perse: **2%** del numero totale delle chiamate ricevute dall'HD;
  5. Tipologia e complessità dei servizi previsti;
  6. Numero di richieste la cui gestione è demandata all'Help Desk di secondo livello;
- **Tempi Medi di Servizio (TMS)**: sono stati infine stimati i TMS differenziati in base ai tre diversi gruppi di supporto ed in particolare, per i contatti telefonici, sono stati considerati i seguenti valori: ✓Informativo: TMS pari a **400 secondi**; ✓Amministrativo: TMS pari a **460 secondi**; ✓Tecnico: TMS pari a **540 secondi**.

I TMS indicati tengono conto sia del "*trattamento del contatto*" stesso (**TMC** + **ACW** = **T**empo **M**edio **C**onversazione + **A**fter **C**all **W**orking) sia del "*tempo di inattività*" (tempo di ready) dopo la chiusura del contatto. Le differenze riportate per i diversi gruppi tengono conto delle specificità delle richieste e dell'andamento del traffico offerto.

Sulla base delle ipotesi descritte in precedenza, utilizzando i classici modelli di teoria delle code (formula di Molina inversa per il calcolo dei serventi necessari), sarà definito il dimensionamento, in termini di FTE, delle risorse necessarie per il corretto funzionamento del servizio di HD. Inoltre, a maggior garanzia della capacità di gestire i picchi di traffico, si sottolinea che il modello organizzativo proposto dal RTI per la struttura di HD, prevede un **Gruppo Regia** che monitora in tempo reale la curva del traffico offerto agli operatori ed è quindi in grado di implementare politiche di bilanciamento adattativo del carico di lavoro sulle code di operatore in tempi estremamente ridotti, sfruttando le caratteristiche di scalabilità della infrastruttura tecnologica.

Aspetti Formativi

Gli operatori dell'HD verranno formati per acquisire competenze su: ✓*tecniche di interazione* – accoglienza, gestione contatto, modalità di ascolto e dialogo, etc.; ✓processo di *gestione della richiesta* e *utilizzo della piattaforma* di Trouble Ticketing; ✓*tematiche di base* della fornitura – per tutti gli operatori di 1° livello; ✓*tematiche specialistiche* della fornitura (contrattuali, amministrative, tecniche) – per gli operatori di 2° livello, differenziate per ciascun gruppo.
La formazione sarà continua sulla base delle esigenze espresse e della gap analysis rilevata. Gli operatori verranno sottoposti a *quick test periodici* per misurare il loro livello di competenza ed evidenziare la necessità di cicli di formazione ulteriore. Gli operatori disporranno di: ✓"*Call Guide*" per i vari tipi di problematiche, per rendere più efficace il contatto e risolvere più velocemente le richieste degli utenti; ✓un sistema di Knowledge Base alimentato in modo incrementale, in cui gli operatori dell'Help Desk potranno memorizzare soluzioni per risolvere richieste ricorrenti o ripetibili, (le cosiddette "one call solution"), e limitare i trasferimenti al 2° livello.

5. PROPOSTA PROGETTUALE PER IL SERVIZIO "SECURITY OPERATION CENTER (SOC)

Il RTI vanta una solida esperienza nell'erogazione di servizi SOC, anche per ambienti critici della PA. Elevati livelli di efficienza ed efficacia delle Security Operations sono raggiunti tramite la specializzazione sulle tecnologie e sui vendor di cui il RTI è partner, che consente agli operatori del SOC di gestire gli incident di sicurezza con maggior precisione e rapidità. Il servizio è finalizzato al monitoraggio e alla gestione continua, adeguatamente alle dimensioni ed alla complessità del perimetro, delle minacce che insistono sulle infrastrutture e sui dispositivi della PA.

Per il Servizio "Security Operations Center" (SOC) e per tutti i Servizi ad esso connessi o relazionabili, il RTI garantisce alle PA contraenti pieno supporto lungo tutto il **ciclo di vita** del servizio (*Service Lifecycle*), dalla fase iniziale di *Assessment* alla fase finale di *Decommissioning & Handover*.

Ciclo di vita del servizio SOC
Il piano di gestione del ciclo di vita del servizio proposto dal RTI e ampiamente collaudato dalle aziende raggruppande, si articola in cinque fasi principali, come di seguito illustrato:

1. **Fase di Assessment**: il fornitore provvede a raccogliere tutti gli elementi necessari per dimensionare e configurare al meglio il Servizio offerto, sulla base delle specificità tecniche e amministrative della PA contraente. A tale scopo, il Fornitore condurrà due distinte attività di Assessment:
   - *Assessment dei requisiti di missione e normativi*: sono raccolti e analizzati sia i requisiti derivanti dalla *mission* specifica della PA contraente, sia i requisiti derivanti dal quadro normativo generale e particolare in cui essa si trova ad operare. Le informazioni raccolte in questa fase contribuiscono a definire i criteri di *Incident Response* in base ai quali si dovrà, ad esempio, favorire la continuità nell'erogazione dei servizi IT coinvolti rispetto alla raccolta di evidenze forensi, o viceversa.
   - *Assessment dei requisiti tecnologici e architetturali*: sono raccolti e analizzati sia i requisiti derivanti dall'architettura generale del *landscape* IT della PA contraente (modelli di dispiegamento e modelli di servizio adottati, tipologia e capacità delle interconnessioni di rete, etc.), sia i requisiti derivanti dalle specifiche tecnologie impiegate (famiglie di sistemi operativi, tipologie di gestori di basi di dati, etc.). Le informazioni raccolte in questa fase contribuiscono a definire i metodi e le procedure più opportune per l'acquisizione degli eventi e per le attività di investigazione, contenimento e ripristino in caso di Incidente.
2. **Fase di Caratterizzazione**: il fornitore provvede a caratterizzare il Servizio SOC in funzione dei requisiti raccolti nella precedente fase di Assessment, definendo o adeguando opportunamente le policy, le procedure e i playbook di analisi e di risposta agli Incidenti per una data PA contraente, in base alle sue specificità. Questa fase prevede le seguenti sotto-fasi:
   - *Caratterizzazione organizzativa*: di concerto con il referente dell'Amministrazione contraente, i requisiti precedentemente raccolti vengono esaminati per determinare le priorità e gli obiettivi dell'Amministrazione e per confermare, ovvero adeguare, il modello di comunicazione e di cooperazione tra fornitore ed Amministrazione, unitamente a tutte le procedure da attivare in caso di Incidente sospetto o conclamato. In questa fase vengono identificate le potenziali frizioni organizzative e individuati i possibili rimedi.
   - *Caratterizzazione tecnica*: di concerto con il referente dell'Amministrazione contraente, le informazioni precedentemente acquisite vengono analizzate per determinare i metodi e le tecniche da adottare in sede di *onboarding*, nonché per definire le policy e le soglie da impiegare al fine di raggiungere il migliore equilibro tra efficacia nella *detection* e riduzione dei falsi positivi. In questa fase vengono intercettate le possibili limitazioni o incompatibilità tecniche e individuati i possibili workaround.
3. **Fase di Attivazione**: il fornitore provvede a eseguire quanto necessario per la corretta attivazione del Servizio, facendo sì che la successiva fase di piena operatività possa avviarsi nel rispetto delle esigenze e delle aspettative dell'Amministrazione contraente. La fase di Attivazione si suddivide in:
   - *Integrazione e Onboarding*: il fornitore provvede ad attivare l'interconnessione geografica tramite rete Internet e/o via rete SPC. Successivamente, con il supporto del referente dell'Amministrazione, il Fornitore procede con la fase di *onboarding* provvedendo alla configurazione delle componenti di inoltro degli eventi di sicurezza per gli apparati di sicurezza di proprietà della PA contraente, in modo da abilitare la raccolta continua degli eventi e delle informazioni di sicurezza. La fase di onboarding termina con l'applicazione delle policy e dei modelli SIEM e con la verifica e l'eventuale adeguamento delle procedure e dei playbook del SOAR, secondo quanto definito e approvato in sede di *Caratterizzazione Tecnica*.
   - *Collaudo e Accettazione*: di concerto con il referente dell'Amministrazione, il fornitore esegue il collaudo del Servizio allo scopo di confermare che sia stato configurato in accordo alle esigenze della PA e che operi secondo i livelli di performance attesi. La fase di collaudo prevede la verifica della piena raggiungibilità di tutti i nodi fisici e degli oggetti logici configurati, nonché la simulazione di un Incidente di sicurezza e della sua successiva gestione da parte di ciascun attore coinvolto, inclusi i referenti dell'Amministrazione. Eventuali eccezioni e non-conformità non sanabili in sede di collaudo saranno registrate e inserite nel documento di *User Acceptance*, unitamente al corrispondente piano di rimedio.
4. **Fase Operativa**: il fornitore assicura la quotidiana operatività del Servizio SOC secondo le buone pratiche di settore e in accordo ai dettami del Capitolato Tecnico, ai pertinenti Indicatori di Qualità e ai requisiti espressi dall'Amministrazione. La fase Operativa a sua volta si suddivide in:
   - *Event monitoring & Incident handling*: il Servizio SOC erogato dal fornitore presidia H24 l'identificazione e l'analisi degli eventi di sicurezza, assicurando il triage e la risposta agli Incidenti rilevati. In questa fase viene avviata, se prevista, un'interlocuzione d'urgenza con il referente dell'Amministrazione,

volta a confermare l'effettiva sussistenza dell'Incidente di sicurezza e a concertare il migliore corso di azione, al fine di rispettare le specifiche priorità della PA coinvolta (ad es. prediligendo la continuità del servizio IT interessato o il suo immediato ripristino rispetto alla preservazione delle evidenze forensi).

- *Incident containment & System recovery*: il personale del Servizio SOC, una volta confermato l'Incidente di sicurezza e stabilito l'opportuno corso d'azione, provvede a contenerne gli effetti (ad es. esfiltrazione dei dati, propagazione del codice malevolo, etc.) isolando, se necessario, i sistemi coinvolti. Laddove tecnicamente possibile, in assenza di vincoli di natura investigativa (preservazione delle evidenze di reato) e in accordo con l'Amministrazione, il personale del Servizio SOC provvede a supportare da remoto l'Amministrazione nel ripristinare l'integrità e la funzionalità dei sistemi colpiti, mediante l'eradicazione del codice malevolo e l'applicazione di misure di protezione temporanee (ad es. chiusura di determinate porte di comunicazione, blocco in scrittura su specifiche aree di sistema, disabilitazione di demoni/servizi di sistema non essenziali, etc.), ovvero mediante la sostituzione di un *workload* immutabile (istanze, container, etc.) ricorrendo alla corrispondente *master image*.
- *Digital forensic & Post-mortem analysis*: a valle dell'Incidente di sicurezza il personale del Servizio SOC provvede a identificare, acquisire e analizzare le evidenze forensi connesse all'Incidente di sicurezza occorso, avendo cura di preservare l'integrità della catena di custodia. Le evidenze così raccolte vengono successivamente trasmesse all'Amministrazione interessata per l'archiviazione, unitamente al *Report* sintetico e di dettaglio contenente, fra le altre informazioni, il risultato dell'analisi *Post-mortem* incluse le eventuali *Root Cause Analysis* e *Lesson Learned*, se identificate.

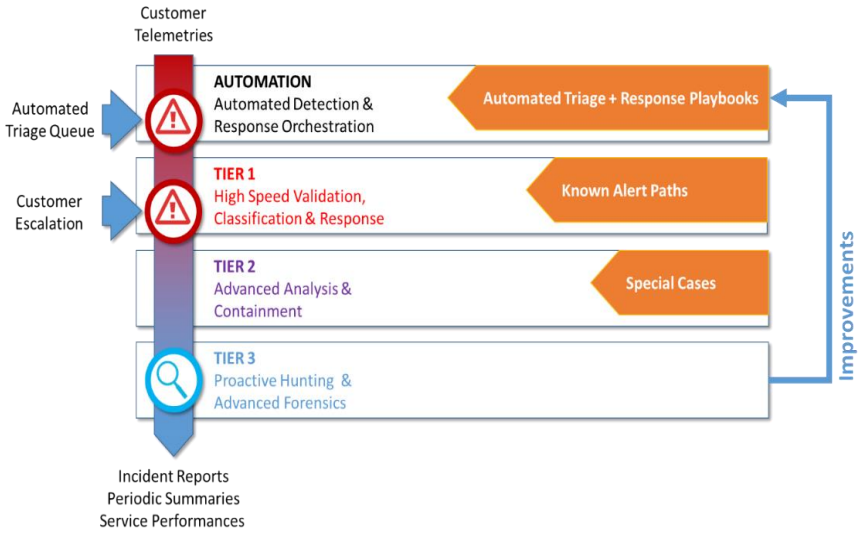

Figura 7 – Ciclo di gestione incidenti

5. **Fase di Terminazione**: al termine del contratto, il fornitore provvede a ripristinare la situazione originaria, rimuovendo tutti i componenti tecnici installati presso le sedi della PA. Del pari, si adopererà per trasferire alla medesima i registri di interesse e la conoscenza tecnica acquisita durante il periodo di erogazione del servizio, in modo da agevolare l'Amministrazione nel trasferimento del Servizio SOC ad altro gestore o presso le proprie strutture tecniche interne. Più nel dettaglio, la fase di Terminazione prevede le sotto-fasi di:

- *Decommissioning dei componenti tecnici*: salvo differente accordo con la PA, tutte gli eventuali componenti software (agent, connettori, API, etc.) e hardware (concentratori VPN, collettori di log, etc.) installati per abilitare l'erogazione del Servizio sono rimossi o ritirati dal Fornitore, il quale avrà cura di ripristinare contestualmente le condizioni originarie della rete della PA interessata.
- *Handover dei registri e della conoscenza*: tutti i registri creati in sede di attivazione del Servizio e aggiornati in itinere e tutta la conoscenza acquisita nel corso della sua erogazione saranno trasmessi all'Amministrazione in forma documentale, secondo un formato standard di comune fruizione. Il Fornitore presterà inoltre il proprio supporto all'Amministrazione affinché questa possa completare la propria transizione verso una differente gestione nel minor tempo e con la minore interruzione di servizio possibile.

Modello Operativo

Per poter conseguire il livello di efficienza necessario per assicurare continuità nel supportare i propri clienti in condizioni spesso di emergenza, il servizio SOC è organizzato su diversi livelli definiti come "tier", la cui differenziazione è legata alla capacità operativa e al grado di approfondimento e autonomia via via crescente per ogni livello.

Il processo di revisione continua delle situazioni di rischio, di approfondimento tecnico e classificazione di eventuali incidenti informatici di sicurezza e di gestione delle attività di incident response, in termini di supporto al contenimento e valutazione continua dello stato di efficacia dello stesso, viene integralmente gestito dal SOC. Questo sfrutta l'organizzazione a più livelli, le tecnologie e le best practice consolidate grazie alla continua esperienza maturata dal RTI in contesti complessi e su threat actor significativi. In particolare, il primo livello (**Tier 1**) è costituito da operatori in turnazione che si occupano principalmente del controllo e monitoraggio costante di anomalie di sicurezza o di fornire un'accoglienza specialistica di secondo livello (cfr. §4.3) in caso di richieste dell'Amministrazione. L'operatività del Tier 1 si estende alla prima classificazione di un eventuale incidente di sicurezza, all'apertura di un caso di analisi, alla gestione delle procedure di response codificate in funzione della classificazione effettuata e alla gestione dell'eventuale processo di escalation. Tale livello prevede quindi la gestione continuativa del servizio "proattivo" di monitoraggio della sicurezza del dominio dell'Amministrazione, al fine di:

- Gestire attività di triage autonome o approfondimenti richiesti dall'Amministrazione;
- Classificare eventuali minacce attive, validarne l'effettivo impatto e diffusione e avviare le procedure di escalation;
- Coordinare la prima fase di response per le attività di contenimento più idonee e misurarne l'efficacia.

Di seguito si riportano le funzioni gestite dal Tier 1 e le capacità del SOC espresse da questo livello: ✓Security Monitoring; ✓Customer Escalation Point of contact; ✓Threat Hunting; ✓Security Analysis (telemetrie); ✓Anomalies Categorization; ✓Triage (case management); ✓Preliminary Response (Incident Management di primo livello); ✓Incident Report; ✓Escalation al secondo livello.

Il secondo livello del SOC (**Tier 2**) è costituito da un team di specialisti di sicurezza senior in grado di intervenire a seguito di una richiesta di ingaggio da parte del primo livello, mettendo a fattore comune le competenze relative alle minacce e vulnerabilità al momento riscontrate. Questo team conduce attività

di analisi approfondite che necessitano di competenze tecniche avanzate in termini di conoscenza del funzionamento delle contromisure presenti nel dominio sotto monitoraggio, delle tecniche e tattiche tipicamente utilizzate dagli attaccanti per comporre la kill-chain, delle tecniche di investigazione necessarie sulle telemetrie raccolte al fine di ricostruire l'effettiva situazione in corso ossia: ✓Sistemi impattati e catena degli eventi generata dall'attacco; ✓Presenza di artefatti all'interno dei sistemi e analisi preliminare per identificare eventuali componenti malevoli (APT); ✓Root cause che ha generato la catena di eventi osservata; ✓Identificazione e coordinamento di tattiche di contenimento "specifiche" in funzione della situazione ricostruita; ✓Coordinamento stakeholder per attività di response complesse; ✓Gestione della Knowledge Base (KB) interna e avvio attività di miglioramento dei processi di classificazione e response di primo livello; ✓Escalation al terzo livello.

Di seguito si riportano le funzioni gestite dal Tier 2 e le capacità del SOC espresse da questo livello: ✓In-depth Incident Investigation (Incident Management di secondo livello); ✓Security Analysis (telemetrie, contenuto sistemi, artefatti sospetti); ✓Response coordination; ✓Incident Containement; ✓Threat Intelligence (creazione indicatori a partire dai dati esecutivi degli incidenti gestiti); ✓Incident Report.

Il terzo livello del SOC (**Tier 3**) è costituito da team ad-hoc di specialisti per i processi di incident response avanzato e per tutti i servizi a valore aggiunto che richiedano competenze e capacità come il reverse engineering di eventuali artefatti, la ricerca continua di informazioni o indicatori per la Cyber Threat Intelligence o l'esecuzione di attività di ricerca continua di vulnerabilità esposte sul perimetro dell'Amministrazione. L'intervento del Tier 3 è basato su micro-team costruiti all'occorrenza che vengono assegnati ad un task specifico tra quelli sopra elencati, e generano report di dettaglio sensibili condivisi con l'Amministrazione.

Di seguito si riportano le funzioni gestite dal Tier 3 e le capacità del SOC espresse da questo livello: ✓Advanced Security Analysis (e.g. reverse engineering, attack attribution); ✓Threat Intelligence maintenance; ✓Continuous Vulnerability Assessment services.

5.1. SOLUZIONI TECNOLOGICHE PROPOSTE PER IL SOC

Il RTI propone per il Servizio SOC una soluzione integrata che consente agli analisti di rilevare rapidamente le anomalie di sicurezza, contestualizzarle e creare le condizioni per porre rapidamente in essere le necessarie azioni di contenimento.

Nella successiva figura sono schematizzate tutte le componenti funzionali che sottendono all'erogazione dei servizi di AQ con particolare riferimento a quelle necessarie per il Servizio SOC.

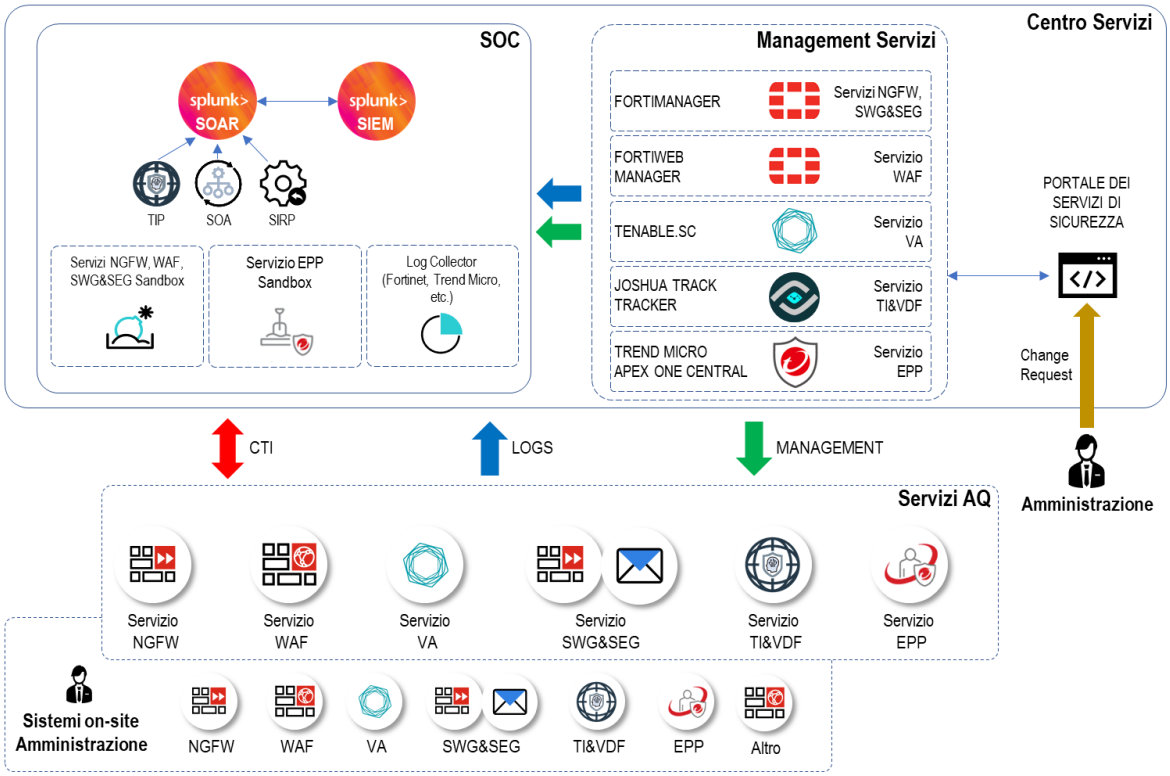

Figura 8 – Componenti funzionali del servizio SOC

La soluzione tecnologica prevista per il Servizio SOC è costituita dalle componenti SIEM e SOAR, Log Collector e le Sandbox previste in funzione del servizio erogato. Sono inoltre presenti le console di gestione per ciascuna delle tecnologie di erogazione dei servizi che interagiscono con la piattaforma SOC. Completa l'architettura il Portale dei Servizi di Sicurezza che consente alle Amministrazioni di richiedere change alle policy e modifiche alle configurazioni per i servizi proposti.

La progettazione di tutti i servizi previsti in AQ è stata effettuata in maniera sinergica ed integrata secondo una visione unitaria che è in grado di garantire la migliore postura di sicurezza dell'Amministrazione contraente. Ciascun servizio, pur ottimizzato per essere erogato anche singolarmente, esprime la massima potenzialità ed efficacia all'interno della visione integrata del proponente insieme con gli altri servizi di sicurezza. A questo riguardo si rappresenta di seguito lo schema dei flussi di interazione tra tutti i servizi dell'AQ che sono funzionali a tale visione progettuale descritti nel dettaglio nei capitoli successivi.

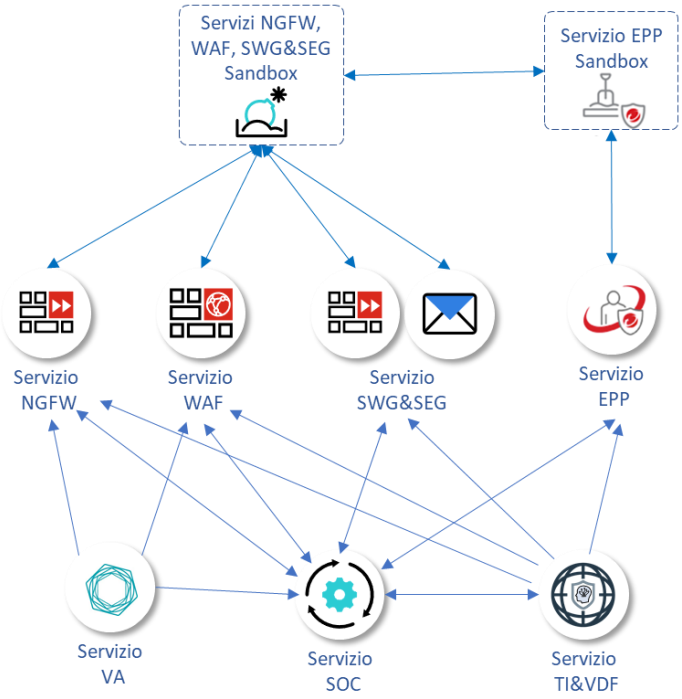

Figura 9 – Flussi di interazione

Per l'erogazione del Servizio SOC, il RTI si avvale di una piattaforma tecnologica leader di mercato: **Splunk Security Suite**. La piattaforma utilizza l'approccio "Data-to-Everything", gestendo efficacemente la raccolta di informazioni dagli asset IT della PA con il supporto di avanzati processi di intelligence, anche automatici, che consentono ai team di sicurezza di eseguire analisi statistiche, visive, comportamentali ed esplorative, identificare rapidamente un possibile incidente di sicurezza, velocizzando il processo decisionale e di individuazione della risposta più efficace, con la conseguente riduzione dei rischi per la PA.

La soluzione fornita dal RTI copre molteplici aree della Cyber Security, favorendo la collaborazione fra i vari team di sicurezza e supportando la corretta implementazione delle migliori pratiche per la protezione di infrastrutture e dispositivi. La piattaforma consente di attuare un flusso di lavoro completo, dalla raccolta dati fino all'invocazione delle azioni necessarie a contrastare le più disparate minacce, indirizzando efficacemente tutte le fasi della gestione delle informazioni e degli eventi di sicurezza.

La suite Splunk si compone di differenti elementi architetturali e servizi specializzati, volti ad ottenere un insieme completo e omogeneo di funzionalità di sicurezza integrate:

Figura 10 – Splunk DtE

Splunk Security Suite	
Splunk Enterprise	Una piattaforma di data-analytics potente e flessibile, in grado di gestire svariati scenari di analisi dei dati con finalità di sicurezza. Consente di monitorare e analizzare rapidamente i dati da qualsiasi fonte, alimentando le altre funzionalità di sicurezza.
Splunk Enterprise Security	Una soluzione di gestione delle informazioni e degli eventi di sicurezza (SIEM) che fornisce approfondimenti sui dati generati dagli endpoint e dalle tecnologie di sicurezza operanti sulla rete, nonché sulle informazioni relative a malware e vulnerabilità.
Splunk SOAR	Una piattaforma di orchestrazione, automazione e risposta agli eventi di sicurezza (SOAR) che si integra con le tecnologie di sicurezza esistenti per fornire uno strato di "tessuto connettivo" tra di esse, rendendole più intelligenti, più veloci e resilienti.
Splunk Applications	Applicazioni sviluppate da Splunk, dai suoi partner e dalla comunità per migliorare ed estendere le potenzialità della piattaforma, ad esempio l'App per la Compliance GDPR e per il MITRE ATT&CK Navigator.
Splunk Security Essentials	Un'applicazione che permette di esplorare nuovi casi d'uso e di distribuire indicatori di compromissione da Splunk Security Essentials a Splunk Enterprise e ai componenti Splunk SIEM e SOAR.
Splunk Enterprise Security Content Updates	Archivio di documentazione dettagliata sull'analisi della sicurezza, chiamato 'Analytic Stories', che supporta gli analisti nell'indagine e contrasto alle nuove minacce rilevate.

Tabella 8 – Suite Splunk

5.2. LIVELLO DI AUTOMAZIONE DEI PROCESSI DI MANAGEMENT, MODALITÀ E STRUMENTI DI CONTROLLO CENTRALIZZATO (CASE MANAGEMENT)

Il modello operativo del SOC proposto si basa sulle interazioni tra persone, tecnologie e processi, che operano tra loro secondo uno schema collaborativo ampiamente consolidato e riportato nella figura seguente, dove sono rappresentate le capacità che il SOC mette a disposizione delle PA e come queste ultime sono impiegate in funzione delle azioni, degli scambi informativi o delle necessità operative inerenti il mantenimento dell'integrità del livello di sicurezza della PA gestita. Ogni capacità è espressa integrando: ✓**strumenti di supporto** all'avanguardia per automatizzare l'operatività e normalizzare il processo di comunicazione verso le altre capacità del SOC; ✓**team di lavoro** organizzati su vari livelli (tier) formati per gestire le attività di identificazione di anomalie, validazione delle stesse e supporto alla response;✓**sistemi di comunicazione** adeguati a velocizzare le operazioni di scambio e supportare la creazione di una KB interna.

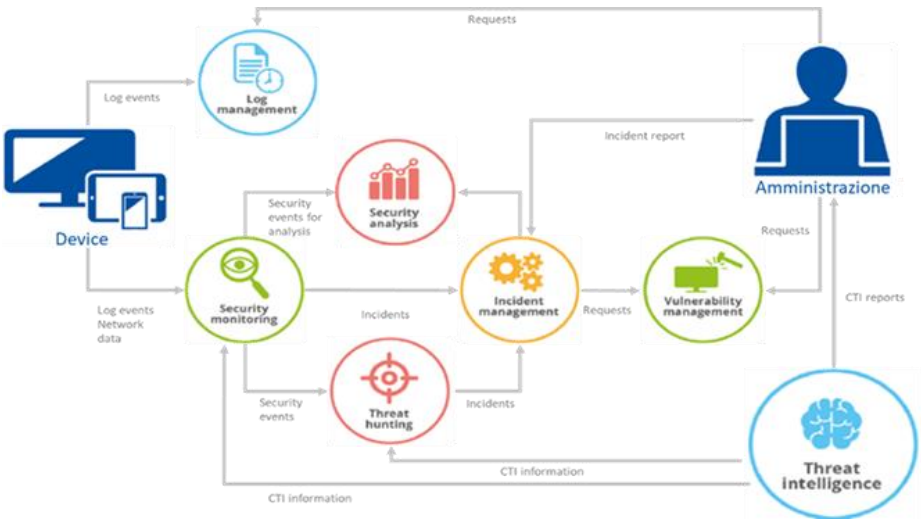

Figura 11 – Capacità del SOC

All'interno della suite Splunk le funzionalità di orchestrazione, automazione e risposta sono fornite dal componente **SOAR**, che integrano e potenziano le capability del SIEM della suite. Il SOAR supporta una vasta gamma di funzioni di sicurezza, tra cui la gestione degli eventi e dei casi, l'intelligence integrata per l'identificazione delle minacce e gli strumenti di collaborazione e di reporting. Permette inoltre agli analisti di sicurezza di lavorare in modo più efficace ed efficiente, automatizzando le attività ripetitive e velocizzando la gestione degli incidenti grazie al supporto all'automazione delle fasi di rilevamento, di indagine e di risposta alle minacce. Infine, consente di incrementare la produttività e di rafforzare al contempo il livello di difesa connettendo e coordinando flussi di lavoro complessi attraverso i team di sicurezza e gli strumenti da essi impiegati.

In particolare, Splunk SOAR consente di: ✓automatizzare sia il triage degli eventi sia le attività più ripetitive, in modo da permettere agli operatori SOC di focalizzarsi sulle attività di analisi che traggono maggiore valore dall'interazione umana; ✓investigare e rispondere agli incidenti di sicurezza con tempistiche di rilevamento (MTTD) e di risposta (MTTR) misurabili nell'ordine dei secondi o dei minuti invece che in ore, grazie all'uso di playbook che automatizzano le attività di sicurezza su una moltitudine di scenari. Il componente proposto orchestra i flussi di lavoro e la risposta agli incidenti integrandosi con altri strumenti di sicurezza; infatti supporta nativamente oltre 350 strumenti di terze parti e oltre 2.400 azioni automatizzate. Ciò non solo massimizza la velocità di investigazione e di risposta ma sblocca anche l'efficacia potenziale degli altri strumenti di sicurezza impiegati nel SOC.

Figura 12 – Dashboard Splunk SOAR

Automazione ed integrazione dei processi operativi e di management

Il RTI pone, alla base dell'efficacia del proprio modello operativo, l'automazione dei processi di management come elemento distintivo della soluzione proposta. Infatti, Splunk SOAR consente di attivare/gestire l'apertura manuale/automatica di casi di incidente e avviare il processo di orchestrazione e automazione della response mediante l'impiego di playbook specializzati, con sequenze di azioni di verifica aggiuntiva, di contenimento o di comunicazione programmate, in grado di rispondere in maniera adeguata all'incidente di sicurezza.

In caso di apertura di un case sulla piattaforma SOAR in maniera automatica/proattiva sarà generato e gestito il ticket sul sistema di trouble ticketing del RTI.

La soluzione SOAR proposta consente agli analisti di sfruttare l'automazione per accelerare la gestione degli incidenti e intraprendere azioni difensive in contemporanea su più sistemi di sicurezza, riducendo al minimo il cambio di contesto richiesto agli operatori, diminuendo l'eccessivo numero di avvisi e velocizzando la risposta agli incidenti.

Il livello di maturità della soluzione consente di gestire il processo di contestualizzazione e fusione con la threat intelligence direttamente in fase di acquisizione delle informazioni grezze, dettagliando tutta la base di conoscenza e non solo gli eventi sospetti. Questo approccio esalta la capacità di automazione delle attività di gestione e di organizzazione della risposta, in quanto i modelli di analisi possono beneficiare dell'integrazione con i dati aggiuntivi incrementando la capacità di interpretazione della situazione e di identificazione di comportamenti anomali anche complessi.

Il Servizio SOC dispone, pertanto, di capacità di contestualizzazione e di procedure tipiche di un SOAR, fondendole con le funzionalità di approfondimento e identificazione delle anomalie, consentendo una gestione dei playbook di intervento più efficace e indirizzata per: ✓gestire un processo "misto",

orchestrando procedure di contenimento iniziali in funzione del triage effettuato, insieme alla richiesta di azioni di intervento da parte degli operatori per ulteriori accertamenti o validazione dello scenario ricostruito; ✓automatizzare azioni rapide di primo contenimento indirizzate allo specifico scenario di attacco sintetizzato (ad es. sospendere utenze, mettere in quarantena endpoint, bloccare zone di rete); ✓automatizzare eventuali azioni di approfondimento su sistemi terzi prima di richiedere l'intervento dell'operatore (ad es. screenshot del contenuto associato ad una URL sospetta, sottomissione hash a Knowledge Base relativi ad artefatti malevoli, esecuzione triage su sistema EDR connesso, etc.); ✓tracciare in ogni momento lo stato di gestione di un incidente e tutte le entità "osservate" al fine di avere una visione completa di quanto accaduto, utile per le successive esecuzioni degli stessi playbook.

Modalità e strumenti di controllo centralizzati

Per facilitare la gestione delle attività di analisi e risposta agli incidenti, gli operatori possono contare su funzionalità di controllo centralizzato finalizzate alla gestione del processo di incident management. La piattaforma è in grado di aprire e gestire automaticamente i casi di analisi le cui informazioni provenienti dal triage automatico mappano i modelli predefiniti (playbook). L'analista può comunque prendere in carico il caso, assegnarlo ad un altro analista e seguirne l'evoluzione nel tempo. Un caso può essere aperto anche manualmente partendo da altri componenti di visualizzazione (dashboard, drill-down, grafico), utilizzando un template predefinito.

Un caso contiene un insieme di informazioni completo e coerente, quali, a titolo di esempio: ✓Il livello di gravità assegnatogli; ✓Il livello di triage specifico; ✓Il titolo breve; ✓Una serie di tag utili per la classificazione; ✓La descrizione dettagliata; ✓La data di apertura; ✓L'assegnatario; ✓L'elenco delle attività in corso e l'assegnatario di ciascuna attività; ✓L'elenco delle attività che devono essere eseguite per la risoluzione; ✓Un insieme di metriche misurate in funzione della situazione.

Per la fase di Incident Response è disponibile una serie di playbook già "strutturati" per ottimizzare l'efficacia delle soluzioni di sicurezza specificate in questa proposta, garantendo l'attivazione automatizzata delle funzioni di contenimento previste dalle varie piattaforme. Inoltre, è anche disponibile un set di playbook relativi alle principali tecnologie di mercato che possono essere attivati in funzione dello scenario di integrazione specifico di ciascuna PA, per incrementare sensibilmente la capacità di risposta del servizio. Infine, sono previsti una serie di playbook mirati a garantire la distribuzione delle informazioni operative consentendo l'allineamento della base di conoscenza sulle piattaforme interessate.

Nell'ambito dei processi a supporto della gestione degli incidenti, le attività possono essere assegnate a specifici analisti SOC e viene mantenuta una bozza delle attività svolte con la possibilità di allegare evidenze o bookmark di ricerche precedenti gestite su altri componenti grafici (dashboard, drill-down e grafici).

Per supportare al meglio l'automazione durante la fase di analisi, è possibile definire modelli di casi in grado di migliorare la produttività in base alla classificazione iniziale di un incidente. I modelli possono essere correlati a categorie di incidenti di sicurezza o a situazioni rischiose che possono essere considerate importanti per il dominio specifico. All'interno del modello solitamente sono definiti: ✓una serie di tag per la classificazione; ✓prefissi da utilizzare per titoli e descrizioni; ✓un elenco personalizzabile di attività da gestire; ✓un insieme di metriche che saranno valutate dagli analisti durante l'attività.

Per ogni caso viene gestito e visualizzato un log di tracciabilità che elenca tutte le azioni svolte dagli utenti e le attività ad esso correlate, riportando anche la durata di ogni operazione effettuata.

La piattaforma, infine, mostra una dashboard riepilogativa sullo stato dei casi gestiti (numeri e tempi di risoluzione).

5.3. CARATTERISTICHE TECNICHE DELLA SOLUZIONE SOFTWARE SIEM

L'elemento che distingue maggiormente la piattaforma Splunk, rispetto alle altre soluzioni SIEM, è la sua natura di piattaforma espressamente concepita per la data-analytics. Basandosi su un motore per l'analisi dei dati robusto e performante, il componente SIEM di Splunk consente di acquisire dati con volumi e velocità non raggiungibili dalle altre soluzioni concorrenti, nonché di effettuare attività di analisi e correlazione sia sui dati acquisiti in tempo reale sia sui dati storicizzati, anche a lungo termine. La soluzione Splunk, caratterizzandosi come SIEM 'analytics-driven', è nativamente predisposta per l'applicazione di metodi di machine learning, data science e statistica avanzata: ciò pone Splunk nelle condizioni di effettuare analisi predittive volte ad identificare in tempo reale l'occorrenza di eventi avversi. Nella seguente tabella è possibile trovare una comparazione delle caratteristiche della soluzione SIEM Splunk rispetto alle soluzioni SIEM tradizionali (non analytics-driven), alle soluzioni Open Source e ai nuovi competitor sul mercato. Il valore in colonna 'DIY' (Do It Yourself) indica una funzionalità implementabile solo tramite la scrittura e la successiva integrazione di codice ad-hoc.

	Splunk ES	SIEM Tradizionali	SIEM Open Source	Nuovi Competitor
1. Raccolta di log ed eventi	Sì	Sì	Sì	Sì
2. Applicazione in tempo reale delle regole di correlazione	Sì	Sì	DIY	Sì
3. Applicazione in tempo reale di metodi di analisi avanzata e di tecniche di *machine-learning*	Sì	Limitato	DIY	Sì
4. Analisi di dati storicizzati a lungo termine, anche con tecniche di *machine-learning*	Sì	Limitato	DIY	Limitato
5. Conservazione degli eventi a lungo termine	Sì	Limitato	Sì	Limitato
6. Ricerca e reportistica su dati normalizzati	Sì	Sì	Sì	Sì
7. Ricerca e reportistica su dati grezzi ('*raw data*')	Sì	Difficile	Sì	Difficile
8. Ingestione di dati di contesto per l'esecuzione di correlazioni e di analisi addizionali	Sì	Limitato	Sì	Limitato
9 Gestione di scenari non strettamente legati alla sicurezza	Sì	No	DIY	No

Tabella 9 – Confronto funzionalità SIEM

Splunk SIEM consente agli operatori del servizio SOC di effettuare un monitoraggio evoluto basato sulla capacità di aggregare dati significativi, provenienti da molteplici fonti, stabilendo in tempo reale analisi e correlazioni finalizzate a individuare comportamenti anomali, segnali critici e a generare allarmi, rispondendo alle esigenze di incident response, compliance e analisi forensi.
Il SIEM raccoglie i log e centralizza l'analisi degli eventi generati da applicazioni e sistemi in rete. Grazie alle funzionalità di machine learning, le attività di correlazione e monitoraggio sono potenziate, abilitando una security intelligence evoluta.
La soluzione proposta dal RTI supporta gli operatori del SOC nell'erogazione del servizio lungo le seguenti fasi:

1. COLLEZIONE. Raccolta dei log di sicurezza basilari e di altri eventi dall'ambiente informatico gestito. La raccolta dei log e degli eventi si esplica, al minimo, nei seguenti ambiti: ✓**Traffico di rete**, dai log di traffico generati da firewall *Fortinet, Cisco, Palo Alto, CheckPoint* e di altri vendor; ✓**Attività sugli endpoint**, inclusi gli eventi Windows, i system log Linux, i log auditd Linux, i system log MacOS; ✓**Sistemi di autenticazione**, per eventi Active Directory, log LDAP, eventi di Identity and Access Management (IAM) basati su cloud, eventi da autenticazione locale (NTLM, PAM, etc.); ✓**Traffico web**, inclusi i log generati da NGFW, WAF, SWG e Proxy Server prodotti da vendor quali *Fortinet, Cisco, Palo Alto, Websense, Bluecoat* e altri.
2. NORMALIZZAZIONE. Applicazione di una tassonomia di sicurezza standard e integrazione con ulteriori dati relativi ad asset e identità. Questa fase è volta ad assicurare che i dati raccolti nella precedente fase di Collezione siano conformi ad una tassonomia di sicurezza standard, ovvero che dati comuni quali, ad es., indirizzi IP, porte TCP, nome utente o nome macchina siano normalizzati e rappresentati attraverso una nomenclatura standard, indipendentemente dal dispositivo che ha generato o registrato l'evento. L'attività di normalizzazione migliora significativamente l'efficacia della correlazione specie con l'impiego di sorgenti diverse. La successiva integrazione con dati relativi ad asset e identità può avvenire interfacciando la piattaforma con sistemi di gestione degli asset IT (sistemi, reti, dispositivi e applicazioni) e con sistemi di gestione delle identità quali Microsoft Active Directory, OpenLDAP e altri sistemi IAM/SSO.
3. ESPANSIONE. Raccolta di ulteriori dati quali eventi di dettaglio sugli endpoint o metadati di rete, al fine di abilitare il rilevamento avanzato degli attacchi. Dati provenienti da fonti quali query DNS e ulteriori dati generati dagli endpoint ampliano le capacità di detection, consentendo un'efficace ricerca delle minacce eventualmente residenti all'interno della rete. Le fonti di dati impiegate in questo stadio includono almeno: ✓**La rete**, con metadati legati agli specifici protocolli di rete utilizzati, forniti da componenti specifici come *Splunk Stream* e *Bro*, accanto ai dati provenienti da query DNS e lease DHCP; ✓**Gli endpoint**, con la cattura dettagliata di attività quali creazione di processi, modifiche a file e a valori di registro, apertura di socket di rete, etc., consentita da tool specifici quali *Microsoft Sysmon*, *Osquery* e *Carbon Black Defense*.
4. ARRICCHIMENTO – Integrazione degli eventi e delle informazioni di sicurezza con fonti di Cyber Security Intelligence per una migliore comprensione del contesto e del potenziale impatto di un evento. In aggiunta all'espansione dei dati con elementi raccolti dalla rete e dagli endpoint, la piattaforma Splunk consente l'arricchimento dei dati con informazioni di intelligence provenienti da fonti interne ed esterne. Elementi di conoscenza contestuale e investigativa, unitamente a feed di threat-intelligence e fonti di open-source intelligence (OSINT), consentono di estrarre maggiore valore dai dati raccolti, in modo da consentire una più rapida e accurata identificazione degli eventi di sicurezza significativi e dei potenziali incidenti.
5. AUTOMAZIONE E ORCHESTRAZIONE – Conferimento di una capacità operativa di reazione agli incidenti di sicurezza coerente e ripetibile. Grazie al componente SOAR è possibile incrementare le capacità operative del SOC, consentendo una risposta agli incidenti di sicurezza più tempestiva e sistematica, un processo di investigazione più rapido, nonché una significativa riduzione dei danni conseguenti agli attacchi. Le fonti di dati impiegate in questo stadio includono eventi ad elevata accuratezza generati dalla piattaforma Splunk Enterprise.
6. RILEVAMENTO AVANZATO – Applicazione di meccanismi di rilevamento sofisticati, inclusi quelli basati sull'apprendimento automatico. Attraverso l'applicazione di metodi di **machine learning, data science e statistica avanzata** applicati al comportamento di utenti, dispositivi e applicazioni, viene abilitata la capacità di individuare entità avversarie, minacce sconosciute e agenti malevoli interni anche con tracce di attività molto ridotte. Le fonti di dati impiegate sono le medesime descritte nel precedente punto 3.

Figura 13 – Dashboard Splunk

Gli strumenti messi a disposizione dalla piattaforma Splunk presentano, inoltre, un'**interfaccia chiara ed intuitiva** che migliora l'interazione da parte degli analisti, nella rappresentazione degli esiti delle ricerche e delle correlazioni che avvengono analizzando set informativi anche non omogenei provenienti da più fonti di dati. Le correlazioni possono quindi riguardare eventi provenienti da qualsiasi dominio di sicurezza (accesso, identità, endpoint, rete), liste di asset, liste di identità, threat intelligence e altri dati nella piattaforma. I dataset risultanti possono essere ulteriormente trattati con un potente linguaggio di elaborazione ed attivare azioni in risposta adattativa a eventi che corrispondono alle condizioni di ricerca. Essendo la ricerca una delle attività che maggiormente caratterizza l'operatività degli analisti, la piattaforma mette a disposizione, oltre ad un nutrito numero di regole esistenti e template a supporto, anche delle procedure guidate grazie alle quali la creazione di regole viene resa semplice ed immediata.
Il SIEM analizza i registri raccolti per evidenziare eventi o comportamenti di interesse consentendo, ad esempio, di rilevare un accesso amministrativo al di fuori del normale orario di lavoro, quindi informazioni sull'host, sull'ID e altro ancora. Le informazioni contestuali raccolte rendono i **report estremamente più dettagliati** e permettono di ottimizzare i flussi di lavoro finalizzati alla risoluzione degli incidenti.

5.4. PROPOSTE INNOVATIVE PER IL CONTROLLO ED IL MIGLIORAMENTO CONTINUO DELLA QUALITÀ PERCEPITA DEL SERVIZIO.

Il RTI propone un servizio SOC basato su standard e best practice nazionali ed internazionali, quali SANS, NIST 800-61, CIS, MITRE ATT&CK, ispirato ai quattro "classici" stadi Predict-Prevent-Detect-Respond ed estendendone i contenuti ed i concetti ad una visione più ampia. Il principio che ispira il servizio è quello di far evolvere i modelli di gestione standard dei SOC, compenetrando tematiche tradizionali con il nuovo paradigma del rischio cyber, che prevede la gestione di minacce di tipo asimmetrico in cui, a prescindere dalla robustezza dei meccanismi di difesa adottati, permane sempre il rischio che un attacco abbia successo.

Il Servizio SOC nella sua interezza adotta un approccio olistico e focalizza l'attenzione costante sulle attività di governo, prevenzione e reazione tempestiva, anche e soprattutto nell'ottica del miglioramento continuo. A tal proposito, la soluzione proposta attraverso il modulo Splunk Dashboard Studio mette a disposizione della PA apposite viste integrate, sia sull'andamento generale dei servizi e sul loro funzionamento, sia sulla continua e reale erogazione a valore di questi. La proposizione, nello specifico, si concretizza in un **cruscotto unificato**, orientato ad illustrare lo stato della sicurezza dell'Amministrazione comparato in tempo reale con tutte le informazioni ricevute dal campo. In questo modo il Referente Tecnico della PA dispone di informazioni contestualizzate, sintetiche e di dettaglio, attraverso le quali poter avere contezza direttamente di quanto sta accadendo e dell'efficacia delle azioni intraprese.

Figura 14 – Cruscotto unificato

Al fine di alimentare il processo di **controllo e di miglioramento continuo della Qualità del Servizio**, con particolare riferimento alla qualità percepita dai soggetti fruitori, il sotto-processo di interazione e comunicazione con l'utilizzatore opererà in modalità '**closed-loop**', raccogliendo costantemente **feedback** a valle di una serie di interazioni ricorrenti appositamente selezionate. Il meccanismo proposto, atto a misurare e a incrementare il livello di **customer-satisfaction**, rappresenta una **innovazione di processo** ampiamente collaudata in diversi settori consumer (e-Commerce, e-Banking, servizi di Streaming multimediale, etc.) e qui applicata, per la prima volta, all'erogazione di servizi tecnici rivolti al mondo delle Pubbliche Amministrazioni.

La raccolta dei feedback potrà avvenire immediatamente a valle dell'interazione con il referente dell'Amministrazione o in qualsiasi momento successivo, eventualmente anche dopo la chiusura dell'incidente. Il feedback raccolto sarà di tipo quali-quantitativo, in modo da poter sia misurare il grado di soddisfazione generale per ciascuna categoria di interazione (o di deliverable) consumata, sia identificare in maniera circoscritta le specifiche aree di miglioramento.

Il modulo di feedback, concepito per garantire tanto l'intuitività e la rapidità della compilazione quanto la completezza delle informazioni acquisibili, sarà strutturato come di seguito:

1. **Indicatore generale di soddisfazione**, selezionabile in una scala da *1* a *5*, dove *1* rappresenta un elevato grado di insoddisfazione e *5* un elevato grado di soddisfazione;
2. **Elenco chiuso di voci selezionabili**, specifiche per ciascuna tipologia di interazione o di deliverable, cui attribuire una delle possibili valutazioni fra *Inferiore alle attese*, *Pari alle attese* o *Superiore alle attese*;
3. **Campo a testo libero**, volto alla raccolta degli eventuali suggerimenti per il perfezionamento dei moduli, delle procedure e dei processi, ovvero per la raccolta di eventuali encomi mirata a identificare le possibili aree di eccellenza da assumere a modello per il miglioramento dei servizi esistenti e per lo sviluppo di nuovi servizi.

Per agevolare la raccolta del feedback, al termine di ciascuna interazione contemplata dal processo di controllo e di miglioramento continuo, il referente dell'Amministrazione riceverà un messaggio di posta elettronica contenente il collegamento ipertestuale al form, specifico per l'Incidente in oggetto e per la tipologia di interazione (o di deliverable) oggetto di valutazione, unitamente alle informazioni e alle istruzioni necessarie per la corretta compilazione del modulo di feedback.

Nello specifico ambito del Servizio SOC, il RTI ha individuato in particolare tre aree di controllo e miglioramento, corrispondenti alle seguenti fasi e/o deliverable del Servizio:

a) Riduzione delle casistiche che richiedano, o comunque inneschino, un contatto con il referente dell'Amministrazione. Poiché non è infrequente che un sospetto Incidente di sicurezza possa occorrere anche al di fuori del comune orario di ufficio, è di fondamentale importanza che il contatto con il referente dell'Amministrazione avvenga solo quando effettivamente necessario. Ciò include non soltanto i possibili falsi positivi ma anche tutte quelle situazioni di deficit informativo, sia esso di natura procedurale o di natura circostanziale. In questa fase, il processo di controllo e di miglioramento continuo acquisirà i necessari input da parte del referente dell'Amministrazione e con questi alimenterà gli strumenti a disposizione degli analisti SOC.
b) Chiarezza e completezza della comunicazione in fase di primo contatto con il referente dell'Amministrazione all'atto dell'apertura dell'Incidente. Affinché il referente dell'Amministrazione possa acquisire tutte e sole le informazioni effettivamente rilevanti per supportare l'attività del SOC ovvero per intervenire in prima persona laddove opportuno, risulta di primaria importanza la definizione di un protocollo di comunicazione che consenta di veicolare, specie in sede di primo contatto, un set di informazioni il più possibile chiaro, completo e corretto. In questa fase, il processo di controllo e di miglioramento continuo acquisirà i necessari input da parte del referente dell'Amministrazione (ad es., possibili lacune nelle informazioni fornite, eventuale eccesso di informazioni non rilevanti, utilizzo di un gergalismo tecnico non comune ovvero eccessivo, etc.) che alimenterà gli strumenti a disposizione degli analisti SOC, con particolare riferimento alla Procedura di Comunicazione seguita nello specifico contesto e a ogni altra procedura attinente la comunicazione con gli stakeholder interni o esterni al RTI.

c) Fruibilità dei deliverable trasmessi al referente dell'Amministrazione, all'atto della chiusura dell'Incidente. Poiché i deliverable consegnati alle Amministrazioni contraenti possono essere destinati ad un'audience diversificata, comprendente anche stakeholder privi di adeguata preparazione tecnica, risulta fondamentale trovare un giusto equilibrio fra esaustività e rigore tecnico da un lato, e piena comprensibilità della reportistica da parte di figure non tecniche dall'altro. In questa fase, il processo di controllo e di miglioramento continuo acquisirà i necessari input da parte del referente dell'Amministrazione (ad es. utilizzo eccessivo di gergalismo tecnico, struttura della reportistica percepita come dispersiva, scarsa chiarezza nell'esposizione di Root Cause e Lesson Learned, eventuali indicazioni di Remediation troppo vaghe o scarsamente applicabili, etc.) e con questi alimenterà gli strumenti a disposizione degli analisti SOC, con particolare riferimento ai Template e alle Linee Guida per la redazione della Reportistica e ad ogni altro modello documentale attinente la trasmissione di informazioni agli stakeholder interni o esterni al RTI.

Infine, il servizio SOC proposto, anche attraverso consolidate **funzionalità di intelligenza artificiale e machine learning**, non solo è in grado di comprendere i fenomeni in accadimento, ma soprattutto fornisce comparazioni e suggerimenti in ottica di "**decision support system**", grazie a specifiche capacità di **predictive analytics**, fondamentali nell'ottica di prevenzione di eventi o incidenti.

6. PROPOSTA PROGETTUALE PER IL SERVIZIO "NEXT GENERATION FIREWALL"

Il servizio "Next Generation Firewall", proposto dal RTI, finalizzato a garantire la protezione di sistemi e rete da minacce esterne, viene fornito attraverso appliance **FortiGate** (hardware appliance o virtual appliance on premise) di **Fortinet**, un'avanzata tecnologia firewall con evoluti servizi di sicurezza multi-minaccia, erogati attraverso un'unica piattaforma integrata che consente di contrastare efficacemente attacchi e minacce informatiche, grazie anche alla semplicità di gestione e alla flessibilità di inserimento in una vasta gamma di scenari di implementazione.
La gestione del servizio viene effettuata attraverso il sistema di management centralizzato costituito dalle componenti **FortiManager** e **FortiAnalyzer**, attraverso VPN create su connettività INTERNET o SPC e terminate, lato Centro Servizi, sui concentratori attestati sull'infrastruttura di management del servizio. Il RTI vanta una consolidata partnership con il vendor ed ha una vasta e profonda esperienza nell'erogazione di servizi NGFW.
L'infrastruttura di erogazione del servizio di Next Generation Firewall si avvale delle componenti di seguito descritte:

- **Piattaforma di Gestione NGFW (FortiManager) –** Piattaforma centralizzata multitenant instanziata presso il Centro Servizi del RTI, utilizzata per la gestione del servizio NGFW. Consente la separazione logica delle PA contraenti in domini distinti (Tenant) garantendo la segregazione completa dei dati. Il FortiManager è una singola console di management che consente di gestire dispositivi Fortinet e fornire funzionalità di update manager centralizzato per tutti gli apparati gestiti. Si riassumono di seguito le caratteristiche principali: ✓Gestione centralizzata di oggetti e policy; ✓Capacità evolute di tracciamento delle revisioni; ✓Comparazione delle configurazioni e auditing delle attività effettuate dagli amministratori; ✓Gestione dei Workflows per una migliore implementazione dell'utilizzo multiutenza; ✓Gestione Centralizzata di SD-WAN, Reti Wireless e VPN; ✓Automazione: Gestione di templates and scripts per il provisioning di nuovi dispositivi o modifica degli esistenti; ✓API JSON o XML per l'interazione con sistemi di orchestrazione di terze parti; ✓Multitenancy e RBAC per una precisa definizione dei ruoli degli amministratori e del loro perimetro di gestione; ✓Software upgrades e security updates centralizzati per i dispositivi gestiti.
- **Log Collector (FortiAnalyzer)** – Piattaforma centralizzata multitenant instanziata presso il Centro Servizi del RTI, utilizzata per il logging e la reportistica del servizio NGFW. Il FortiAnalyzer è uno strumento che integra funzionalità di raccolta di log, analisi e reporting per tutti i dispositivi che compongono la Fortinet Security Fabric; offre capacità di analisi in un'unica piattaforma centralizzata in grado di svolgere ricerche forensi, anche tramite Indicatori di Compromissione (IOC), reportistica, data mining, event handling, archiving e visualizzazione unificata di tutti i log generati dagli apparati. Si riassumono di seguito le caratteristiche principali disponibili agli operatori ed analisti: ✓**FortiView**: consente una visualizzazione interattiva ed un monitoraggio in tempo reale degli eventi di sicurezza. In figura è rappresentata la capability di Threat Mapping che consente la visione grafica di come la minaccia si sviluppa per criticità, tempo, sorgente e destinazione; ✓**NOC&SOC Dashboard**: permette di costruire dashboard personalizzate utili agli ambienti di esercizio e di monitoring per governare la disponibilità delle risorse di rete e sicurezza; ✓**Event Manager**: permette di personalizzare la gestione degli allarmi in seguito ad eventi di sicurezza singoli e la correlazione degli stessi; contribuisce a ridurre lo sforzo di mantenere efficienti le policy di sicurezza grazie alla visibilità degli eventi e ad una rapida individuazione degli attacchi e delle minacce di sicurezza; ✓**Reporting avanzato** che consente di produrre report predefiniti e definirne di personalizzati con l'utilizzo di data set e query ad hoc in linguaggio SQL.
- **FortiSandbox** – Il componente FortiSandbox permette la detonazione anche dei malware di ultima generazione, costituisce parte integrante dell'architettura Fortinet Security Fabric ed utilizza tre modalità di intelligence sulle minacce per il rilevamento e la prevenzione degli Incidenti di sicurezza. In primis, il FortiSandbox utilizza l'intelligence globale sulle minacce emergenti, raccolta in tutto il mondo tramite i ricercatori dei FortiGuard Labs; in secondo luogo, esso condivide i dati di intelligence con altri prodotti Fortinet (WAF, SWG&SEG) o di altri vendor, incrementando l'efficacia dei diversi sistemi nella protezione del patrimonio informativo dell'Amministrazione; infine, aspetto più importante, FortiSandbox applica una forma di **intelligenza artificiale** vera e propria, che include l'analisi statica e comportamentale, al fine di migliorare l'efficacia del rilevamento delle minacce **Zero-day**. L'Artificial Intelligence (AI) è applicata durante l'intero processo di sandboxing, sia tramite analisi statica sia tramite analisi dinamica ad elevata interazione su molteplici sistemi operativi in parallelo. Le caratteristiche principali di un'analisi in Sandbox includono: ✓Motore Antimalware dinamico e aggiornamenti effettuati dai FortiGuard Labs, a cui può inviare query in tempo reale, permettendo così di rilevare in modo veloce minacce esistenti ed emergenti.

Figura 15 – Dashboard FortiManager e FortiAnalyzer

✓Emulazione di Codice: esegue in tempo reale una ispezione di tipo "lightweight sanboxing", con cui si riesce ad identificare tipologie di malware che utilizzano tecniche di evasione e/o si attivano solo in presenza di versioni software specifiche. ✓Ambiente virtuale completo (detonazione): fornisce un ambiente isolato per analizzare codice sospetto o ad alto rischio, permettendo di esplorare e verificare l'intero ciclo di vita della minaccia. ✓Visibilità avanzata: fornisce un quadro globale in una vasta gamma di reti, sistemi e attività di file classificati per livello di rischio, per migliorare la velocità di risposta agli incidenti. ✓Analisi Manuale: consente agli analisti di sottomettere manualmente campioni di malware per effettuare sandboxing virtuale senza la necessità di avere un dispositivo separato.

- **Appliance FortiGate Next Generation Firewall -** Gli apparati Next Generation Firewall permettono la visibilità completa del traffico attraverso la gestione di indirizzi IP, utenti e dispositivi con la possibilità di creare policy di sicurezza con una combinazione di questi fattori. L'ispezione del livello applicativo (Application Control feature), permette una accurata identificazione delle applicazioni che generano traffico all'interno della rete senza comprometterne le performance. Una volta individuato il traffico applicativo, è possibile controllare le applicazioni, bloccare quelle indesiderate, limitare e garantire la relativa banda (Traffic Shaping feature), attivare i profili di protezione antivirus/antimalware, IPS, DLP e le altre verifiche di sicurezza dettagliate precedentemente.

Nella tabella seguente si riportano le appliance proposte dal RTI per le diverse fasce:

Fasce	Fortinet appliance
Fascia 1: fino a 250 Mbps	FortiGate-40F
Fascia 2: fino a 2 Gbps	FortiGate-100F
Fascia 3: fino a 4 Gbps	FortiGate-400E
Fascia 4: fino a 7 Gbps	FortiGate-600E
Fascia 5: fino a 15 Gbps	FortiGate-2600F
Fascia 6: > 15 Gbps	FortiGate-3400E

Tabella 10 – Servizio Next Generation Firewall – Appliance on-premise

La soluzione proposta dal RTI garantisce: ✓funzionalità di firewalling avanzate (es. policy enforcement, statefull inspection, packet filtering, NAT, VPN client-to-site e site-to-site); ✓rilevamento e prevenzione delle intrusioni (IDS, IPS); ✓controllo delle applicazioni; ✓ispezione approfondita del traffico di rete con analisi delle intestazioni e del contenuto di ogni pacchetto; ✓visibilità del traffico crittografato con protezione da relative minacce tramite analisi del traffico HTTPS e altro traffico TLS/ SSL crittografato; ✓protezione e prevenzione delle vulnerabilità conosciute e virus (anti-malware, anti-spam e anti-botnet inspection); ✓QoS bandwith management; ✓trasmissione di eventi e log alla funzionalità di SIEM; ✓produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report).

Le scelte architetturali definite per l'implementazione, la definizione delle misure e delle regole di protezione e le modalità operative di gestione del servizio stesso derivano da una precisa strategia progettuale che consente al servizio di operare con la massima efficacia sia come singolo servizio sia, come meglio specificato nel seguito del presente capitolo, mediante l'**interazione in forte sinergia con gli altri servizi** della fornitura.

6.1. CARATTERISTICHE TECNOLOGICHE E PRESTAZIONALI MIGLIORATIVE

La soluzione tecnologica adottata dal RTI, oltre a garantire la disponibilità di tutti i requisiti minimi di Capitolato, si caratterizza per una serie di aspetti migliorativi che la pongono all'avanguardia nell'erogazione del servizio oggetto del presente paragrafo. In particolare:

- Funzionalità di firewalling avanzate con supporto dell'alta disponibilità, routing avanzato, SDWAN, proxy esplicito, bilanciamento dei server, ispezione di traffico crittografato dei protocolli SMTPS, FTPS, POP3S, IMAPS etc., DLP, gestione del traffico IPv6, DoS Policy, Traffic Shaping;
- Nell'ambito della funzionalità IPS è possibile creare **signature personalizzate** ed è previsto il **software bypass** in caso di fault del suo motore. L'aggiornamento del servizio è continuo e garantito dai laboratori FortiGuard, centro di intelligence Fortinet;
- La funzionalità di controllo delle applicazioni (Application Control) consente di ottimizzare l'utilizzo della banda di rete fornendo **priorità alle applicazioni più critiche** ed il controllo è organizzato in categorie dinamiche, gestite e aggiornate costantemente;
- L'ispezione del traffico di rete garantisce l'analisi sia dell'header (intestazione) sia del payload (contenuto) di ogni pacchetto e può essere effettuata in due modalità: **Flow mode** per un'analisi in tempo reale "packet by packet" e **Proxy mode** per un'analisi di tipo "Store and Forward".
- Adozione del modello di difesa "**Kill chain**" mediante la combinazione **in tempo reale** di servizi di sicurezza che includono anche il **DNS e Web Filtering**.
- **Granularità delle policy legate al QoS**, mediante traffic shaping che permette di applicare politiche anche in base all'applicazione o alle categorie di URL Filtering.
- Invio dei log sia in formato proprietario per il log collector di Fortinet (FortiAnalyzer del Centro Servizi) sia in formato standard syslog con la possibilità di inoltro **fino a 4 log collector/SIEM** diversi.
- Funzionalità di ricerche forensi e IoC, data mining, event handling, archiving, dashboard NOC/SOC personalizzabili.

Con riferimento alle performance, si evidenzia che tutti gli apparati FortiGate, sfruttando le potenzialità offerte dal sistema operativo proprietario FortiOS e la potenza dei processori ASIC proprietari, sono in grado di elaborare in hardware le principali funzionalità di network security e ispezione dei contenuti garantendo elevate prestazioni ed affidabilità. In tabella si evidenzia il miglioramento delle performance in termini di throughput rispetto ai requisiti minimi.

Fasce	NGFW Throughput migliorativi
Fascia 1: fino a 250 Mbps	800 Mbps **(+220%)**
Fascia 2: fino a 2 Gbps	2 Gbps
Fascia 3: fino a 4 Gbps	6 Gbps (**+50%**)

Fascia 4: fino a 7 Gbps	9,5 Gbps (+**36%**)
Fascia 5: fino a 15 Gbps	19 Gbps (+**27%**)
Fascia 6: > 15 Gbps	34 Gbps (+**127%**)

Tabella 11 - Throughput migliorativi per il servizio NGFW

6.2. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il servizio NGFW viene erogato dal Centro Servizi del RTI. Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**) conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT** (**SGS-IT**) conforme allo standard ISO/IEC 20000-1 e dall'implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

Organizzazione del servizio

L'organizzazione del servizio NGFW si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- *acquisizione* del know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione, e delle relative modalità operative, linee guida e metodologie in uso presso l'Amministrazione;
- predisposizione e configurazione del servizio e delle relative piattaforme di management:
  - Il *NGFW Team* attiva il Tenant dedicato all'Amministrazione su ciascuna delle piattaforme di gestione del servizio (FortiManager e FortiAnalyzer);
  - Il *Team on-premise* esegue l'installazione delle componenti previste on-site secondo il piano condiviso con l'Amministrazione. Gli apparati NGFW saranno resi raggiungibili, presi in carico dal sistema di management e configurati da remoto. Il servizio sarà predisposto sulla base di quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano;
  - se necessario, il *Team on-premise* ed il *NGFW Team* gestiscono il processo di migrazione secondo quanto stabilito nel piano di migrazione.

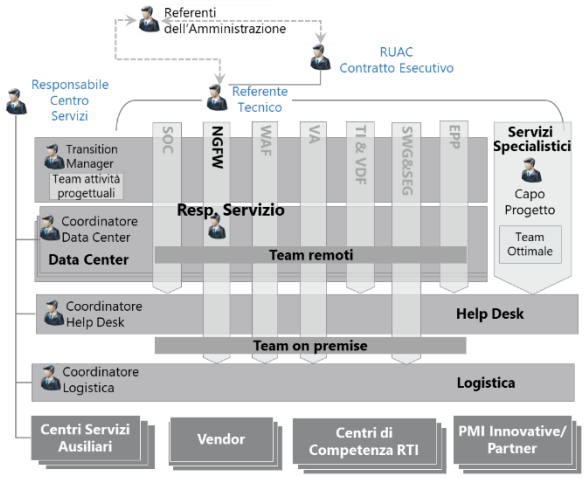

Figura 16 – Organizzazione Servizio NGFW

Erogazione del servizio:

- *Monitoraggio della disponibilità*: gli operatori dell'Help Desk di 2° livello monitorano il servizio attraverso la console (FortiManager) e gestiscono gli allarmi o in autonomia o coinvolgendo le strutture specialistiche di 3° livello.
- *Richieste di modifica delle configurazioni*: L'Amministrazione potrà richiedere l'aggiornamento delle policy di sicurezza utilizzando il portale dei servizi di sicurezza o mediante l'apertura di un ticket (cfr. § 4.3). La richiesta sarà presa in carico dal NGFW team che, una volta effettuate le necessarie attività, provvederà al collaudo della modifica congiuntamente con il personale preposto dell'Amministrazione.
- *Reporting* La reportistica permette di verificare la conformità agli standard scelti e il livello di protezione delle applicazioni. Prevede report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.
- *Supporto alla gestione incidenti*: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

Modalità di erogazione

La modalità di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓installazione di appliance dedicati fisici o virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione; ✓utilizzo di una istanza del servizio NGFW installata presso il Centro Servizi del RTI ed acceduta in modalità SaaS. L'architettura di default proposta dal RTI è quella on premise.

In fase di definizione del progetto esecutivo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione principali per la scelta dello scenario sono: ✓fascia di throughput richiesta; ✓tipologia dei servizi da proteggere, se cioè occorre proteggere servizi esposti su internet o servizi interni del cliente.

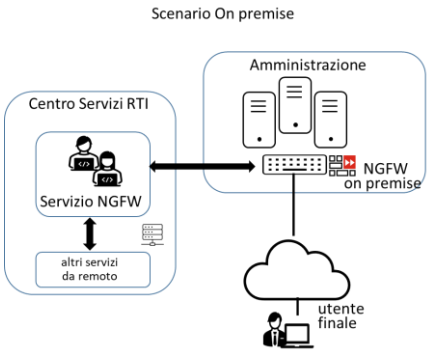

Figura 17 – Modalità di erogazione on premise

Interazione con gli altri servizi

Si riportano di seguito le interazioni principali del Servizio Next Generation Firewall verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: i log del servizio saranno inviati al servizio SOC per la registrazione, tracciatura e correlazione degli eventi, delle minacce e per l'allarmistica. La globalità degli eventi provenienti da domini tecnologici diversi, opportunamente cross

correlati ed orchestrati dal servizio SOC, non solo permettono il rilevamento precoce e proattivo di situazioni anomale, ma consentono anche di rendere particolarmente efficiente il processo di analisi abbreviando i tempi necessari all'individuazione delle azioni mirate al contenimento e alla successiva mitigazione di eventuali incidenti. Le soluzioni tecnologiche presenti nel SOC (SIEM, SOAR, etc.), contribuiranno alla rilevazione di attacchi sofisticati anche con il supporto di tecnologie di machine learning e threat intelligence (cfr. cap.5).

- **Interazione con il servizio Web Application Firewall L1.S3**: La FortiSandbox è a supporto dei servizi NGFW, WAF, SWG&SEG e, attraverso le capacità della Fortinet "Security Fabric", contribuisce alla realizzazione di una forte interazione tra questi servizi. Infatti, qualora la sandbox rilevi una minaccia a seguito di un'analisi eseguita su un file proveniente da uno dei tre servizi, essa produce e rende disponibile una nuova firma zero-day che sarà utilizzata dagli altri servizi per una migliore e più efficace mitigazione di future occorrenze dello stesso malware. Nello specifico, per il solo servizio WAF, in fase di configurazione delle regole, saranno armonizzate le policy che riguardano la protezione dagli attacchi da parte di IP con "bad reputation", oppure le funzionalità di blocco di eventuali indirizzi IP sulla base di geolocalizzazione. Ad esempio, per servizi web che dovranno essere fruiti da utenza presente solo nell'UE, sarà tipicamente impedito il collegamento da indirizzi IP extra UE.
- **Interazione con il servizio Gestione continua delle Vulnerabilità di Sicurezza L1.S4**: Le informazioni sulle vulnerabilità riscontrate saranno utilizzate dal NGFW Team per supportare il tuning delle funzionalità NIDS/NIPS per la riduzione dei falsi positivi.
- **Interazione con il servizio Threat Intelligence & Vulnerability Data Feed L1.S5**: gli IoC dei data feed intelligence sono condivisi con le piattaforme di gestione FortiAnalyzer (post-mortem) e con gli appliance FortiGate (real time) per la ricerca di eventi di compromissione.
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6**: l'interazione avviene secondo le stesse modalità descritte al precedente punto "Interazione con il servizio Web Application Firewall L1.S3".
- **Interazione con il servizio Protezione degli End Point L1.S13**: Qualora la FortiSandbox rilevi una minaccia zero-day, a seguito di un'analisi eseguita su un file proveniente dal servizio NGFW, e conseguentemente produce e rende disponibile una nuova firma/IoC, questa potrà essere utilizzata per alimentare la base di conoscenza della Trend Micro Sandbox Deep Discovery Analyzer (cfr. cap.13) al fine di consentire la protezione anche degli End-Point. Tale interazione è bidirezionale.

6.3. CAPACITÀ DI FORNIRE VISIBILITÀ E CONTROLLO DEGLI UTENTI PER CREARE POLICY, GENERARE REPORT ED ESEGUIRE INDAGINI FORENSI

Il servizio NGFW dispone di una funzionalità avanzate legata alla **User Identity** che consente al RTI di fornire un elevato livello di visibilità ed un granulare controllo degli utenti. L'autenticazione è un processo necessario a confermare l'identità di un utente per garantire che abbia accesso solo alle risorse a cui è autorizzato ad accedere. L'autenticazione degli utenti dell'Amministrazione avviene attraverso l'integrazione diretta con i sistemi esistenti presso l'Amministrazione (ad esempio LDAP, RADIUS, TACACS+, AD o POP3). In questo caso l'appliance FortiGate invia le credenziali immesse dall'utente al server esterno in modalità cifrata ed il server esterno risponde indicando se le credenziali fornite sono valide o meno. In ambiente Microsoft Active Directory è inoltre possibile configurare strategie di SSO per permettere l'autenticazione trasparente senza impatti sulla user-experience.

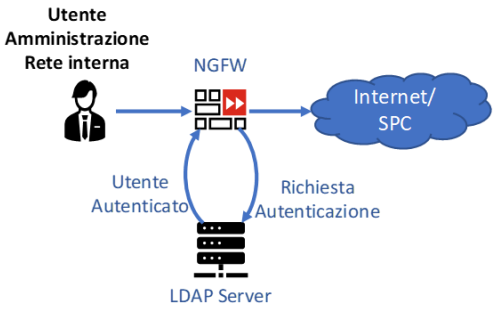

Figura 18 – Interazione NGFW-LDAP

Una volta introdotta la configurazione della **user identity** è possibile la **configurazione di policy specifiche associate a utenti e/o gruppi** al fine di applicare controlli mirati e gestirne le autorizzazioni. Inoltre, il campo "user" consente la generazione di **report specifici relativi agli utenti** ed arricchisce ogni log di traffico con l'informazione relativa all'utente che lo ha generato. Tali log

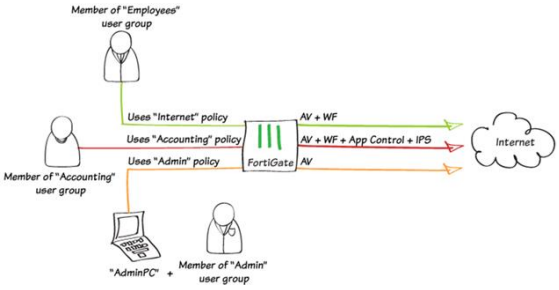

Figura 19 – Esempio di Policy per User

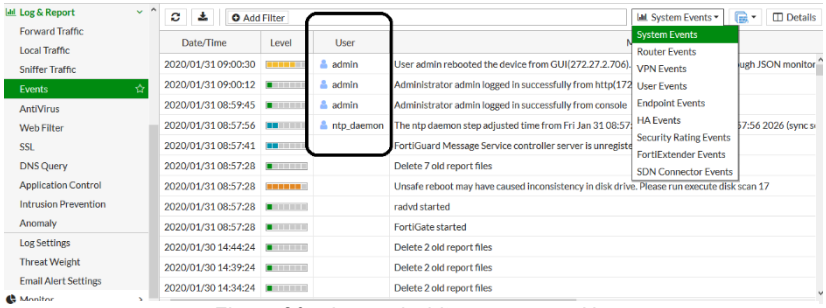

Figura 20 – Log arricchito con campo User

racchiudono quindi tutte le informazioni necessarie all'esecuzione di eventuali **indagini forensi** a seguito di incidenti informatici. Utilizzando la componente dedicata FortiAnalyzer del sistema di gestione, oltre alla capacità di memorizzare i log per un periodo di almeno sei mesi, è garantita l'applicazione della pseudoanonimizzazione dei dati secondo la normativa GDPR. I dati raccolti vengono trattati garantendo cifratura, integrità e non alterabilità; gli apparati NGFW inviano i log al FortiAnalyzer con protocollo proprietario che sfrutta la crittografia TLS/SSL, quindi il trasferimento dei log è cifrato dalla sorgente al log collector (FortiAnalyzer). Il dato viene immagazzinato in un file reso non modificabile in base a politiche di natura dimensionale oppure temporale. Al file così creato, viene applicato un hash (log checksum) per cui sarà possibile verificarne l'integrità al momento in cui sarà necessario importarlo per una eventuale ricerca forense.

7. PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL"

Il servizio di Web Application Firewall (WAF) ha come obiettivo principale quello di proteggere le applicazioni Web esposte su Internet da attacchi specifici al protocollo HTTP/HTTPS e relative anomalie allo stack applicativo, come ad esempio: SQL Injection, Cross-site Scripting (XSS), accesso illegale alle risorse e bot malevoli. L'approccio completo alla protezione delle applicazioni web prevede varie opzioni come la validazione dei metodi HTTP permessi, l'API protection, la firma/criptazione dei cookies e la gestione di meccanismi di accesso alle URL riservate tramite definizione di regole 'custom' specifiche.

Il servizio WAF permette la capacità di controllo degli attacchi **DoS/DDoS** in particolare a livello applicativo (livello 7 ISO/OSI) ed il motore di riconoscimento di tali attacchi è in grado di analizzare le connessioni e permette di controllare le seguenti condizioni: ✓Le richieste HTTP per sorgente; ✓Limitare il numero massimo di connessioni TCP per sessione HTTP attraverso il cookie di sessione; ✓Limitare il numero di richieste HTTP per secondo, per sessione, per URL; ✓Limitare il numero di connessioni TCP per client; ✓Riconoscere se il client è effettivamente un internet browser (real browser enforcement) effettuando sfide al client attraverso javascript.
È inoltre disponibile la possibilità di analizzare la nazione di origine del DDoS e di imporre blocchi sulla stessa.
Il servizio WAF, proposto dal RTI, sarà erogato attraverso il prodotto **FortiWeb** (hardware appliance o virtual appliance on premise) di **Fortinet**. La gestione del servizio viene effettuata mediante la console di management centralizzata **FortiWeb Manager**, attraverso VPN create su connettività INTERNET o SPC e terminate, lato Centro Servizi, sui concentratori attestati sull'infrastruttura di management del servizio.
L'infrastruttura di erogazione del servizio di Web Application Firewall si avvale delle componenti di seguito descritte:

- **FortiWeb Manager:** FortiWeb Manager è una console web che consente di gestire centralmente più dispositivi FortiWeb in remoto. Gli amministratori possono controllare i propri dispositivi (eventualmente, raggruppati logicamente), gestire job e licenze, effettuare upgrade di firmware e signature, controllare rapidamente i vari log e monitorare le statistiche sulle minacce in tempo reale.
- **FortiSandbox** – Il componente FortiSandbox costituisce parte integrante dell'architettura Fortinet Security Fabric e utilizza tre modalità di intelligence sulle minacce per il rilevamento e la prevenzione degli Incidenti di sicurezza (cfr. cap.6).
- **Repository di utenze e dati**: conserva le informazioni più rilevanti (contatti referenti, IP, FQDN, template usato nella configurazione, etc.) relative alle applicazioni di cui sia stato effettuato il provisioning.
- **Appliance FortiWeb Web Application Firewall**: Gli apparati Web Application Firewall rappresentano un elemento chiave nella realizzazione di una piattaforma di sicurezza che, insieme agli altri servizi costituisce un ecosistema di sicurezza "collaborativa" che permette di correlare le informazioni di security tra i diversi servizi
  Nella tabella seguente si riportano le appliance proposte dal RTI per le diverse fasce:

Fasce	Fortinet appliance
Fascia 1: fino a 500 Mbps	FortiWeb-600E
Fascia 2: fino a 5 Gbps	FortiWeb-2000F
Fascia 3: fino a 10 Gbps	FortiWeb-3000F

Tabella 12 – Appliance e throughput previste per il servizio WAF

Il RTI vanta una vasta e profonda esperienza nella erogazione di servizi WAF, in particolare nel comparto della Pubblica Amministrazione. AlmavivA, aggiudicataria in qualità di mandataria dell'accordo quadro SPC Lotto 3 e Lotto 4 ha realizzato e attualmente gestisce presso il proprio Centro Servizi il servizio WAF per importanti portali di primarie amministrazioni centrali, quali MAECI (portale ItalyExpoDubai), portale istituzionale AIFA, Dipartimento della funzione pubblica, IVASS, Consip, MIUR, Presidenza Consiglio dei Ministri (portale G20 e inPA-Portale del Reclutamento) e locali quali Regione Calabria, Campania, Sardegna, Sicilia, Provincia di Como, Comune di Roma e Palermo. Il RTI ha quindi una profonda conoscenza ed esperienza con la tecnologia scelta per questa fornitura oltre ad una consolidata partnership con il vendor. Oltre a rispettare pienamente i requisiti del Capitolato, il servizio WAF proposto dal RTI presenta una serie di caratteristiche tecnologiche e prestazionali migliorative come meglio descritto nel seguito. Tale servizio è caratterizzato dall'utilizzo di un approccio strutturato e integrato con i servizi oggetto di fornitura e **fortemente orientato agli aspetti della sicurezza applicativa WEB** e non solo alla protezione infrastrutturale e di rete. Le scelte architetturali per l'implementazione del servizio, la definizione delle misure e delle regole di protezione e le modalità operative di gestione del servizio stesso discendono da una precisa strategia progettuale. Quest'ultima, infatti, come illustrato in figura, tiene conto dei requisiti e vincoli di sicurezza del cliente e degli scenari delle minacce alle applicazioni che sono in continua evoluzione. A questo riguardo il servizio è progettato per operare con la massima efficacia sia come singolo servizio che, come meglio specificato nel seguito del presente capitolo, mediante l'**interazione in forte sinergia con gli altri servizi** della fornitura.

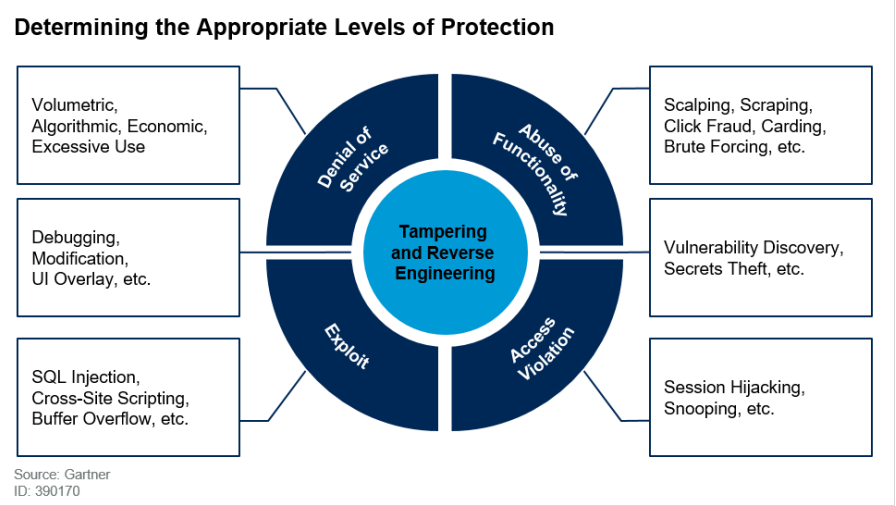

Figura 21 – Decision Point for Deploying WAFs for Application Protection, Gartner 2019

7.1. CARATTERISTICHE TECNOLOGICHE E PRESTAZIONALI MIGLIORATIVE

La soluzione tecnologica adottata dal RTI, oltre a garantire la disponibilità di tutte le funzionalità richieste da Capitolato Tecnico, si caratterizza per una serie di aspetti migliorativi che la pongono all'avanguardia nella erogazione del servizio oggetto del presente paragrafo, in particolare, sotto i punti di vista di:

- **Innovatività e resilienza**: ✓è fornito il riconoscimento evoluto dei Good-Bot dei motori di ricerca noti (es. Google, Yahoo, etc.) e dei Bad-Robots (scanners, crawlers, spiders). Un cruscotto mostra, a livello statistico la ripartizione del traffico tra utenti reali e robot; ✓sono disponibili funzionalità per la prevenzione dalla fuga di diverse tipologie di dato (es. lista directory, dati relativi alla disponibilità e agli errori delle applicazioni, codice sorgente

ASP/JSP, carte di credito); ✓è fornito il supporto alla georeferenziazione degli IP con possibilità di blocco a livello geografico ed analisi dei log basata su dati geografici e il blocco per IP reputation basata sulla categorizzazione del servizio di intelligence Fortinet fornita tramite FortiGuard; ✓è gestita la prevenzione da attacchi brute-force login: la funzionalità tiene traccia della velocità con cui ciascun indirizzo IP sorgente effettua richieste per URL specifici; se l'indirizzo IP di origine supera la soglia, il WAF penalizza l'indirizzo IP di origine bloccando le richieste aggiuntive per il periodo di tempo indicato in configurazione; ✓sono presenti funzioni di offloading dell'autenticazione così da impedire l'accesso ai server da parte di client non autenticati; sono incluse anche funzionalità di supporto al Single Sign-On (sono supportati meccanismi di autenticazione attraverso protocollo LDAP e Active Directory, RADIUS ed NTLM); ✓il livello del log degli eventi è molto dettagliato ed è consentito l'oscuramento di dati sensibili quali password e altre informazioni personali (GDPR); ✓è prevista la verifica della conformità alle HTTP RFC al fine di verificare l'eventuale codice malevolo contenuto nelle connessioni; ✓è disponibile una funzione di protezione dal Web Defacement.

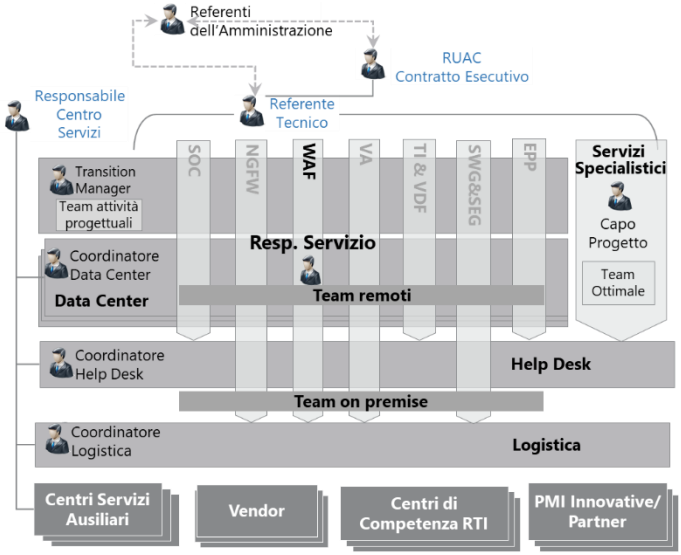

Figura 22 – Organizzazione del servizio

- **Configurabilità**: ✓è possibile definire regole e firme personalizzate, così da garantire l'aderenza a contesti diversi e prevenire falsi positivi; ✓è disponibile la possibilità di gestire eccezioni a vari livelli al fine di eliminare blocchi indesiderati. Le eccezioni per le firme creano dei log a disposizione per analisi da parte degli amministratori; ✓è possibile intervenire con regole di rewrite e reindirizzamento sul flusso http. Ad esempio, è possibile reindirizzare in https il traffico http, restituire pagine in response custom a fronte di particolari condizioni configurabili, modificare alcuni contenuti della response http.
- **Prestazioni e robustezza**: ✓gli apparati FortiWeb previsti offrono prestazioni migliorative in termini di throughput nell'ambito della fornitura in fascia 1, che risulta superiore del 50%, ed in fascia 3 (cfr. 7.3); ✓sono supportate architetture in alta disponibilità secondo due modalità: Active/Passive e Active/Active; ✓possono essere definite regole di compressione e caching in modo molto granulare, così da poter decidere quali siano le risorse cui applicare le funzionalità in oggetto e poter escludere tutti gli oggetti dinamici e, comunque, quelli che non possono essere elaborati attraverso caching e/o compressione.

Nella tabella successiva si evidenzia il miglioramento delle performance in termini di throughput

Fasce	WAF Throughput migliorativi
Fascia 1: fino a 500 Mbps	750 Mbps (+**50%**)
Fascia 2: fino a 5 Gbps	5 Gbps (in linea)
Fascia 3: > di 5 Gbps	10 Gbps (+**100%**)

Tabella 13 – Throughput migliorativi per il servizio WAF

7.2. PROTEZIONE DA EXPLOIT ZERO-DAY, INFEZIONI DA MALWARE E VULNERABILITÀ

Il servizio WAF implementa un modello di protezione ibrido che applica sia meccanismi negativi (blocco di ciò che è conosciuto come malevolo in base a signature) che positivi (è possibile definire il traffico autorizzato e bloccare quello non autorizzato, quindi anche gli attacchi zero-day). La protezione da zero-day è realizzata mediante funzionalità di input validation e parameter validation che bloccano eventuali richieste malformate.

Sono, inoltre, disponibili controlli di tipo sintattico, non basati su pattern, volti a prevenire attacchi di tipo XSS o SQL Injection.

Sono fornite anche funzionalità di machine learning volte a rilevare automaticamente traffico web pericoloso e attacchi provenienti da Bot.

Il modello di *rilevamento delle anomalie* osserva URL, parametri e metodi delle sessioni HTTP e/o HTTPS verso i server Web protetti e utilizza un meccanismo di apprendimento automatico per rilevare il traffico anomalo. Per riconoscere una richiesta come legittima o come potenziale attacco, esegue le seguenti azioni in automatico:

1. Acquisisce e raccoglie input, quali ad esempio i parametri delle URL o i metodi utilizzati, e crea un modello matematico che descrive il corretto utilizzo dei servizi protetti;
2. Rileva eventuali anomalie rispetto al modello precedente e le confronta con modelli pre-costruiti che descrivono le tipologie di minacce conosciute;
3. Rileva eventuali attacchi in base alla correlazione in tempo reale di entrambi i modelli.

L'utilizzo di questa tecnologia, resa disponibile dal FortiWeb, consente di indirizzare attacchi di tipo zero-day con una minimizzazione di falsi positivi.

Il modello di *rilevamento dei bot*, invece, osserva e traccia i comportamenti degli utenti su diverse dimensioni, ad esempio: quante volte le richieste HTTP vengono generate dall'utente, se le richieste utilizzano versioni HTTP illegali, se la richiesta recupera risorse JSON/XML, etc.

A differenza dei meccanismi tradizionali per il rilevamento dei bot, il sistema basato su intelligenza artificiale consente di evitare l'operazione manuale di tuning delle soglie per distinguere le attività lecite da quelle illecite.

Va evidenziato che sul WAF FortiWeb è disponibile, inoltre, una funzione nativa di scansione sugli allegati finalizzata ad individuare virus, malware e grayware sulla base di signature presenti in un database aggiornato automaticamente attraverso una connessione ai laboratori di intelligence FortiGuard.

Infine, il servizio di WAF FortiWeb può utilizzare le funzioni di Forti-Sandbox al fine di migliorare ulteriormente le capacità di identificazione di Zero-Day.

7.3. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il servizio WAF proposto dal RTI viene erogato dal Centro Servizi del Fornitore. Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT (SGS-IT)** conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

Organizzazione del servizio

L'organizzazione del servizio WAF, suddiviso per fasi:

Presa in carico del servizio

- *Acquisizione*, attraverso il *Team on-premise* (cfr. § 4), *di know how relativo al contesto*: il responsabile del servizio WAF invia un documento template al Referente dell'Amministrazione affinché, per ogni applicazione web da integrare, siano fornite le informazioni di base che innescano il processo: responsabile/referente dell'applicazione, IP/FQDN cui risponde ogni applicazione.
- *Predisposizione e configurazione del servizio e delle relative piattaforme di management*: il *WAF Team* procede alla configurazione di base dell'apparato dopo averne assicurato la raggiungibilità da remoto. Questo comporta, oltre alla definizionecoordinatore delle utenze amministrative necessarie, la configurazione di policy standard di base e di policy template rispondenti alle principali casistiche delle applicazioni web da integrare (ad esempio portali CMS, servizi Web, applicazioni transazionali autenticate e non, applicazioni con architetture a microservizi) da utilizzare a modello per le singole integrazioni di applicazioni, l'integrazione del sistema SIEM di riferimento per l'esportazione degli eventi relativi alle applicazioni ed alle operazioni di configurazione effettuate dagli amministratori WAF. Il *Team on-premise* gestisce l'installazione delle componenti previste on-site secondo il piano di installazione condiviso con l'Amministrazione. Gli apparati WAF saranno resi raggiungibili, presi in carico dal sistema di management e configurati da remoto. Il servizio sarà predisposto sulla base di quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano.
- *Migrazione*: nel caso che l'Amministrazione chieda al Fornitore di subentrare da una precedente installazione WAF propria o di terza parte, il Team on-premise e il WAF Team predispongono un processo di verifica delle configurazioni implementate allo scopo di appurarne l'efficacia (si rende utile, allo scopo, il servizio di Gestione continua delle vulnerabilità di sicurezza), la necessità di ottimizzazione prestazionale, la possibilità di integrazione con gli altri servizi. È possibile prevedere una migrazione su apparati proposti dal RTI.

Erogazione del servizio:

- *Provisioning di una configurazione aggiuntiva*: il responsabile del servizio WAF intervista il referente della applicazione usando un formulario (checklist) mirato a stilare le caratteristiche funzionali, architetturali e dimensionali dell'applicazione in oggetto. Tali caratteristiche saranno analizzate al fine di definire una proposta di configurazione che sarà trasmessa al referente. In funzione delle caratteristiche delle policy di sicurezza individuate e approvate dal referente, sarà proposto un processo graduale di attivazione in modalità 'prevent' delle regole. Alcune di esse, infatti, necessiteranno di un periodo di monitoraggio (operato sia tramite le dashboard del WAF stesso, sia tramite alert e report del SIEM) durante il quale saranno configurate in modalità 'detect'. Tale periodo di osservazione, potrà comportare l'affinamento delle stesse a seguito di osservazione (e convalida da parte del referente applicativo) di falsi positivi. L'effettivo onboarding dell'applicazione su WAF comporterà l'interazione con altri servizi della fornitura descritti nel seguito.
- *Conduzione operativa e sistemistica della piattaforma*: ✓monitoraggio della disponibilità e delle prestazioni; ✓applicazione di patch sia a fronte di segnalazione del vendor che di manutenzione in seguito a malfunzionamenti.
- *Supporto alla gestione incidenti*: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓produzione di reportistica per l'Amministrazione, realizzata sulla base di una serie di template standard definiti in fase di progetto esecutivo. Se l'Amministrazione ha aderito al servizio SOC, la reportistica verrà prodotta mediante l'integrazione con il SIEM del Centro Servizi; ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

Modalità di erogazione

La modalità di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓installazione di appliance dedicati fisici o virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione; ✓utilizzo di una istanza del servizio WAF installata presso il Centro Servizi del RTI ed acceduta in modalità SaaS. L'architettura di default proposta dal RTI è quella on premise.

In fase di definizione del progetto esecutivo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono:

✓fascia di throughput richiesta; ✓tipologia dei servizi web da proteggere, se cioè occorre proteggere servizi esposti su internet o servizi interni del cliente; ✓numerosità delle web application da proteggere.

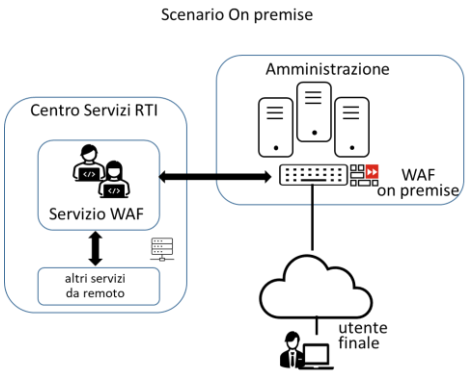

Figura 23 – Modalità di erogazione

Interazione con gli altri servizi

Si riportano di seguito le interazioni principali del Servizio Web Application Firewall verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Security Operation Center L1.S1".
- **Interazione con il servizio Next Generation Firewall L1.S2**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Web Application Firewall L1.S3".
- **Interazione con i servizi Gestione continua delle Vulnerabilità di Sicurezza L1.S4**: Le evidenze dei WAF saranno rese disponibili in maniera da consentire eventuali correlazioni, con un approccio olistico e a 360 gradi rispetto alla superficie di attacco.

  Dal servizio di gestione delle Vulnerabilità verranno recepite eventuali vulnerabilità di natura infrastrutturale e applicativa rilevate durante le scansioni periodiche al fine di implementare, in accordo con la PA, delle regole temporanee di mitigazione (virtual patching) nelle more della realizzazione di un piano di rientro definitivo da parte del personale incaricato dalla PA per la manutenzione correttiva/evolutiva. Inoltre, sarà possibile ridurre il numero dei falsi positivi grazie all'output del VA recepiti dal WAF.
- **Interazione con il servizio Threat Intelligence & Vulnerability Data Feed L1.S5**: L'interazione avviene tramite la FortiSandbox e consente di aumentare la base di conoscenza del servizio WAF per prevenire e mitigare gli incidenti di sicurezza, ad esempio, da malware zero-day.
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Web Application Firewall L1.S3".
- **Interazione con il servizio "Protezione degli End Point" L1.S13**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Protezione degli End Point L1.S13".

8. PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL" - FUNZIONALITA' AGGIUNTIVE

Si conferma la disponibilità di funzioni di "Protezione dagli attacchi DDOS - Distributed Denial of Service" per il servizio WAF (cfr. cap.7).

9. PROPOSTA PROGETTUALE PER IL SERVIZIO "GESTIONE CONTINUA DELLE VULNERABILITA' DI SICUREZZA"

L'aumento degli attacchi informatici e i metodi sempre più sofisticati con cui vengono condotti, ha accresciuto la consapevolezza dei responsabili della sicurezza e della compliance in merito alla necessità di integrare nelle strategie di difesa strumenti e metodologie di verifica continuative. Il servizio proposto dal RTI segue le logiche della **Continuous Adaptive Risk & Trust Assessment** (**CARTA**). L'approccio adottato dal RTI per garantire la sicurezza delle infrastrutture e dei dati delle Amministrazioni promuove una valutazione continua del rischio in modo iterativo. Questa permette di monitorare i cambiamenti di stato e di reagire alla presenza di minacce o pericoli di sicurezza.

9.1. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI** conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale**)** dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT (SGS-IT)** conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

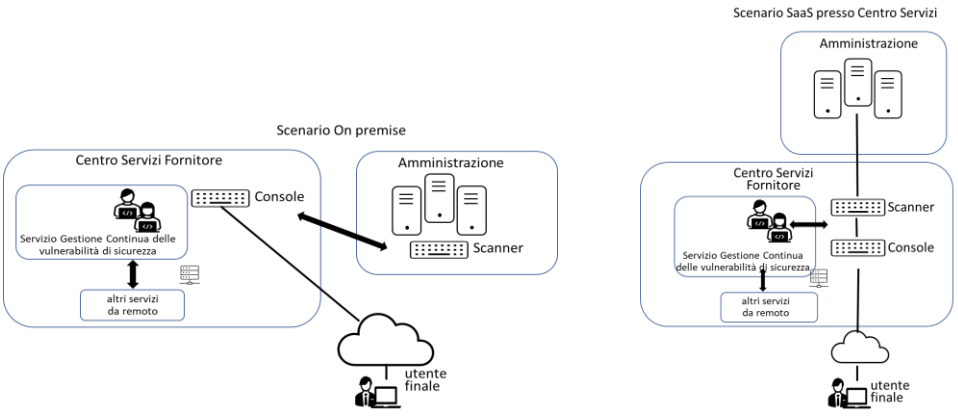

Figura 24 – Modelli di erogazione del servizio VA

Il **modello operativo** di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓installazione di appliance dedicati virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione, architettura di default proposta dal RTI in caso di IP privati; ✓utilizzo di una istanza del servizio installata presso il Centro Servizi del RTI, architettura di default proposta dal RTI in caso di IP pubblici.

In fase di definizione del Piano Operativo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono: ✓frequenza delle analisi richieste per il modello continuativo; ✓tipologia di esposizione dei target analizzati (reti private o pubbliche); ✓numerosità dei sistemi da analizzare.

L'organizzazione del servizio si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- **Manleva:** sarà richiesta la sottoscrizione di una manleva al fine di procedere con l'erogazione del servizio.
- **Referenti:** vengono definiti i referenti del servizio che potranno accedere ai risultati in tempo reale tramite dashboard, gestire le pianificazioni e le scansioni e ricevere i report.
- **Target:** si definiscono la lista degli IP dei sistemi che dovranno essere sottoposti ad analisi
- **Frequenza:** si definisce la frequenza con cui gli IP saranno analizzati

Erogazione del servizio:

- **Scansione**: vengono eseguite analisi e verifiche di sicurezza dei sistemi oggetto del servizio, senza soluzione di continuità e con la frequenza definita dalle PA.
- **Interruzione d'emergenza:** Le Amministrazioni potranno richiedere la sospensione delle analisi in caso di criticità.
- **Richieste di modifica della configurazione:** Le Amministrazioni potranno aggiornare le politiche di sicurezza utilizzando il portale dei servizi di sicurezza (in caso di contestuale acquisizione del servizio SOC) o mediante l'apertura di un ticket. La richiesta sarà presa in carico dal team specialistico che, una volta effettuate le necessarie attività, provvederà a darne comunicazione al referente dell'Amministrazione in funzione del canale di ingaggio.

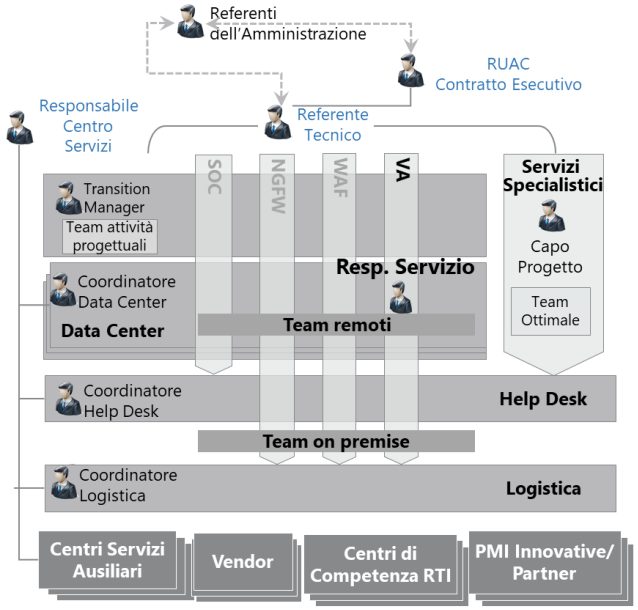

Figura 25 – Organizzazione del servizio VA

- **Reporting:** La reportistica permette di verificare il livello di sicurezza dei sistemi, riportando ogni vulnerabilità rilevata. La reportistica prevede report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), ad esempio evidenziando lo stato su base dello storico delle vulnerabilità, quali ad esempio vulnerabilità nuove e vulnerabilità sanate. La piattaforma offre un sistema di reporting basato su modelli che possono produrre report tecnici altamente dettagliati, scorecard sintetiche per i C-Level, VP-Level, D-Level, Manager, Technical SME-Level (es: CISO, CTO, CIO, DPO, etc.). Tutti gli elementi grafici o testuali possono essere selezionati singolarmente (es. solo le vulnerabilità critiche) ed ordinati. È possibile pianificare la generazione dei report ed il reperimento in diversi formati, inclusi HTML, PDF, CSV e formati XML, inoltre via API possono essere generati e scaricati automaticamente. Tutti i dati delle scansioni, indipendentemente dalla sorgente, vengono memorizzati e consolidati in modo sicuro in un singolo database, gestito in conformità con le primarie compliance di settore (GDPR, PCI-DSS, HIPAA, HITECH, SOX, ISO, GLBA, CobiT), all'interno del Centro Servizi. La reportistica sarà inviata automaticamente dal Centro Servizi, ai referenti del servizio, tramite e-mail, al termine di ogni singola scansione. Le Amministrazioni, come valore aggiunto, possono ottenere la reportistica anche accedendo alla Console nel Centro Servizi, in modo:
  - **Real time:** per visualizzare sia i risultati sia lo stato delle scansioni, in tempo reale, accedendo alla Dashboard interattiva
  - **On Demand**: per scaricare i risultati delle analisi completate

Il servizio è erogato in modalità SaaS dal Centro Servizi e può analizzare il livello di rischio sia di sistemi esposti su internet sia sistemi interni all'Amministrazione.

Nel caso di IP esposti su Internet, il servizio viene erogato tramite scanner abilitati al traffico Internet, tale configurazione non richiede l'uso di scanner dedicati per le Amministrazioni. Nel caso di IP privati delle Amministrazioni invece, ad ogni Amministrazione sarà messo a disposizione un proprio scanner virtuale su cui sarà applicata una configurazione VPN (Virtual Private Network) per consentire la raggiungibilità dal Centro Servizi.

Questa soluzione, quindi, consente di coniugare i benefici di una soluzione centralizzata (Console), con la scalabilità derivante da una soluzione multi-tenant.

Il servizio sarà basato sulla piattaforma Tenable.sc, la miglior piattaforma disponibile oggi sul mercato per rilevare e gestire le vulnerabilità, indicata nella The Forrester Wave™ come Leader di Vulnerability Risk Management, con la miglior strategia e la miglior offerta oggi disponibile su scala mondiale. Caratteristiche fondamentali e distintive della piattaforma sono:

1. capacità di verificare più di 65.000 vulnerabilità;
2. capacità di rilasciare tempestivamente aggiornamenti mantenendo una copertura accurata nel rilevamento delle vulnerabilità. La Tenable.sc Research Organization produce aggiornamenti in 12-72 ore dalla divulgazione della vulnerabilità/data di pubblicazione del fornitore, ciò include vulnerabilità di alto profilo e avvisi di fornitori standard come Microsoft Patch Tuesday, CPU Oracle, avvisi di sicurezza della distribuzione Linux/Unix e altri;
3. Disponibilità della Predictive Prioritization, che consente di concentrare i propri sforzi in base alle vulnerabilità che è più probabile che vengano sfruttate, che avrebbero un impatto maggiore. La Predictive Prioritization combina dati provenienti da varie fonti, includendo lo standard CVSS, che in ogni caso è disponibile anche esplicitamente. Inoltre essa analizza oltre 111.000 vulnerabilità distinte ogni 24 ore per aggiornare costantemente il mutevole panorama delle minacce, riducendo del 97% il numero di vulnerabilità critiche e alte che le Amministrazioni dovranno correggere.

L'infrastruttura di erogazione del servizio si avvale delle componenti di seguito descritte:

- **Scanner** – Software reso disponibile su sistema virtuale dell'Amministrazione e presente di default nel Centro Servizi, che esegue le verifiche di sicurezza sui dispositivi raggiungibili ed identificati come target, tramite comunicazioni basate su protocollo IP. La soluzione abilita le Amministrazioni a: ✓analizzare sia sistemi esposti su Internet sia sistemi interni; ✓eseguire ricerche di vulnerabilità sui propri sistemi senza soluzione di continuità.

- **Console** - Piattaforma centralizzata multi-tenant istanziata presso il Centro Servizi del RTI, utilizzata per la gestione del servizio. Consente la separazione logica delle PA contraenti in domini distinti (Tenant) garantendo la segregazione completa dei dati. È una singola console di management che consente di gestire dispositivi Scanner e fornire funzionalità di settings e update centralizzato per tutti gli apparati gestiti. Il modulo contiene la base dati con le configurazioni, l'asset inventory, le pianificazioni, i profili di analisi, la base di conoscenza delle vulnerabilità pubblicamente note su scala internazionale, la base dati delle verifiche possibile sui sistemi, il motore di generazione ed invio della reportistica, l'archivio dei risultati delle analisi eseguite, i feed ed i contenuti di Cyber Threat Intelligence per estendere la soluzione proposta con metodi di interoperabilità. Include una interfaccia web per gli utenti per consentire di interagire con la piattaforma, di visualizzare in tempo reale i risultati, lo stato delle scansioni, le pianificazioni e le configurazioni.

Monitoraggio e scansione degli asset

La soluzione implementa funzioni di network discovery, definizione di policy di compliance e auditing, asset inventory, gestione delle vulnerabilità, gestione dei certificati TLS/SSL, asset management, gestione delle credenziali per accessi ai sistemi, gestione di rete per scanner multipli, remediation tracking e integrazione con LDAP.

Per assicurare costantemente il monitoraggio degli asset, la piattaforma offre:

- un sistema integrato di calendarizzazione degli eventi tramite cui le Amministrazioni avranno la possibilità di pianificare le proprie scansioni sui propri sistemi;
- un sistema integrato di feed che consente di ricevere dati sempre aggiornati su scala internazionale, con dettagli tecnici relativi all'enumerazione e all'analisi di sistemi operativi, applicazioni, software, configurazioni, servizi, etc.

La piattaforma ha la capacità di eseguire scansioni multiple in parallelo sui diversi sistemi target, attraverso sia gli scanner posizionati presso le Amministrazioni, sia utilizzando gli scanner esposti su Internet.

La soluzione è in grado di scansionare un elevato numero di sistemi operativi, identificando le vulnerabilità esposte da software e servizi di apparati connessi alla rete, siano essi server, client, database, web application, application server, etc.

Il servizio ha la capacità di classificare i rischi individuando i livelli di gravità, tramite uno standard denominato Common Vulnerability Scoring System (CVSS), già calcolato per ogni vulnerabilità rilevata, con l'ultima versione disponibile, la versione 3.1.

Per una completa contestualizzazione delle minacce, quindi per una chiara interpretazione degli impatti associati alle vulnerabilità, la piattaforma fornirà i seguenti dettagli:

- CVSS Base: un valore da 1 a 10 in cui 10 rappresenta il livello più critico di una vulnerabilità
- CVSS Base Vector: una stringa che consente di conoscere gli impatti RID della vulnerabilità, quindi gli impatti che lo sfruttamento di tale vulnerabilità potranno avere su Riservatezza, Integrità e Disponibilità;
- CVSS Origin: l'ente accreditato che ha elaborato la contestualizzazione della vulnerabilità, prevalentemente ad opera del National Vulnerability Database, repository governativo statunitense dei dati delle vulnerabilità basati sullo standard del Security Content Automation Protocol.
- CVSS Date: la data di classificazione del rischio della vulnerabilità

La soluzione consente di creare Profili che contengono le istruzioni relative alla modalità operativa dell'attività di scansione; in particolare è possibile personalizzare il numero di porte (TCP, UDP), le vulnerabilità da ricercare o ignorare, gli apparati da utilizzare singolarmente o in combinazione per la scansione, il livello di performance desiderato (ovvero le impostazioni dei limiti alle performance per ridurre l'impatto sul network).

Interazione

Si riportano di seguito le interazioni principali del Servizio Gestione continua delle vulnerabilità di sicurezza verso gli altri servizi le cui modalità sono descritte nei paragrafi specificati in elenco: ✓**Interazione con il servizio "Security Operation Center" L1.S1**: (cfr. § 6.2); ✓**Interazione con il servizio Next Generation Firewall L1.S2** (cfr. § 6.2); ✓**Interazione con il servizio Web Application Firewall L1.S3**: (cfr. § 7.3).

9.2. DISPONIBILITÀ DI CRUSCOTTI DINAMICI CHE CONSENTANO DI MONITORARE LA SUPERFICIE VULNERABILE IN TEMPO REALE

Le dashboard della Console consentiranno di default il monitoraggio della superficie d'attacco indicata dal referente della PA, in tempo reale e in modalità interattiva.

La piattaforma offre inoltre la possibilità di organizzare e visualizzare le informazioni più rilevanti in funzione del destinatario. I cruscotti possono essere personalizzati, resi accessibili e condivisi con gli altri utenti autorizzati. Le dashboard consentono di visualizzare informazioni provenienti dalle diverse applicazioni in un'unica schermata, offrendo un framework omogeneo oltre che una visione olistica e generale della postura di sicurezza.

Le dashboard possono essere modificate anche tramite query che consentono di portare in evidenza politiche, standard e linee guida adottate dalle singole Amministrazioni, ciò consente una visualizzazione dei risultati allineata ai processi di manutenzione delle Amministrazioni.

Le dashboard rappresentano graficamente numerosi dati, tra cui: principali vulnerabilità rilevate, distribuzione delle vulnerabilità sui sistemi, variazione delle vulnerabilità nel tempo, i protocolli più

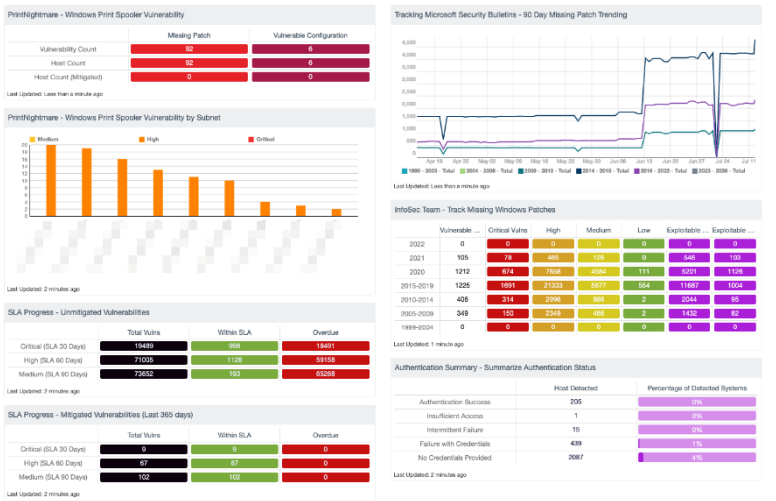

Figura 26 – Dashboard

vulnerabili, le vulnerabilità più frequenti, i software più vulnerabili, i sistemi operativi maggiormente impattati dalle vulnerabilità, i sistemi più vulnerabili, le remediation più importanti non ancora applicate, etc.
Tenable.sc fornisce di default oltre 400 dashboard personalizzabili e oltre 200 template di reportistica.

10. PROPOSTA PROGETTUALE PER IL SERVIZIO "THREAT INTELLIGENCE & VULNERABILITY DATA FEED"

Il servizio predisposto dal RTI offre alle PA una soluzione end-to-end per definire, monitorare, analizzare e migliorare il proprio livello di sicurezza cyber complessivo secondo un approccio predittivo e di analisi di contesto, seguendo logiche cyber-intelligence driven ad ampio spettro. In aggiunta, sfruttando tecniche e strumenti di automazione, consente di definire un livello di rischio in maniera statica e di studiarne le evoluzioni nel corso del tempo, grazie ad un monitoring costante della security posture di una specifica Amministrazione. Il servizio consente di identificare e definire eventuali minacce esterne, accertare le proprie aree di vulnerabilità e i propri asset a rischio di esposizione e compromissione. Il servizio si basa su una **Threat Intelligence Platform** consolidata in ambito internazionale per la collaborazione dei **CSIRT** e l'Info Sharing, denominata **Joshua CybeRisk Vision™**. La soluzione è sviluppata a partire dal 2018 ed ha consentito negli ultimi due anni di enumerare, analizzare e contestualizzare gli asset e definire la postura delle Top 500 PMI in Italia. L'efficacia di tale soluzione è ampiamente osservabile nei contesti moderni che includono il Cloud Computing, in particolare nella capacità di rilevare i sistemi Shadow IT, sistemi al di fuori del governo di un'organizzazione.
Le Amministrazioni che adotteranno questo servizio potranno arricchire i propri apparati infrastrutturali tramite un flusso informativo con dati di minacce globali, forniti dai principali attori internazionali di Info Sharing. In aggiunta, si rendono disponibili in forma esclusiva dati su minacce afferenti sistemi informativi italiani, in particolare flussi contenenti dati sulle minacce attive ai danni della Pubblica Amministrazione.
Il servizio proposto facilita lo scambio e la condivisione di informazioni sulle minacce, Indicatori di Compromissione (IoC) su malware e attacchi mirati come ad esempio frodi finanziarie. La condivisione è basata su un modello distribuito contenente informazioni tecniche e non tecniche che possono essere condivise all'interno di organizzazioni private, semi-private o aperte. Lo scambio di tali informazioni porta a un rilevamento più rapido degli attacchi, riducendo il numero di falsi positivi, e producendo reportistica arricchita grazie a sistemi di automazione e all'ampio utilizzo di standard internazionali, completando il servizio con un sistema integrato di API ReST.
Tramite le informazioni aggiuntive di Intelligence, sarà possibile ricostruire preventivamente la Kill Chain e monitorare eventuali Tattiche, Tecniche e Procedure (TTP) introdotte dai Threat Actor per aggirare i controlli di sicurezza delle Amministrazioni e dei loro fornitori (supply-chain based). Tramite tale servizio saranno resi disponibili feed continuamente aggiornati, con dati di elevato valore e altamente affidabili in quanto prodotti principalmente su dati reali di attacchi rilevati e gestiti, contestualizzati su target italiani. Questo approccio supera qualitativamente le indicazioni globali dei provider internazionali, in particolare supera i data feed basati su sistemi esca non nazionali (Honeypot e Honeynet), che tuttavia sono presenti a completamento del catalogo offerto.
Il servizio genera automaticamente molteplici evidenze di rilevamento delle intrusioni; per esempio, nel caso di sistemi IDS (Intrusion Detection System) sono supportati Indicatori di Compromissione (IoC) basati su IP, domini, nomi di host, user agent, etc. e la generazione di elenchi hash per i valori MD5/SHA1 degli artefatti di file. Le funzionalità API del servizio consentono l'interfacciamento principalmente con strumenti di automazione proposti dal RTI per gli altri servizi in ambito o già in uso presso l'Amministrazione e prevedono una comunicazione di tipo machine to machine, tramite l'uso di opportune chiavi (token) al fine di semplificare il processo di autenticazione.
Elemento distintivo del servizio è la possibilità di ottenere, tramite **Joshua**, per ogni Amministrazione, specifici IoC di **Threat Analytics** per il proprio Sistema Informativo esposto su Internet, indicazioni di **Data Breach** presenti su GitHub, Pastebin o servizi FTP e SMB, gli **Info Leak** su Twitter, gli Asset della PA pubblicamente noti mediante **Postural Assessment**, gli account della specifica PA mediante **Theft Accounts**, minacce agli utenti della PA mediante **Web Malware Detection** sui principali siti della PA. Joshua, erogato nella modalità Threat Intelligence Data Feed, coniuga la capacità di ricercare codici di autenticazione, software, e-mail, dati GDPR rilevanti, etc., sui principali siti utilizzati da sviluppatori e Threat Actor, con la capacità di correlare gli elementi con i dati dello specifico Sistema Informativo esposto su Internet di una PA, **contestualizzando il subset informativo delle minacce**. Saranno infine utilizzate **tassonomie e schemi di classificazione** ben noti per supportare la classificazione standard utilizzata da ENISA, Europol, DHS, CSIRT o molte altre organizzazioni.

10.1. NUMEROSITÀ, TIPOLOGIE E CARATTERISTICHE DEI DATA FEED

Il servizio offre la disponibilità di feed gratuiti, a pagamento, e include Indicatori di Compromissione (IoC), bollettini di sicurezza informatica, e altre informazioni, sia da fonti aperte sia da fonti private.
I data feed sono classificati secondo il Traffic Light Protocol (TLP), un protocollo creato per facilitare una maggiore condivisione delle informazioni. TLP è un insieme di designazioni utilizzate per garantire che le informazioni sensibili siano condivise con il pubblico appropriato ed impiega quattro colori per indicare i limiti di condivisione previsti che devono essere applicati dai destinatari. Il catalogo proposto dispone di **80 data feed**, **classificati TLP: Amber, Green e White**. I dati sorgenti sono principalmente provenienti dal RTI, pertanto focalizzati su dati reali acquisiti su sistemi informativi e riguardante attacchi indirizzati a organizzazioni italiane e **pubbliche amministrazioni**. Sono comunque disponibili dati da sorgenti internazionali, appartenenti ad **enti promotori di Threat Intelligence Information Sharing**.
I Data Feed disponibili out-the-box nella piattaforma includono feed commerciali, con classificazione TLP:Amber e Green, forniti dalle sorgenti Joshua **CybeRiskVision** e **Kaspersky**. Di seguito si riporta il **Catalogo dei Data Feed**:

#	Sorgente	Tipologia		#	Sorgente	Tipologia
1	Kaspersky	Malicious URL		**41**	Blocklist.de	VOIP attack
2	Kaspersky	Phishing URL		**42**	COVID-19 Coalition	Temporary case
3	Joshua	Threat Analytics (Firewall)		**43**	SANS	Handler's Diary
4	Joshua	Threat Analytics (IDS)		**44**	SANS	Up and Coming Ports

5	Joshua	Threat Analytics (AEP)		**45**	SANS	Top 100 Source (NoBlacklist)
6	Joshua	Threat Analytics (Virus)		**46**	SANS	All Source IPs (NoBlacklist)
7	Joshua	Threat Analytics (Exploit)		**47**	SANS	Block List
8	Joshua	Data Breach: GitHub		**48**	US-CERT	All NCAS Products
9	Joshua	Data Breach: Pastebin		**49**	US-CERT	Alerts
10	Joshua	Data Breach (FTP)		**50**	US-CERT	Analysis Reports
11	Joshua	Data Breach (SMB)		**51**	US-CERT	Bulletins
12	Joshua	Info Leak: Twitter		**52**	US-CERT	Tips
13	Joshua	Postural Assessment		**53**	US-CERT	Current Activity
14	Joshua	Theft Accounts		**54**	ICS-CERT	Alerts
15	Joshua	Web Malware Detection		**55**	ICS-CERT	Advisories
16	Telsy/Odino	Network Activity IP		**56**	ICS-CERT	Announcements
17	Telsy/Odino	Network Activity Domini		**57**	malwaredomainlist	Virus
18	Telsy/Odino	Malware Hash		**58**	diamondfox_panels	ioc
19	Telsy/Odino	Detection Rules		**59**	firehol_level1	Network activity
20	Telsy/Odino	Network Activity IP		**60**	cinsscore.com	Network activity
21	CIRCL	All		**61**	alienvault.com	Network activity
22	The Botvrij.eu	All		**62**	Dataplane.org	SSH attack
23	EmergingThreats	Network activity		**63**	Dataplane.org	VOIP attack
24	Dan.me.uk	Tor exit nodes		**64**	Dataplane.org	Mail Server attack
25	Cybercrime	Malware online url		**65**	Dataplane.org	Network activity
26	Phishtank	Phishing url		**66**	Dataplane.org	Other
27	FeodoTracker	Network activity		**67**	Vxvalut	Virus
28	OpenPhish	Phishing url		**68**	Cybercrime-tracker	Virus
29	Bambenekconsulting	Network activity (IP)		**69**	Greensnow.co	Spam attack
30	Bambenekconsulting	Network activity (domain)		**70**	ZeroDot1	Mining
31	Abuse.ch	Malware online url		**71**	CyberCure	Network activity (ip)
32	Mirai Security	Network activity		**72**	CyberCure	Malware online url
33	Malshare	Virus		**73**	CyberCure	Virus
34	Benkow	Virus		**74**	Ipspamlist.com	Network activity
35	Abuse IPDB	Network activity		**75**	MalSilo	Malware online url
36	Blocklist.de	Network activity		**76**	MalSilo	Network activity (ip)
37	Blocklist.de	Spam attack		**77**	MalSilo	Network activity (domain)
38	Blocklist.de	FTP attack		**78**	Ipsum	Network activity (ip)
39	Blocklist.de	Mail Server attack		**79**	DigitalSide	All
40	Blocklist.de	SSH attack		**80**	eCrimeLabs	Metasploit CVE

Tabella 14 – Catalogo dei Data Feed

Il catalogo è **sottoposto periodicamente ad analisi di sovrapposizione** dei dati dei feed, ad oggi la duplicazione dei dati dei diversi data feed è **limitata all'1%.** Si evidenzia che la piattaforma consente un'estensione del catalogo dei data feed attraverso l'inserimento di nuovi flussi eventualmente già nella disponibilità delle Amministrazioni.

10.2. MODALITÀ E FREQUENZA DI AGGIORNAMENTO DEI DATA FEED

I data feed vengono aggiornati in due modalità: automatica e manuale, a seconda della tipologia di feed e delle sorgenti del dato. Nel caso di aggiornamento automatico, sistemi API interrogano e ricevono dati aggiornati da Organizzazioni Sorgenti di data sourcing, nazionali ed internazionali; un esempio è il flusso informativo delle Vulnerabilità note (2002-2021) che include anche la capacità di enumerare sistemi operativi, i software, gli aggiornamenti, arricchiti dai commenti ufficiali dei produttori. Nel caso di aggiornamento manuale, gli analisti del centro di competenza di Advanced Threat Hunting di Joshua CybeRisk Vision arricchiscono i data feed aumentandone i dettagli e la contestualizzazione, in modalità continuativa. La piattaforma prevede di default un aggiornamento della base dati ogni **trenta secondi**, tuttavia, attraverso un sistema parametrico, aggiornamenti con frequenze minori potranno essere implementati su richiesta della PA. Al fine di consentire un'efficiente configurazione dei data feed, implementando una ottimizzazione del consumo delle risorse di rete e di processamento, ogni Organizzazione Sorgente è caratterizzata da una periodicità di pubblicazione basata sulla frequenza degli eventi disponibili di una determinata tipologia di dato. Adottando un modello risk-based, i data feed sono aggiornati con frequenze dipendenti principalmente dal TLP. I data feed TLP: Amber proposti sono aggiornati e resi disponibili in **near real time**.

10.3. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT (SGS-IT)** conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management). Il **modello operativo** di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓comunicazione tramite HTTPS API Gateway; ✓ comunicazione tramite TAXII server.

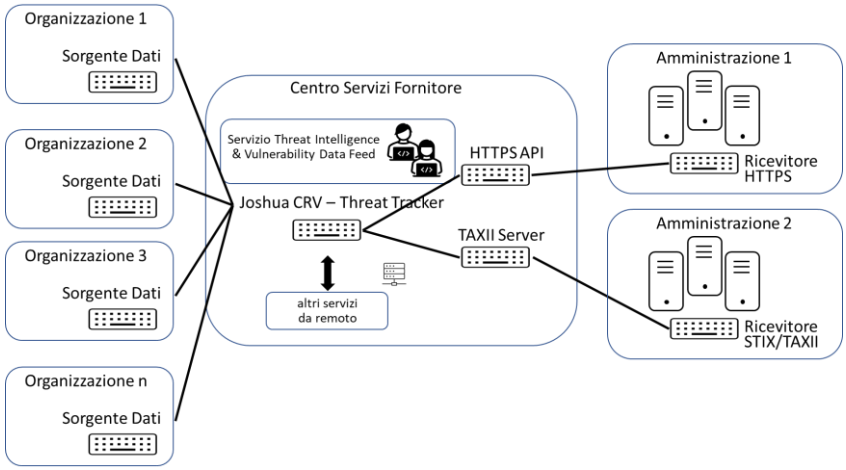

Figura 27 – Modalità di erogazione del servizio TI&VDF

In fase di definizione del Piano Operativo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono: ✓quantità di data feed sottoscritti; ✓tipologia di apparato candidato alla ricezione dei flussi dati.

L'organizzazione del servizio si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- **Catalogo:** ogni Amministrazione indicherà i singoli data feed che vorrà abilitare all'interno del flusso informativo che riceverà costantemente;
- **Modello di comunicazione:** ogni Amministrazione indicherà le modalità di ricezione del flusso informativo che riceverà costantemente. Tali modalità sono: HTTPS API Gateway o TAXII server;
- **Attack Surface Management:** ogni Amministrazione dichiarerà la superficie esposta del proprio Sistema Informativo al fine di sottoporla a monitoraggio passivo, tramite correlazione automatica degli IoC su fonti OSINT e CLOSINT, producendo anche segnali di allerta in caso di minaccia verso un proprio asset;
- **Token di accesso**: ogni Amministrazione avrà un token per accedere al flusso di dati afferenti i feed sottoscritti. Il token sarà generato dal RTI e fornito tramite comunicazione sicura (es: e-mail cifrata).

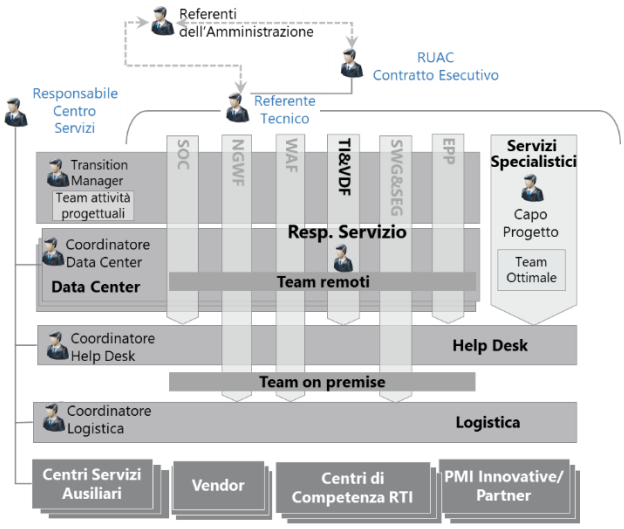

Figura 28 – Organizzazione del servizio TI&VDF

Erogazione del servizio:

- **Info Sharing**: il flusso dei dati richiesti sarà inviato dal Centro Servizi alle Amministrazioni, senza soluzione di continuità. Il flusso sarà disponibile in tempo reale ed includerà tutti i dati di una specifica sottoscrizione.
- **Modalità HTTPS API**: L'erogazione del servizio è prevista tramite API, quindi tramite rilascio da parte del Centro Servizi di un Token per autenticazioni machine to machine. Le API sono rese disponibili tramite protocollo HTTPS, implementando di default un canale di cifratura per una comunicazione sicura delle informazioni, disponibili nei principali formati (JSON, XML, CSV).
- **Modalità STIX/TAXII:** la comunicazione sarà diretta verso il TAXII server ed i dati saranno trasmessi in modo strutturato, nel formato STIX 2.0. Il modello TAXII previsto è **Source/subscriber**, pertanto il Centro Servizi si costituirà singola fonte di informazione per le Amministrazioni richiedenti.
- **Reporting**: Attraverso le API le Amministrazioni potranno generare report o raccogliere i dettagli tecnici di cui necessitano, come ad es. il numero di volte che una specifica minaccia è stata individuata nel mondo, gli URL contenenti codici dannosi e il comportamento tipico di un malware sul sistema dove è stato individuato. A tal proposito di seguito si riporta un estratto esemplificativo dei parametri delle API di ricerca: ✓returnFormat: indica il formato richiesto per i risultati della ricerca (json, xml, openioc, suricata, snort); ✓org: ricerca focalizzata per l'organizzazione che ha rilasciato uno specifico data feed; ✓from: eventi a partire da una determinata data; ✓to: eventi precedenti ad una determinata data; ✓withAttachments: consente di codificare gli allegati come nel caso di malware di esempio.

L'infrastruttura di erogazione del servizio si avvale delle componenti di seguito descritte:

- **Joshua CybeRisk Vision – Threat Tracker:** Sistema centrale di raccolta dei dati, di correlazione e di condivisione. Tramite gli Indicatori di Compromissione sotto forma di eventi arricchiti di numerosi tag, determina gli attributi e li contestualizza per i Sistemi Informativi sottoposti a monitoraggio. Le sorgenti principali di tali indicatori sono le seguenti: ✓Feedback provenienti da una attività continua di ricerca approfondita da parte di analisti del settore; ✓Informazioni provenienti da fonti Aperte (OSINT) opportunamente verificate e certificate come attendibili; ✓Feedback da parte di tecnologie automatizzate dedicate alla ricerca e alla validazione di IoC; ✓Informazioni provenienti da fonti selezionate con le quali esiste una partnership; ✓Informazioni pubbliche relative a liste reputazionali di IP, Black List e output di sandbox.

Per ciascuna macrocategoria di sorgente è previsto uno step di analisi di attendibilità e verifica prima della definitiva pubblicazione dell'evento, con lo scopo di ridurre sensibilmente la possibilità di mettere in produzione dati che potrebbero generare anomalie degli allarmi di sicurezza o addirittura il blocco dei sistemi.

- **HTTPS API Gateway** – Abilita la comunicazione machine to machine per automatizzare la raccolta dei dati e le attività di reporting.
- **TAXII Server** - Abilita l'invio del flusso dati tramite il protocollo di comunicazione TAXII, le cui informazioni sono strutturate secondo il linguaggio **STIX 2.0** (e precedenti).

Interazioni

Si riportano di seguito le interazioni principali del Servizio Threat Intelligence & Vulnerability Data Feed verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: le informazioni gestite dal servizio Threat Intelligence & Vulnerability Data Feed sono inviate al servizio SOC in modalità machine to machine, per supportare il processo di prevenzione e gestione degli incidenti. Inoltre, il servizio SOC invia i data feed al servizio Threat Intelligence & Vulnerability Data Feed che, pertanto, arricchirà a sua volta il bacino informativo a disposizione delle Amministrazioni richiedenti tale servizio.
- **Interazione con il servizio Next Generation Firewall L1.S2:** (cfr. § 6.2 sezione Interazioni).
- **Interazione con il servizio Web Application Firewall L1.S3:** (cfr. § 7.3 sezione Interazioni).
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6:** (cfr. § 6.2 sezione Interazioni).
- **Interazione con il servizio Protezione degli End Point L1.S13**: il servizio di Threat Intelligence invia le segnalazioni (IoC) tramite l'utilizzo di API introducendo, di conseguenza, le protezioni per la rete dell'Amministrazione direttamente su dispositivi degli utenti.

11. PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA"

Il servizio di protezione della navigazione Internet e della posta elettronica (di seguito anche SWG&SEG) proposto dal RTI, si avvale di soluzioni best in class di comprovata efficacia, basate su tecnologia **Fortinet**. Prevede un modello di erogazione composto da due sotto-servizi, uno dedicato alla protezione della navigazione Internet (SWG) ed uno dedicato alla protezione della posta elettronica (SEG).

Il servizio SWG viene erogato attraverso appliance **FortiGate** (hardware appliance o virtual appliance on premise) mentre il servizio SEG viene erogato in modalità SaaS dal Centro Servizi attraverso la soluzione **FortiMail**.

La gestione del servizio viene effettuata attraverso VPN create su connettività INTERNET o SPC e terminate, lato Centro Servizi, sui concentratori attestati sull'infrastruttura di management del servizio.

L'infrastruttura di management del servizio SWG&SEG si avvale delle componenti:

- **Management FortiManager –** Piattaforma centralizzata di gestione del servizio SWG, SEG e della Sandbox (cfr. cap. 4).
- **Logging&Reporting FortiAnalyzer** – Piattaforma centralizzata di logging e reportistica del servizio SWG&SEG (cfr. cap. 4).

L'infrastruttura di erogazione del servizio SWG&SEG si basa sui seguenti apparati:

- **SWG FortiGate** – Appliance in grado di proteggere le Amministrazioni dagli attacchi web grazie alle funzionalità di URL Filtering, alla visibilità e al controllo del traffico web crittografato tramite ispezione SSL e all'applicazione di policy granulari per le applicazioni web. Fortinet è il primo e unico fornitore di gateway di sicurezza ad avere ottenuto la certificazione VBWeb di Virus Bulletin per l'efficacia del web filtering.
  Il Secure Web Gateway mette a disposizione le necessarie funzionalità per proteggere la navigazione web. In particolare, è possibile configurare il servizio nelle modalità Transparent Proxy e di Explicit HTTP/HTTPS Proxy, SOCKS proxy. Tali apparati supportano molteplici modalità di autenticazione (Kerberos, NTLM, LDAP, captive portal, etc.) e protezione/filtering sia in ambito Web sia in ambito applicativo. L'Authentication Rule permette di applicare policy personalizzate per utenti/gruppi. È anche possibile definire se l'autenticazione deve essere fatta su base IP o su base sessione. Le proxy policy consentono di definire un controllo molto granulare delle applicazioni web utilizzando l'ispezione di particolari campi del pacchetto HTTP. Sulla proxy policy è quindi possibile applicare, oltre il web filtering che è il servizio principale, ulteriori controlli di sicurezza come **Application Control**, **Antivirus, IPS, DLP, File Filter, Video Filter, ICAP** per l'interfacciamento con ispezioni di terze parti, **SSL inspection** per estendere l'analisi al traffico cifrato come HTTPS.
- **FortiSandbox** – Il componente FortiSandbox supporta il servizio SWG&SEG per la detection di **malware Zero-Day** e/o **ransomware** e costituisce parte integrante dell'architettura Fortinet Security Fabric e utilizza tre modalità di intelligence sulle minacce per il rilevamento e la prevenzione degli Incidenti di sicurezza (cfr. cap. 6).
- **SEG FortiMail** – Il FortiMail è un potente secure email gateway in grado di proteggere la posta elettronica da una vasta tipologia di attacchi specifici tra cui **phishing**, **speal phishing**, **Business Email Compromise** (BEC), prevenendo la perdita di dati sensibili e coadiuvando il raggiungimento ed il mantenimento della conformità alle diverse compliance normative. Permette di scansionare il body delle mail per rilevare, riscrivere o bloccare eventuali URL che fanno riferimento a campagne di phishing e vengono rilevati attraverso la categorizzazione dei FortiGuard Labs o attraverso l'analisi avanzata in sandboxing. È possibile applicare un intero servizio di URL filter in modo da poter verificare anche ulteriori categorie a rischio Security.
  FortiMail combina funzionalità **antispam multilivello**, un potente motore **antimalware** e diverse funzionalità aggiuntive quali **Data Leak Prevention** (DLP), **Identity Based Encryption** (IBE), archivio mail e **anti-blocklisting** all'interno di un'unica soluzione integrata. La soluzione FortiMail è stata spesso oggetto del **premio VBSpam**, a testimonianza di un'altissima percentuale di rilevamento a fronte di un bassissimo numero di falsi positivi.

11.1. ORGANIZZAZIONE DEI SERVIZI, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il servizio SWG&SEG proposto dal RTI viene erogato dal Centro Servizi del RTI. Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**) conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici

e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT** (**SGS-IT**) conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

Organizzazione del servizio

L'organizzazione del servizio SWG&SEG si sviluppa nelle fasi di seguito riportate.

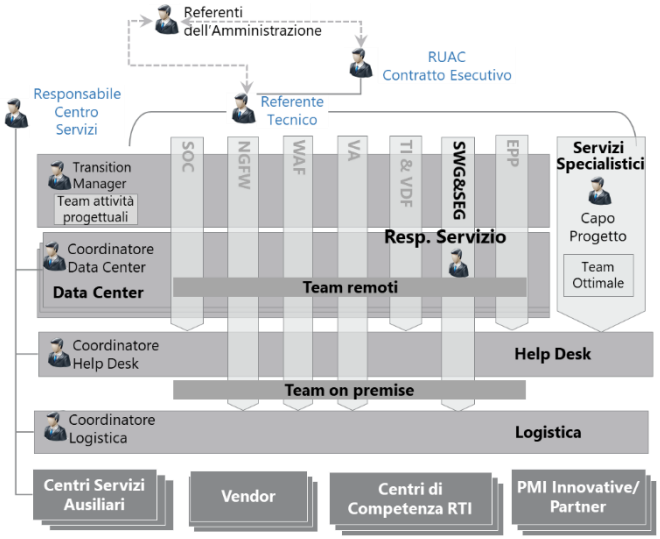

Figura 29 – Organizzazione del servizio SEG&SWG

Presa in carico del servizio:

- *acquisizione*, attraverso il *Team on-premise* (cfr. § 4), di know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione, delle relative modalità operative, delle linee guida e metodologie in uso presso l'Amministrazione;
- predisposizione e configurazione del servizio e delle relative piattaforme di management:
  - Il *SWG&SEG Team* attiva il servizio dedicato all'Amministrazione su ciascuna delle piattaforme di gestione del servizio descritte precedentemente. Attiva inoltre il servizio SEG (erogato dal Centro Servizi) secondo quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano;
  - Il *Team on-premise* gestisce l'installazione delle componenti previste on-site secondo il piano di installazione condiviso con l'Amministrazione. Gli apparati SWG saranno resi raggiungibili, presi in carico dal sistema di management e configurati da remoto. Il servizio sarà predisposto sulla base di quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano;
  - se necessario, il *Team on-premise* ed il SWG&SEG *Team* gestiscono il processo di migrazione secondo quanto stabilito nel piano di migrazione.

Erogazione del servizio:

- *Monitoraggio della disponibilità*: gli operatori dell'Help Desk di 2° livello monitorano il servizio attraverso la console gestiscono gli allarmi o in autonomia o coinvolgendo il supporto di 3° livello;
- *Richieste di modifica delle configurazioni*: L'Amministrazione potrà aggiornare le politiche di sicurezza utilizzando il portale dei servizi di sicurezza in modalità self-ticketing (in caso di contestuale acquisizione del servizio SOC) o mediante l'apertura di un ticket. La richiesta sarà preso in carico dal team specialistico SWG&SEG che, una volta effettuate le necessarie attività, provvederà al collaudo della modifica congiuntamente con il personale preposto dall'Amministrazione;
- *Reporting*: La reportistica permette di verificare la conformità agli standard scelti e il livello di protezione delle applicazioni. Prevede report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.
- *supporto alla gestione incidenti*: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

Modalità di erogazione

La soluzione verso un modello di erogazione composto da due sotto-servizi, uno dedicato alla protezione della navigazione Internet (SWG) ed uno dedicato alla protezione della posta elettronica (SEG).

La modalità di erogazione del servizio prevede due diversi scenari per entrambi i sotto-servizi in ambito: ✓installazione di appliance dedicati fisici o virtuali on premise presso la sede dell'Amministrazione o presso il proprio Virtual Private Cloud; ✓utilizzo di istanze del sotto-servizio installato presso il Centro Servizi del RTI ed acceduta in modalità SaaS. L'architettura di default proposta dal RTI è quella on premise per il sotto-servizio SWG e SaaS presso il Centro Servizi del RTI per il sotto-servizio SEG.

In fase di definizione del progetto esecutivo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono: ✓numerosità di utenti; ✓dislocazione del mail server; ✓stima traffico generato.

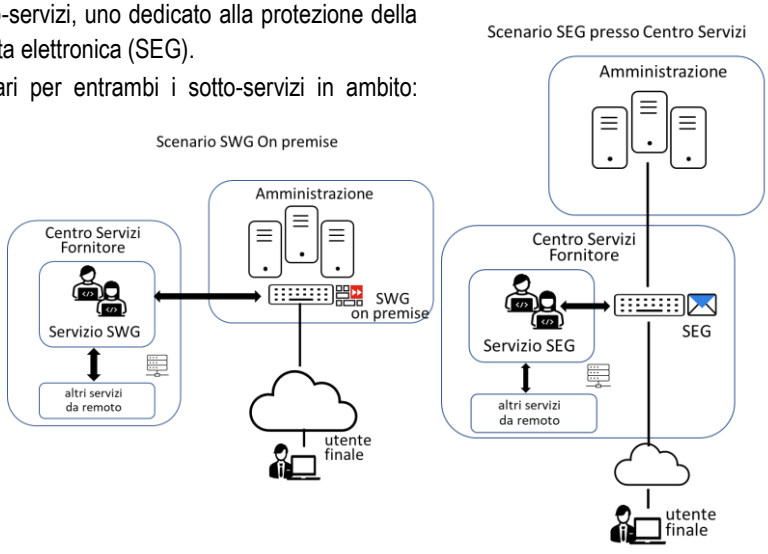

Figura 30 – Modalità di erogazione SEG&SWG

Interazioni

Si riportano di seguito le interazioni principali del Servizio Protezione Navigazione Internet e Posta Elettronica verso gli altri servizi: ✓**Interazione con il servizio Security Operation Center L1.S1**: (cfr. § 6.2 sezione interazioni); ✓**Interazione con il servizio Next Generation Firewall**

L1.S2: (cfr. § 6.2 sezione interazioni); ✓**Interazione con il servizio Web Application Firewall L1.S3**: (cfr. § 7.3 sezione interazioni); ✓**Interazione con il servizio Threat Intelligence & Vulnerability Data Feed L1.S5:** (cfr. § 6.2 sezione interazioni); ✓**Interazione con il servizio Protezione degli End Point L1.S13**: (cfr. § 6.2 sezione interazioni).

11.2. CAPACITÀ DEL SERVIZIO DI PROTEZIONE INTERNET DI "DEEP INSPECTION"

Il servizio di Protezione Navigazione Internet include funzionalità avanzate di Stateful Filtering e "Deep Inspection", che permettono di applicare feature di AV, Application Control e Web Filtering anche su comunicazioni protette da protocolli cifrati. Infatti, l'encryption SSL/TLS, utilizzata dal protocollo HTTPS per proteggere la sessione del client verso una web application, viene spesso sfruttata in maniera malevola per nascondere il payload (spesso malware, anche di tipo ransomware) all'interno del tunnel cifrato, bypassando il controllo del SWG. La funzionalità di SSL Deep Inspection consente di effettuare il parsing dei pacchetti transitanti in chiaro (ovvero decodificati) e quindi la possibilità di esaminare l'eventuale traffico malevolo o comportamenti malevoli pur conservando intatta la sicurezza della sessione di comunicazione.

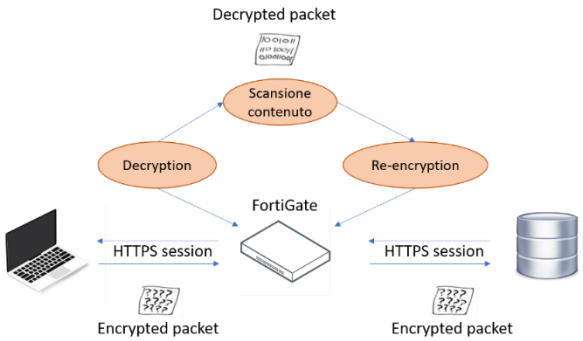

Figura 31 – Deep Inspection

Come si evince, il SWG Fortigate si pone in modalità proxy per poter effettuare la scansione avanzata, di tipo Store&Forward che, per una maggiore efficacia nella rilevazione dei malware, attende che il download del file sia completo prima di analizzarlo con gli engine di sicurezza. Tale operazione viene eseguita in real time direttamente in hardware, utilizzando dei processori ASIC ottimizzati, in modalità del tutto trasparente sia per il client che per il server (infatti, il SESSION ID, la tipologia di encryption etc., rimangono inalterati).

Gli engine di sicurezza utilizzano sia tecniche di scansioni malware "**Signature Based**", sia tecniche di **Sandboxing "Behaviour Based"**. Le tecniche di scansione "Signature Based" utilizzano la Suite di sicurezza AMP (Advance Malware Protection), specifica per la rilevazione Antimalware, che comprende le seguenti funzionalità:

- **Antivirus/AntiBotnet**: la funzionalità di Antivirus/Antimalware permette l'ispezione del traffico su base Signature e su base euristica, permettendo l'identificazione delle minacce più avanzate e l'identificazione di botnet e server Command&Control tipici di architetture di Distributed Denial-of-Service Attacks. Molto spesso i motori Antivirus basati su signatures, pur se queste sono costantemente aggiornate, sono poco efficaci quando i file malevoli vengono intenzionalmente modificati (per evitare di creare un malware ex-novo) con il solo scopo di alterarne la signature (questa pratica viene identificata come polimorfismo) allo scopo di eludere il controllo: la soluzione proposta dal RTI, basata sulla tecnologia Fortinet, utilizza il brevetto Compact Pattern Recognition Language che permette di rilevare un perimetro di polimorfismi da una signature base, rendendo più efficace l'utilizzo delle firme antimalware;
- **Mobile Security**: La funzionalità permette di protegge efficacemente i propri client dalle ultime minacce destinate a colpire in maniera specifica i device mobili, sempre più diffusi in contesti aziendali in linea con il fenomeno BYOD;
- **Virus Outbreak Protection**: questo servizio offre uno strato aggiuntivo di protezione mirato ai nuovi Malware appena nati e a fermare i rapidi attacchi virali, perché di solito occorrono almeno alcune ore per sviluppare e installare le firme; per questo scopo viene utilizzato in tempo reale il DB di checksum delle minacce appena rilevate prima che siano disponibili le firme AV;
- **Content Disarm and Reconstruction**: con questo servizio, il motore AV può rimuovere tutto il contenuto attivo in tempo reale rilasciando all'utente il file "disarmato", come ad esempio macro all'interno di file word oppure collegamenti ipertestuali all'interno di file pdf (le Macro contenute all'interno dei file Word, Excel, PowerPoint etc. rappresentano uno dei 5 modelli di trasmissione dei Virus più utilizzati).

Le tecniche di scansione di tipo "**Behaviour-based**" vengono invece effettuate attraverso la Appliance Sandbox. La Sandbox permette di massimizzare la protezione dalle minacce zero-day, APT, Ransomware (ad esempio Cryptolocker, WannaCry, CryptoWall, etc.). A differenza di altre soluzioni presenti sul mercato, la FortiSandbox è una soluzione basata su MITRE ATT&CK che sfrutta l'Intelligenza Artificiale (AI) e l'apprendimento automatico (Machine Learning - ML) per analisi statiche e dinamiche dei malware. FortiSandbox applica l'AI durante l'intero processo di sandboxing, miscelando analisi sia statica che dinamica per apprendere in modo adattivo i nuovi comportamenti del malware e migliorare l'efficacia del rilevamento delle minacce zero-day. La FortiSandbox permette la detonazione anche dei malware di ultima generazione che sono in grado di disattivarsi quando vengono eseguiti in un contesto virtuale e quindi eventualmente in un LAB specifico per l'analisi (ispezione dell'OUI dei Mac Address delle vNIC delle VM, verifica sui movimenti del mouse che se assenti denotano sicuramente una macchina di laboratorio senza presenza umana, verifica della presenza o meno di un'interfaccia di rete attiva). In funzione dello specifico profilo di sicurezza selezionato, il processo di scansione approfondita del codice terminerà validandone la non pericolosità oppure spostando il malware in quarantena, dandone opportuna comunicazione all'utente. Coerentemente con l'approccio Security Fabric la Sandbox mette a disposizione dei dispositivi connessi l'elenco dei file e delle URL malevole.

11.3. CAPACITÀ DEL SERVIZIO DI PROTEZIONE INTERNET DI DISCOVERY DI ACCESSI AD APPLICAZIONI IN CLOUD (SAAS)

In generale, un SWG operante in modalità 'stateful' lavora con policy/rules costruite sui primi 4 livelli del modello ISO/OSI. Ciò implica che la caratterizzazione del traffico da autorizzare o bloccare è legata principalmente al socket di sessione (IP sorgente, IP di destinazione, porta sorgente e porta di destinazione). Tuttavia, ad applicazioni fruite in Cloud in modalità SaaS (es. Microsoft Office 365), possono corrispondere un insieme piuttosto ampio di indirizzi IP, porte e protocolli da abilitare o bloccare per mezzo di un firewall perimetrale. In tale contesto, la difficoltà di gestione è legata non solo alla quantità dei parametri di rete considerati, che possono assumere simultaneamente decine o centinaia di valori differenti, ma anche alla loro variabilità: si pensi agli indirizzi IP che possono cambiare in base allo spostamento geografico degli ambienti Cloud del Vendor SaaS, all'acquisto o cessione di porzioni di subnet pubbliche, all'utilizzo di tecniche di NAT, etc.). Tale problematica, se non opportunamente indirizzata, potrebbe condurre ad un filtraggio del traffico solamente parziale, lasciando accessibili servizi SaaS che potrebbero rappresentare una possibile breccia di sicurezza, ampliando in conseguenza la possibile superficie di attacco. La soluzione proposta dal RTI supera tale problematica mediante l'impiego di un **Internet Service Database** costantemente aggiornato in maniera automatica e capace di gestire 1.500 applicazioni Cloud SaaS in termini di indirizzi IP, porte e protocolli utilizzati.

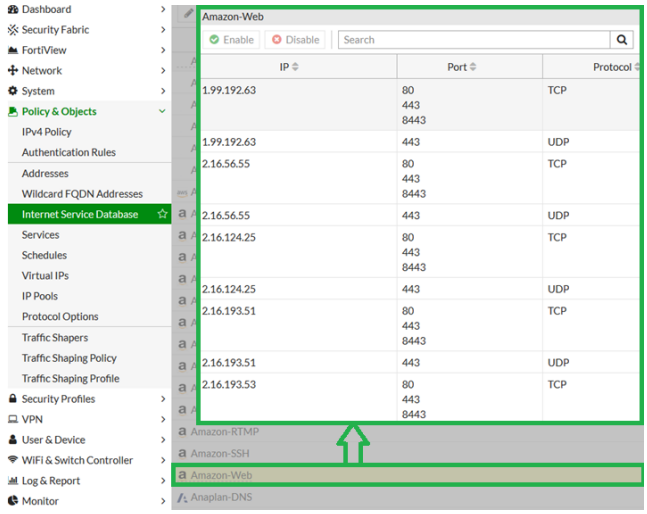

Figura 32 – ISDB

Attraverso l'utilizzo di questo Database è possibile effettuare la Discovery di accessi ad applicazioni in Cloud ed applicare un meccanismo di white/black-listing per consentire/impedire l'accesso ai soli servizi in Cloud censiti. Qualora un'applicazione in Cloud sia ritenuta non conforme alle policy aziendali è possibile negarne agli utenti l'accesso attraverso la definizione di una specifica Proxy Policy che ha, come campo destinazione, il servizio SaaS censito nell'Internet Service Database (ISDB).

È possibile, inoltre, consentire l'accesso all'applicazione SaaS prevedendo tuttavia controlli granulari delle Feature applicative utilizzabili dagli utenti. Le funzionalità avanzate di Application Control e Web Filtering, consentite dall'impiego dell'Internet Service Database, permettono di ottenere efficacemente delle Proxy Policy molto granulari, consentendo inoltre una caratterizzazione dei servizi e delle applicazioni sempre aggiornata. Tali policy possono essere applicate a degli host identificati mediante indirizzo IP oppure direttamente ad un'utenza di rete specifica (Layer 8 – Livello USER).

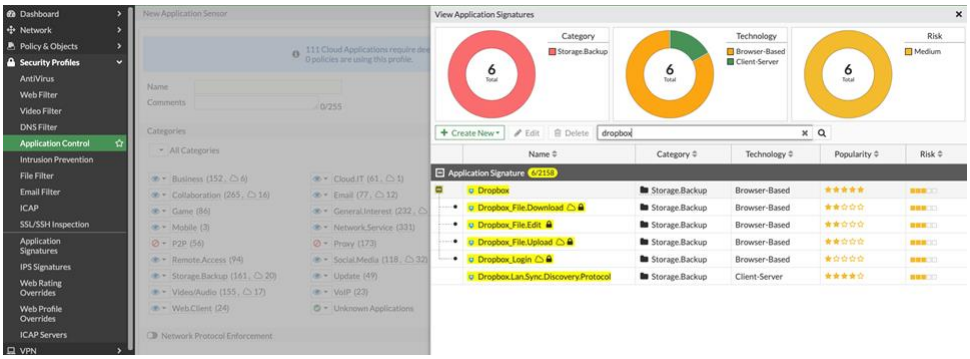

Figura 33 – Interfaccia SWG

Nella Proxy Policy relativa all'applicativo SaaS, è possibile applicare uno specifico profilo di "Application Control", per raffinare ulteriormente il filtering. Ad esempio, qualora un'Amministrazione abbia intenzione di filtrare l'accesso ad un servizio di file sharing SaaS, è possibile definire nel profilo di Application Control della relativa Proxy Policy, dei permessi specifici inerenti la gestione dei file per consentire o negare esplicitamente il download, l'editing o l'upload dei file.

Come menzionato precedentemente, Internet Service DB viene aggiornato automaticamente per cui si avrà, al momento della stesura di una Proxy Policy, la possibilità di utilizzare direttamente l'Internet Service già censito, oppure realizzare dei Custom Service andando a specificare i seguenti campi: ✓IP o IP Range; ✓Protocol Number; ✓Porta o Range di porte; ✓Reputation.

Infine, è possibile anche realizzare una Extension Internet Service che dia la possibilità di aggiungere o rimuovere IP address da un Predefined Internet Service, aggiungere o rimuovere porte etc.

12. PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA" - FUNZIONALITA' AGGIUNTIVE

Si conferma la presenza di "funzioni di protezione della posta anti-phishing e anti-ransomware" con riferimento al servizio di "protezione navigazione internet e posta elettronica" (cfr. cap.6, 11 e §11.2).

13. PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE DEGLI END POINT"

Il servizio di Protezione degli Endpoint ha la finalità di proteggere gli strumenti di lavoro del personale delle Pubbliche Amministrazioni da possibili attacchi informatici che possano sfruttare l'endpoint quale vettore preferenziale verso il Sistema Informativo della PA. Il RTI ha maturato una consolidata esperienza nell'erogazione di servizi di protezione degli endpoint sia nel comparto della Pubblica Amministrazione che nel mondo privato ed una profonda conoscenza ed esperienza sulla tecnologia Trend Micro proposta per questa fornitura, comprovata da numerose **certificazioni delle risorse** ed una **partnership di tipo GOLD.** La soluzione proposta dal RTI oltre a rispettare pienamente i requisiti del Capitolato, presenta una serie di caratteristiche tecnologiche e prestazionali migliorative come meglio descritto nel seguito. Specificatamente, per l'erogazione del servizio di protezione degli endpoint, il RTI adotta la tecnologia Trend Micro Apex One, una soluzione ideata per la protezione degli endpoint da molteplici virus quali ransomware, trojan e altri malware specifici, che consente anche di controllarne ed impedirne la diffusione all'interno della rete. Inoltre, la soluzione tecnologica Apex One di Trend Micro è leader

all'interno del Magic Quadrant di Gartner per le piattaforme di protezione degli endpoint nel 2021. Si evidenzia che come richiesto dal capitolato il servizio è erogato totalmente dal Centro Servizi del RTI senza la necessità di utilizzare componenti nel cloud del vendor.

Trend Micro, grazie alla "Zero Day Initiative", è il primo Vendor in assoluto in termini di ricerca di nuove vulnerabilità con migliaia di scoperte ogni anno. La tecnologia proposta beneficia di queste informazioni con significativo anticipo rispetto alla concorrenza e, grazie al Virtual Patching, è in grado di proteggere i dispositivi fin dal primo istante dalla scoperta senza dover attendere una patch ufficiale da parte del produttore.

A questo riguardo il servizio è progettato per operare con la massima efficacia sia come singolo servizio sia, come meglio specificato nel seguito del presente capitolo, mediante l'**interazione in forte sinergia con gli altri servizi** della fornitura.

Figura 34 – EPP Gartner Magic Quadrant

13.1. FUNZIONALITÀ AGGIUNTIVE E CARATTERISTICHE TECNOLOGICHE MIGLIORATIVE

Il servizio proposto dal RTI prevede l'utilizzo della piattaforma basata sulla tecnologia Trend Micro Apex One installata presso il Centro Servizi.

I componenti principali della soluzione sono:

- **Apex Central:** fornisce attraverso una console centralizza la visibilità ed il controllo per gestire, monitorare e creare policy di sicurezza. Attraverso l'uso di dashboard personalizzabili è inoltre possibile visualizzare e valutare in tempo reale lo stato di sicurezza degli endpoint dell'Amministrazione, rilevare eventuali utenti a rischio, identificare le minacce e rispondere agli incidenti. La visibilità può essere effettuare su base utente (eventualmente anche mediante integrazione con Active Directory) e consente di monitorare cosa accade sui dispositivi, permettendo così di accedere alle policy in maniera granulare e apportarvi modifiche.
- **Apex One Server**: la componente specifica destinata alla singola Amministrazione contraente che controlla operativamente i singoli agent installati sui rispettivi endpoint.
- **Security Agent:** agent installati su ciascun endpoint che permettono di eseguire le operazioni di controllo e verifica degli oggetti malevoli nonché di applicare localmente tutte le policy di sicurezza previste.
- **Deep Discovery Analyzer**: fornisce le funzionalità di sandbox per la *detonazione* degli oggetti potenzialmente malevoli.

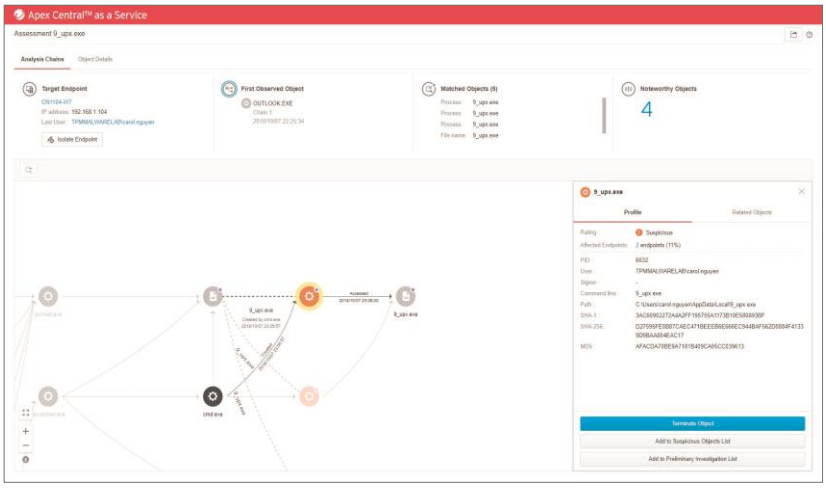

Figura 35 – Console di gestione Apex Central

La soluzione proposta dal RTI introduce alcuni elementi migliorativi rispetto ai requisiti minimi del Capitolato Tecnico che consentono di innalzare ulteriormente la postura di sicurezza degli endpoint dell'Amministrazione contraente.

Tutti gli endpoint vengono dotati di un agent in grado di erogare tutte le funzionalità messe a disposizione dalla tecnologia sinteticamente riportate nella figura seguente.

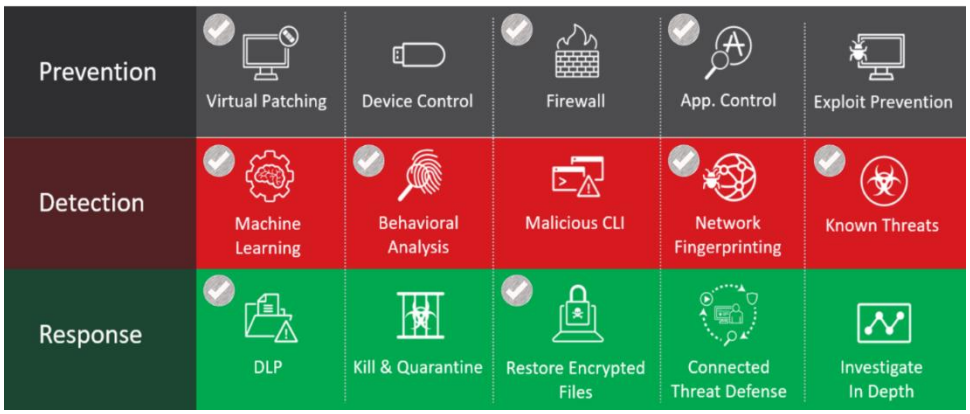

Figura 36 – Matrice delle funzionalità di Apex One

Le funzionalità che si caratterizzano come migliorative rispetto ai requisiti minimi sono evidenziate con una spunta nella figura e descritte di seguito:

- **Virtual Patching e Firewall**: La soluzione offre una protezione avanzata e preventiva degli endpoint mediante l'integrazione di patch virtuali a fronte di vulnerabilità note e sconosciute. Un motore dedicato monitora costantemente il traffico alla ricerca di eventuali attacchi zero-day e nuove vulnerabilità specifiche utilizzando i filtri del sistema di prevenzione dalle intrusioni (IPS) basato su host. In questo modo è possibile rilevare deviazioni del protocollo di rete o contenuti sospetti

che segnalano un attacco o violazioni dei criteri di sicurezza. Se vengono rilevate minacce, la soluzione impedisce che queste vulnerabilità vengano sfruttate grazie all'utilizzo di filtri prontamente distribuiti sugli agent che offrono una protezione completa prima che le patch possano essere distribuite o siano disponibili. Apex One detiene centinaia di regole IPS, regolarmente aggiornate tramite l'analisi dei laboratori di ricerca e della Zero Day Initiative (ZDI), grazie alle quali è in grado di fornire le soluzioni più idonee all'endpoint.

- **Application Control:** al fine di evitare che i singoli endpoint possano essere utilizzati quali trampolino di lancio per l'esecuzione di software malevolo, è inibita l'esecuzione di applicazioni indesiderate, sconosciute e potenzialmente dannose. Il controllo dell'esecuzione delle applicazioni viene realizzato attraverso la combinazione di vari criteri dinamici, di funzionalità di "whitelisting/blacklisting" e di un vasto catalogo di applicazioni.
  Tutti questi elementi vengono configurati e combinati direttamente dalla console centralizzata consentendo una gestione granulare per ogni singola Amministrazione contraente, oltre che per unità organizzativa o per singolo utente.
- **Machine Learning e Behavior Analysis**: Alle tradizionali tecniche anti-malware è affiancato un motore di nuova generazione che include analisi comportamentale e meccanismi di machine-learning predittivi. L'approccio basato sul Machine learning, applicato prima e durante l'esecuzione dei file, unito a tecniche di *cancellazione del rumore*, ha l'obbiettivo di ridurre drasticamente i falsi positivi. L'analisi comportamentale risulta efficace contro tecniche di injection, ransomware e attacchi alla memoria o al browser.
- **Network Fingerprinting**: La funzionalità permette di monitorare il traffico di rete sull'endpoint alla ricerca di pattern noti al fine di identificare possibili comunicazioni originate da oggetti malevoli.
- **Known Threats**: La soluzione beneficia dell'accesso alla vasta fonte di intelligence fornita dalla Smart Protection Network di Trend Micro, alimentata da più di 3500 ricercatori nel mondo con centinaia di terabyte analizzati giornalmente. Ciò consente di mantenere una protezione metodicamente aggiornata con migliaia di informazioni su zero-days e minacce. Tutte le informazioni raccolte ed elaborate dagli analisti vengono rese disponibili ad Apex One sottoforma di oggetti come URL, IP, Domini, File, Network Pattern, Firme e altri. La fase di analisi e risposta a fronte di eventuali minacce è supportata dalle informazioni fornite dalla Smart Protection Network, che facilitano la comprensione della natura di un oggetto analizzato. Inoltre, sulla base di un comportamento noto all'intelligence, è possibile ottenere un riscontro automatico sulle tecniche di attacco utilizzate (MITRE ATT&CK), e sul dataset di informazioni presenti nel database globale delle minacce.
- **Data Loss Prevention (DLP)**: La protezione DLP, integrata nell'agent endpoint, consente di avere visibilità e controllo dei dati sia "at rest" che "in transit" oltre che prevenirne la perdita.
  Mediante la console di gestione è possibile sia determinare la natura di un dato da proteggere indicandolo in termini di parole chiave, attributi di file o di regular expression, sia creare un template composto da più "Data Identifiers" garantendo granularità nell'identificazione dell'informazione da monitorare.
  Grazie ad un approccio basato su policy è possibile assegnare ad ogni utente o gruppo di utenti un set di regole DLP composte da: ✓*Template*: modello di regola preconfezionato o personalizzato che determina la natura del dato da monitorare e/o proteggere ✓*Canale*: la selezione degli ambiti di applicazione della policy con la possibilità di scegliere il flusso del dato da monitorare su canali specifici (Email, Web, FTP, SMB, Peer To Peer, USB, Clipboard, Stampanti, etc.) ✓*Azione*: scelta dell'azione da intraprendere quando un dato trova riscontro nella policy. Azioni possibili sono il logging, il blocco della trasmissione, il consenso alla trasmissione dietro giustificazione e la registrazione del dato. Inoltre è possibile gestire le notifiche agli utenti tramite pop-up del software agent.
- **Restore Encrypted Files**: il comportamento dei ransomware segue un modello noto finalizzato a cifrare, rendendo inaccessibili, i file sugli endpoint. Il motore di analisi comportamentale effettua il backup predittivo dei file potenzialmente oggetto di attacco, la funzionalità di Restore Encrypted Files permette di ripristinare i file cifrati da un malware subito dopo la sua identificazione, recuperandone i contenuti dal backup.

13.2. PROTEZIONE DALLE MINACCE WEB AVANZATE "ZERO-DAY" TRAMITE ISOLAMENTO REMOTO DEL BROWSER

La piattaforma presente nel Centro Servizi per la protezione degli endpoint è dotata di componenti tecnologiche dedicate con capacità avanzata per proteggere i dati dell'Amministrazione contraente dalle minacce veicolate attraverso la navigazione sul Web. Il sistema ha la capacità di monitorare l'uso degli endpoint alla ricerca di oggetti malevoli al fine di prevenirne l'azione e la diffusione. L'identificazione di **oggetti sospetti, comprensivi delle URL di navigazione del browser,** ne consente l'invio all'ambiente isolato, sandbox, per un'analisi avanzata utilizzando diversi metodi di rilevamento. Nel momento in cui viene rilevata dalla analisi della sandbox una minaccia, gli agent installati sugli endpoint recepiscono automaticamente l'IOC e/o la signature per intraprendere le azioni di rilevamento, blocco, quarantena o eliminazione dell'oggetto. La sandbox consente agli amministratori di accedere ad una reportistica dettagliata con la descrizione delle diverse fasi dell'attacco rilevato, riportando ogni singola azione effettuata dall'oggetto malevolo di tipo zero-day quali, per esempio, comandi powershell eseguiti, file o chiavi di registro modificate, chiamate URL verso l'esterno.
Le ulteriori funzionalità a supporto della detection delle minacce web avanzate "zero-day" sono le seguenti:

1. **Analisi avanzata:** La sandbox utilizza immagini virtuali personalizzabili, coincidenti con i sistemi operativi da analizzare, che contengono configurazioni, driver, applicazioni, versioni e linguaggi. Questo approccio aumenta drasticamente la capacità di rilevazione di minacce avanzate, comprese quelle che tentino l'evasione dagli ambienti sandbox più comuni.
   La stessa ha accesso internet esterno sicuro tale da permetter l'identificazione di minacce multi-stage, download, URL, Command and Control (C&C) e altro. Inoltre, la soluzione permette il caricamento manuale di artefatti da parte degli amministratori.

2. **Rilevazione malware:** Viene eseguita con tecniche di analisi statica, euristica, comportamentale, web e file reputation consentendo la rilevazione su numerosi tipi di file quali, a titolo di esempio non esaustivo: documenti, file compressi, oggetti dinamici, contenuti web, script e URL. La soluzione è in grado di *detonare* oggetti anche su ambienti **Android** (mobile, IoT, Automotive).
3. **Rilevazione ransomware:** La capacità di rilevazione e blocco, consente di identificare e stoppare attività legate ad attacchi Ransomware. Sfruttando un mix di tecniche composte da analisi statica, dinamica ed euristica (behaviour analysis, pattern analysis, verifiche reputazionali e sandbox per oggetti sospetti), il motore di analisi comportamentale analizza le attività eseguite dal sistema e ne valuta le reali intenzioni per ricercare minacce potenzialmente insediate negli asset.

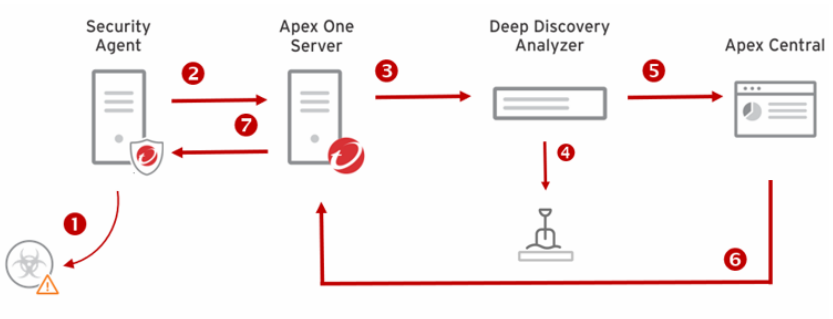

Figura 37 – Workflow del contrasto alle minacce tramite sandbox

La figura illustra le fasi di contrasto alle minacce attraverso l'uso della sandbox.
L'agent rileva una potenziale minaccia (**1**) e la invia all'Apex One Server (**2**). Il potenziale malware o url viene quindi inviato al modulo di esecuzione nella Sandbox Deep Discovery Analyzer (**3**), dove, all'interno della sandbox, viene fatto *detonare* e viene analizzato il suo comportamento (**4**). L'esito dell'analisi viene notificato sulla console (**5**) che istruisce l'Apex One Server sulle modalità di protezione da attuare (**6**). In ultimo l'Apex One Server istruisce gli agent installati sugli endpoint sulle operazioni da eseguire (**7**).
Nella figura a fianco è rappresentato un dettaglio dell'esecuzione nella sandbox di una url eseguita in automatico tramite le fasi del processo sopra descritte.

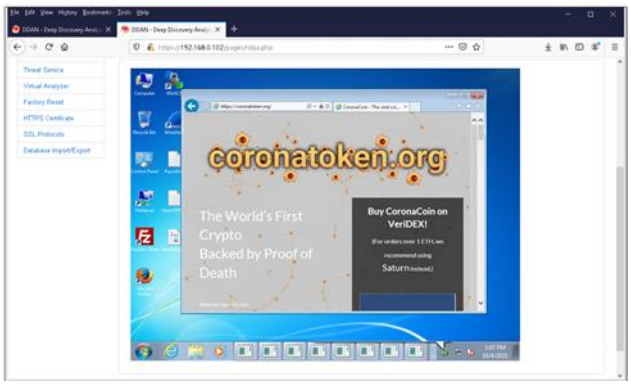

Figura 38 – Esempio di esecuzione nella sandbox

13.3. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI.

Il Servizio di protezione degli endpoint, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**) conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT** (**SGS-IT**) conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management). L'organizzazione del servizio EPP si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- **Assessment degli endpoint**: si procede con il censimento di tutti i dispositivi fissi (postazioni di lavoro) e mobile (Laptop, Smartphone, etc…) in uso presso l'Amministrazione nel perimetro del servizio. Per ciascuno dei dispositivi individuati viene verificata la compatibilità con la soluzione tecnologica in uso. Inoltre, in questa fase, viene identificato in dettaglio lo stato dei sistemi logici, fisici e virtuali, acquisendo tutte le informazioni relative anche agli apparati di sicurezza presenti.
- **Pianificazione delle installazioni:** A valle dell'assessment e delle verifiche di compatibilità si procede con la pianificazione dell'installazione degli agent di Endpoint protection su ciascun dispositivo rilevato secondo le priorità identificate in accordo con l'Amministrazione.

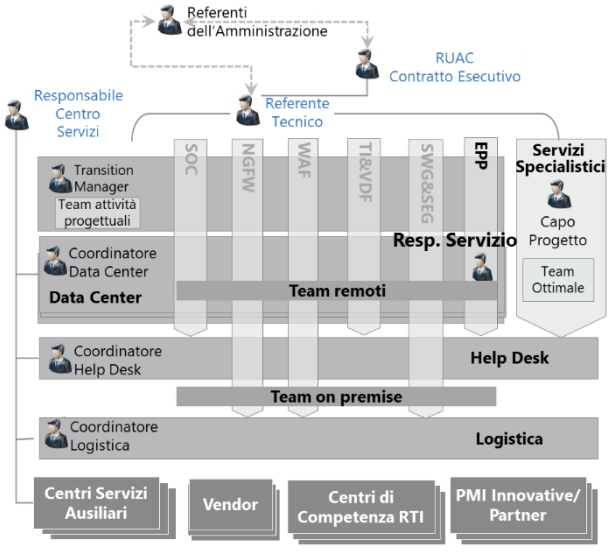

Figura 39 – Organizzazione del servizio EPP

Erogazione del servizio:

- **Implementazione delle policy di sicurezza:** la soluzione tecnologica implementerà le policy di sicurezza dell'Amministrazione in conformità a quanto disposto per i dispositivi connessi alla rete, come ad es. utilizzo di un sistema operativo approvato, installazione di una VPN o l'esecuzione di un software antivirus aggiornato.
- **Installazione degli agent:** La procedura di installazione viene concordata congiuntamente con l'Amministrazione. La procedura di installazione può prevedere anche la rimozione di un antivirus eventualmente già presente sulle postazioni, al fine di evitare finestre temporali in cui i dispositivi non siano coperti dalla protezione o conflitti tra i due strumenti di protezione. Ove si renda necessario, ad esempio per il numero elevato di endpoint, è possibile creare, in accordo con l'Amministrazione, un ambiente di staging per eseguire la fase pilota del servizio e dove replicare configurazione particolari che richiedano un tuning della configurazione.
- **Attivazione del Servizio:** Attivazione del servizio per tutti gli endpoint censiti in accordo con il piano di rollout condiviso con l'Amministrazione.
- **Conduzione operativa**: la conduzione della soluzione tecnologica riguarda tutte le fasi del ciclo di vita del servizio e si sostanzia nelle seguenti attività: ✓Gestione centralizzata; ✓Conduzione applicativa; ✓Manutenzione ordinaria della piattaforma; ✓Attivazione dei nuovi sistemi con le corrette policy

di pertinenza; ✓eventuale deprovisioning dell'agent; ✓Tuning delle configurazioni; ✓Monitoraggio e gestione di eventuali malfunzionamenti degli agent.

- **Produzione della Reportistica**: Vengono prodotti periodicamente dei report per l'Amministrazione finalizzati all'individuazione della diffusione di malware o di eventi sospetti che richiedono un approfondimento. I report vengono realizzati sulla base di una serie di template standard definiti in fase di progetto esecutivo.
- **Supporto alla gestione incidenti**: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

La piattaforma eroga i propri servizi verso la rete dell'Amministrazione ma rende possibile l'ulteriore erogazione anche attraverso internet per garantire la copertura dei device anche quando non sono fisicamente collegati dall'interno delle infrastrutture dell'Amministrazione. La comunicazione via internet è corredata da funzionalità di firma e cifratura dei dati scambiati che ne garantiscono la sicurezza.

Per ciascuna Amministrazione contraente viene configurato un Apex One Server dedicato presso l'Amministrazione. In sede di progettazione della soluzione, per ogni singola Amministrazione, è possibile prevedere ulteriori livelli di segregazione tali da garantire la presenza di apparati di frontiera che separino le reti delle amministrazioni rispetto al Centro Servizi. Tutti i sistemi e le applicazioni coinvolte subiscono un regolare processo di aggiornamento periodico sulla base delle distribuzioni delle patch rese disponibili dai vendor.

La figura illustra l'architettura di alto livello proposta.

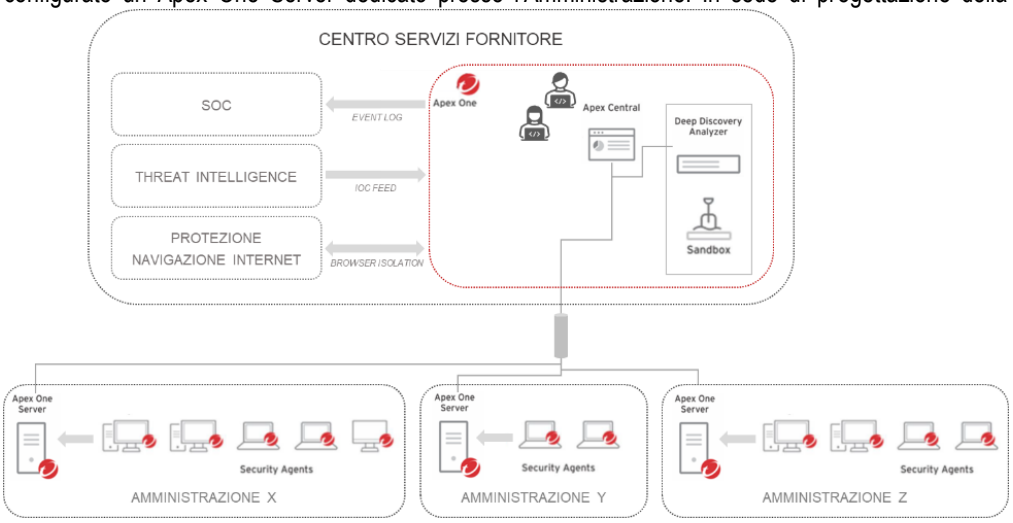

Figura 40 – Architettura del servizio di Protezione degli Endpoint

Si riportano di seguito le **interazioni** principali del Servizio Protezione End Point verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: (cfr. § 6.2 sezione interazioni).
- **Interazione con il servizio Next Generation Firewall L1.S2**: (cfr. § 6.2 sezione interazioni).
- **Interazione con il servizio Web Application Firewall L1.S3**: (cfr. § 6.2 sezione interazioni).
- **Interazione con il servizio "Threat Intelligence & Vulnerability Data Feed" L1.S5**: (cfr. § 10.3 sezione interazioni).
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6**: (cfr. § 6.2 sezione interazioni).

14. PROPOSTA PROGETTUALE PER IL SERVIZIO "FORMAZIONE E SECURITY AWARENESS"

Una strategia efficace di prevenzione di attacchi di natura cyber prevede l'implementazione di **iniziative formative a carattere innovativo** allo scopo di promuovere comportamenti in linea con i principi e gli obiettivi di sicurezza informatica. L'incremento della **consapevolezza** e della **sensibilità** degli utenti si posiziona quale **obiettivo strategico** per contrastare potenziali minacce informatiche e preservare il patrimonio informativo delle Amministrazioni. In tale contesto il RTI propone un Servizio di "Formazione e Security Awareness" efficace ed efficiente, **caratterizzato da numerosi elementi a valore aggiunto, migliorativi rispetto ai requisiti minimi di gara,** che il RTI è in grado di offrire grazie all'utilizzo di approcci metodologici innovativi riconosciuti a livello nazionale ed internazionale; alle numerose esperienze maturate dal RTI; alle competenze messe a disposizione anche mediante il coinvolgimento dei Centri di Ricerca/Competenza e partnership tecnologiche; all'utilizzo di strumenti e tecniche di apprendimento innovative.

14.1. METODOLOGIE E COMPETENZE MESSE A DISPOSIZIONE

Il fattore umano è ancora oggi un elemento chiave della sicurezza rispetto ai rischi e alle minacce cyber. Per questo, il RTI ritiene che il miglior "firewall umano" sia l'investimento nella formazione e nella sensibilizzazione degli utenti e ha dunque consolidato un approccio didattico basato su **attività formative sinergiche ed eterogenee** volte a incrementare l'attenzione e le competenze necessarie per prevenire e riconoscere potenziali minacce cyber.

Nello svolgimento di tali attività, il RTI fa principalmente riferimento alle **metodologie** ed agli **approcci innovativi** già adottati e largamente validati per attività analoghe in Italia e nel contesto internazionale del suo network.

Le **attività di formazione** sono suddivise in **diverse sessioni**, catalogate per area tematica. Dal punto di vista operativo, ogni fase progettuale prevede l'esecuzione delle seguenti attività:

1) **Pianificazione.** La prima fase del progetto mira a definire in dettaglio le attività, il gruppo di lavoro e i temi specifici da trattare. Il RTI predispone meeting e incontri con i referenti dell'Amministrazione per individuare i temi specifici e pianificare il materiale.
2) **Implementazione.** Formalizzazione del materiale predisposto, a seguito di una adeguata implementazione, per le sessioni di formazione sulla base delle indicazioni e delle scelte dei contenuti formativi fatti dalla stessa Amministrazione.
3) **Condivisione.** Le bozze dei contenuti formativi saranno valutate e approvate dagli organi predisposti dalla stessa Amministrazione dopo opportuna condivisione.

4) **Erogazione.** Il RTI erogherà il servizio attraverso le modalità previste, quali: sessioni di formazioni frontali e/o da remoto, divulgazione del materiale informativo in tema "Security Awareness", somministrazione dei test di verifica e sessioni di review.

Il RTI eroga il servizio di formazione in linea con l'**expertise**, la **seniority** e l'**interesse** dei partecipanti di ciascuna sessione. Ciascuna sessione è adeguata e calibrata secondo la platea di fruitori, garantendo così un significativo coinvolgimento dei partecipanti e una facile ed immediata trasmissione delle conoscenze. Al fine di garantire una efficace erogazione del servizio "Formazione e Security Awareness", il RTI mette a disposizione **specifiche figure professionali** con competenze adeguate maturate in molteplici esperienze pregresse di erogazione di servizi di formazione. Il RTI gode di una **comprovata esperienza** nel settore grazie alla molteplicità di corsi erogati a multinazionali e PMI, nazionali ed internazionali in molti settori: dal farmaceutico, chimico, energetico.

Particolarmente rilevanti sono gli accordi di collaborazione che il RTI ha già in essere con l'**International Institute for Counter Terrorism di Tel Aviv – Israele,** impegnato nella formazione specialistica sui temi della lotta al terrorismo, intelligence e protezione della sicurezza nazionale, e con la **Fondazione YMCA Italia**, con la mission di sostenere attività indirizzate allo sviluppo professionale, per l'erogazione di corsi specialistici di alta formazione su temi specifici in ambito Cyber Security e intelligence, avvalendosi anche di docenti internazionali di comprovata esperienza in contesti operativi sensibili.

Nell'ambito specifico, le figure identificate possiedono una conoscenza approfondita delle diverse tipologie di attacchi informatici, delle policy e linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. gestione del rischio, classificazione delle informazioni, gestione degli incidenti, utilizzo sicuro dei servizi informativi), delle tecniche di attacco e delle metodologie e degli strumenti operativi richiesti nell'ambito dell'Information e Cyber Security. Inoltre, sono previste all'interno del team figure in possesso delle **certificazioni CISM** (Certified Information Security Manager) e qualifica di **Lead Auditor ISO 27001**. Infine, il RTI ha definito un percorso di **formazione continua per il proprio personale** che prevede il conseguimento delle principali certificazioni internazionali in ambito Cyber Security e Information Security (CISA, CISM, CISSP, CSX, CEH, ISO27001, ISO22301, ITIL, COBIT, CIPM, CIPT, etc.). Il RTI garantirà le competenze/certificazioni sopra riportate anche attraverso **le collaborazioni con i Competence Center** (Cyber 4.0, etc.) che garantiranno formazione continua alle risorse del RTI coinvolte nei Contratti Esecutivi (cfr. cap. 17).

14.2. PROPOSTE INNOVATIVE, ADEGUATEZZA DEI CONTENUTI ED EFFICACIA DEGLI STRUMENTI PER L'EROGAZIONE DEL SERVIZIO

L'obiettivo del percorso formativo è quello di **trasmettere le competenze, le tecniche e i metodi necessari** per prevenire e reagire al meglio qualora si verifichi un incidente di sicurezza. Le competenze trasversali, quali la conoscenza dei rischi di sicurezza e il corretto uso dei dispositivi aziendali e personali, ricoprono oggi un ruolo cruciale nel mondo delle Amministrazioni.

Dal punto di vista contenutistico, il servizio di formazione prevede di trattare argomenti di complessità crescente. Questo approccio è in grado di garantire una maggiore assimilazione degli argomenti trattati da parte dei partecipanti e di garantire un'efficace costruzione della consapevolezza delle risorse (fattore umano e strumenti) e del loro utilizzo per ridurre la superficie di attacco e di conseguenza i possibili incidenti informatici. In particolare, il RTI garantisce la **copertura di argomenti di base**, come la protezione dei dispositivi personali e aziendali (es. computer, smartphone e tablet); la formazione del personale in merito **all'importanza e alla protezione delle credenziali d'accesso** (es. robustezza password) e la **salvaguardia dei propri dati e delle informazioni personali**; il **riconoscimento di tentativi di intrusione e truffa** (es. spam, phishing, social engineering); il **governo delle politiche di sicurezza**; l'**analisi del rischio**, anche in relazione alle metodologie AgID e le soluzioni di controllo e pratiche di prevenzione/risposta ad eventuali incidenti.

Figura 41 – Fasi Processo Formazione

Nello specifico, d'accordo con gli organismi, le figure preposte all'interno dell'Amministrazione e le esigenze evolutive dei corsi di formazione**,** il RTI potrà affrontare alcune tra le tematiche sopradescritte con particolare riferimento: ✓alle funzioni dei dispositivi aziendali e alle eventuali minacce e criticità ad essi associate; ✓all'approfondimento dell'importanza delle credenziali di accesso, le loro caratteristiche e i metodi per creare credenziali di accesso efficaci; ✓alle linee guida in merito all'utilizzo dei dispositivi aziendali on-site e in remote-working, d'accordo con gli organi preposti in merito e in linea con le policy dell'Amministrazione di riferimento; ✓all'importanza delle informazioni e dei dati, con particolare attenzione alle caratteristiche peculiari di questi, al fine di garantire una panoramica sulla loro salvaguardia; ✓alle minacce cyber, elencando tipologia e possibili azioni; ✓alla social engineering e al riconoscimento delle truffe; ✓alle principali normative nazionali ed europee in ambito di sicurezza informatica; ✓alle metodologie dell'analisi del rischio; ✓alle indicazioni di eventuali soluzioni di controllo utili alla prevenzione e alla risposta di eventi negativi; ✓all'introduzione alla gestione del rischio e dei comportamenti individuali da usare in caso di incidenti di sicurezza.

Inoltre, il RTI prevede l'erogazione di contenuti formativi in tema di analisi del rischio anche **sulla base del tool di risk assessment dell'Agenzia per l'Italia Digitale (AgID) messo a disposizione della PA**. Lo strumento, accessibile in modalità web, è pensato per guidare l'utente nelle varie fasi di esecuzione del Risk Assessment e consente ad ogni PA di effettuare le operazioni di self assessment, predisporre gli opportuni piani di trattamento ed eseguire il monitoraggio delle iniziative volte a ridurre il livello di rischio informatico. Il RTI prevede l'erogazione dei contenuti formativi relativi attraverso la **predisposizione di lezioni frontali ad hoc** con personale specializzato; la creazione di una sezione dedicata sulla piattaforma e-Learning e la creazione e la diffusione di pillole di sicurezza in merito, al fine di garantire una conoscenza quanto maggiore dello strumento AgID.

L'approccio proposto dal RTI per l'erogazione del servizio "Formazione e security awareness" si articola nelle seguenti iniziative, garantendo così **l'alternanza di pratiche formative tradizionali ed innovative.**

01 **Le attività di formazione verranno così predisposte**, garantendo l'utilizzo di tecniche formative innovative utili per la costruzione ed erogazione dei contenuti:

Preparazione di materiale formativo ed erogazione di sessioni frontali, contestualizzando il materiale in base alle **pratiche operative** adottate dagli utenti (es. Mobile, BYOD, Cloud Computing), al **ruolo** da essi ricoperto e alle necessità dell'Amministrazione (es. normative di settore, minacce già verificate). Il materiale, inoltre, potrà basarsi su **fatti realmente accaduti presso l'Amministrazione**, avvalendosi delle testimonianze delle persone interne coinvolte. Tale approccio innovativo mira a coinvolgere nell'interezza il discente ed alimentare il suo interesse costruendo il know how a partire da eventi

realmente accaduti. Nel corso delle sessioni frontali il RTI garantisce l'erogazione dei contenuti con l'obiettivo di costruire una consapevolezza della sicurezza informatica collettiva quanto più approfondita. Per questo motivo, il RTI identificherà, di concerto con l'Amministrazione e le strutture interne, i contenuti da inserire in **appositi spazi** (es. Piattaforma di e-learning, Portale Intranet dell'Amministrazione) dedicati alla fruizione del materiale condiviso nel corso delle diverse sessioni. All'interno di questi spazi, il RTI potrà prevedere anche l'inserimento di una sezione di "Frequently Asked Questions" (FAQ) che riporterà le domande e le relative risposte che, con ricorrenza frequente, sono emerse nel corso delle sessioni formative. Infine, sarà possibile inserire nella sezione dedicata il materiale multimediale preparato per lo svolgimento delle lezioni frontali ed **eventuali immagini di sensibilizzazione** contenute all'interno delle "pillole di sicurezza" di seguito descritte.

02 **Preparazione e condivisione di un set di "pillole di sicurezza"**. I contenuti delle "pillole di sicurezza" si focalizzano su numerosi aspetti relativi alla sicurezza delle informazioni e includono **suggerimenti e buone pratiche** che prenderanno in considerazione sia le principali minacce cyber (es. Phishing) sia minacce connesse alle nuove tecnologie (es. Mobile, BYOD, IoT). Nelle pillole, inoltre, sono inseriti e approfonditi alcuni esempi riguardanti attacchi realmente subiti dall'Amministrazione allo scopo di sensibilizzare ulteriormente gli utenti. Infine, come sopra riportato, all'interno di ogni pillola è previsto l'inserimento di apposite immagini di sensibilizzazione che possono essere distribuite sui diversi **endpoint dei dipendenti** e fruite anche attraverso la piattaforma di e-learning, di cui al successivo punto 04, messa a disposizione dal RTI. **Si rappresenta in figura un esempio di "pillole di sicurezza".**

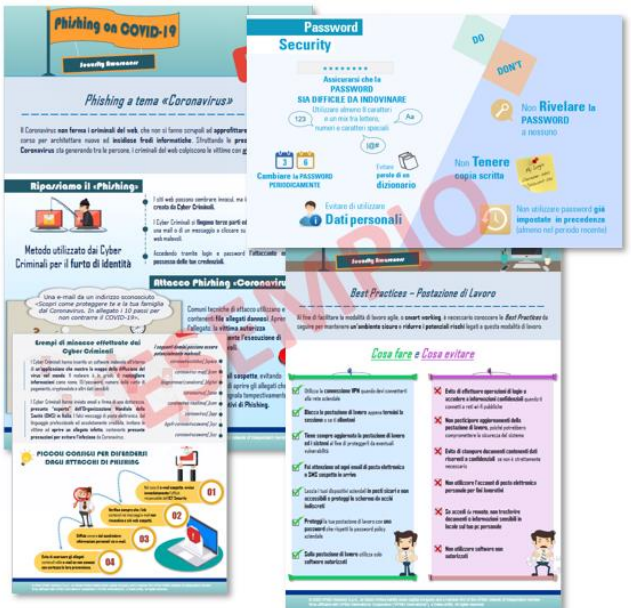

Figura 42 – Esempi di pillole di sicurezza

03 **Diffusione newsletter periodiche.** Le newsletter sono inviate tramite mail a tutti i dipendenti con cadenza concordata con l'Amministrazione in funzione delle esigenze da questa identificate. I contenuti delle newsletter vertono, ad esempio, su tematiche relative alla sicurezza informatica, alla Cyber Security, all'intelligenza artificiale (IA). All'interno delle newsletter sono previsti anche aggiornamenti su fatti ed eventi recentemente accaduti, è possibile includere anche commenti di esperti e di personale interno all'Amministrazione che possa testimoniare su fatti realmente accaduti all'interno della stessa. È inoltre possibile segnalare eventi di interesse comuni relativamente alle tematiche trattate. Le newsletter possono, inoltre, comprendere anche **le "pillole di sicurezza"** predisposte dal RTI ed essere corredate dalle immagini di sensibilizzazione precedentemente citate.

04 **Preparazione e condivisione di materiale informativo tramite contenuti e-Learning anche in modalità escape-room ed erogazione di "Security Gaming".** Lo scopo della condivisione di materiale virtuale è quello di **rendere** accessibile in ogni momento le conoscenze e le informazioni condivise dal RTI e di supportare attivamente l'evoluzione del singolo individuo da potenziale fattore di rischio ad attore protagonista per la difesa di asset e informazioni aziendali. Il RTI offre la **piattaforma di e-learning Cyber GURU** (cfr. §17.2), **personalizzata con logiche innovative di comunicazione, interazione e ingaggio** con un percorso formativo articolato nel tempo che consente di mantenere alta l'attenzione. Grazie alla creazione di un piano editoriale personalizzabile sulla base delle esigenze specifiche e i moduli auto-consistenti, ispirati alla logica del microlearning, l'approccio formativo del RTI favorisce una fruizione allineata all'esigenze dell'utente.

Come elemento a valore aggiunto il RTI si rende disponibile, se richiesto dall'Amministrazione, ad erogare un servizio di supporto e assistenza sulla piattaforma di e-learning allo scopo di favorire un utilizzo corretto da parte dell'utente finale. Il servizio può comprendere, qualora ritenuto necessario dall'Amministrazione, una guida all'utilizzo della piattaforma da pubblicare all'interno dell'intranet aziendale. Il RTI ha sviluppato un **corso completo inerente ai numerosi rischi di natura cyber** ed erogato per mezzo della già citata piattaforma e-learning. Tale corso è supportato da un framework narrativo di riferimento grazie alle tecniche dello storytelling e alle logiche innovative di gamification. Con riferimento a quest'ultimo aspetto, il RTI prevede anche l'erogazione di **"Security gaming"**, della durata di due minuti ciascuno, al fine di migliorare la consapevolezza sull'utilizzo dei dispositivi e degli strumenti informatici.

Tra i temi trattati dai "Security gaming" (es. "Gioco dell'Oca" o "Puzzle Game"): la robustezza delle password, malicious mail, reti sicure e social media. Infine, il RTI prevede anche la predisposizione di **escape-room** dedicate per accrescere il coinvolgimento e la consapevolezza relativa alla sicurezza (es. ai giocatori sono concessi 20 minuti per fuggire da una stanza chiusa a chiave dopo aver trovato una serie di indizi nascosti relativi ai rischi di Cyber Security).

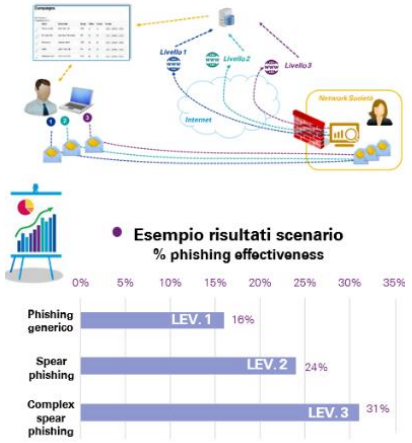

Figura 43 – Esempio risultati scenario

05 **Simulazioni di campagne di Phishing** per sensibilizzare i dipendenti dell'Amministrazione ricreando uno scenario di attacco apparentemente verosimile. L'approccio proposto dal RTI per tali attività si basa sulla corretta individuazione dei possibili elementi di vulnerabilità (es. attuale sensibilità a tematiche di COVID-19) ed al loro exploiting mediante campagne progressivamente evolute. La campagna di phishing viene lanciata da server gestiti dal team del RTI verso i dipendenti dell'Amministrazione, secondo gli scenari concordati. A seguito dell'invio **vengono monitorati i comportamenti degli utenti tramite la console di controllo**.I risultati di questa prima simulazione di attacco phishing vengono raccolti ed analizzati per stimare una panoramica del livello **"**as-is" di awareness. Il RTI è disponibile, se richiesto, ad erogare **simulazioni di campagne di Phishing più sofisticate** (es. Spear Phishing), caratterizzate dall'invio di mail in numero ridotto ma mirate ad un gruppo di destinatari specifici (es. ai dipendenti che sono risultati presentare carenze durante le esercitazioni precedenti).

Il livello di complessità comprende, a titolo esemplificativo, l'inclusione di apposite landing page in cui l'utente viene invitato ad inserire informazioni di carattere personale (es. credenziali di accesso).

14.3. TECNICHE INNOVATIVE DI VERIFICA DEL LIVELLO DI APPRENDIMENTO E SENSIBILIZZAZIONE

Il raggiungimento degli obiettivi formativi e la qualità di tale servizio saranno garantiti mediate l'utilizzo di un approccio metodologico ben strutturato che prevede come punto centrale il monitoraggio continuo dell'apprendimento attraverso una molteplicità di strumenti a carattere innovativo. L'attività di verifica del livello di apprendimento e sensibilizzazione è effettuata mediante l'utilizzo di innovativi strumenti di "*addestramento esperienziale*" ed in particolare mediante **la simulazione di campagne di Phising**, attività già descritta al punto 5 del paragrafo precedente. Tale strumento innovativo consente infatti di verificare sul campo l'effettiva messa in pratica di comportamenti adeguati e delle buone pratiche apprese durante il percorso formativo. Le verifiche del livello di apprendimento vengono effettuate anche attraverso **esercitazioni e sessioni collettive di "Review".** Il RTI predispone dei **test scritti a risposta multipla** che, una volta completati, vengono discussi con tutta l'aula, dando luogo ad una "review" collettiva. Le "Review" finali sono parte integrante dei programmi formativi finalizzati a garantire il confronto tra i partecipanti sulle nozioni apprese, su eventuali dubbi e sulle curiosità emerse. Il RTI prevede la somministrazione di test a risposta multipla e l'inserimento di **quiz anche all'interno della sessione e-Learning.** I test hanno come oggetto tutti gli argomenti trattati nel corso di formazione e sono soggetti ad una correzione collettiva al fine di sensibilizzare e coinvolgere quanto più possibile gli utenti e rispondere ad eventuali curiosità. Oltre ai test a risposta multipla, sono previsti anche **test in modalità multimediale** che possono essere predisposti mediante filmati interattivi incentrati sulle dinamiche proprie del gioco (es. punti, livelli, premi) al fine di sollecitare l'impegno e la competitività sulle tematiche di cyber security, affrontate durante il corso. I test possono essere svolti individualmente e sono suddivisi rispettando le sessioni di erogazione del corso. Il RTI può prevedere, qualora richiesto, una **breve sessione di esercitazione orale per ogni partecipante**. Il formatore responsabile della sessione, a fine programma e a seguito dell'erogazione dei test scritti, sottopone al partecipante un quesito relativo ad un possibile incidente di sicurezza. Al partecipante vengono messi a disposizione cinque minuti per indicare la natura dell'incidente di sicurezza e una sua possibile risoluzione. Al termine dei cinque minuti, il formatore svela la risposta più appropriata e la condivide con l'intera classe per raccogliere eventuali dubbi o commenti.
Inoltre, il RTI aggiunge come ulteriore elemento migliorativo, in base agli ambiti progettuali precedentemente descritti, la predisposizione e la condivisione, con l'Amministrazione, della seguente documentazione:
Executive report: reportistica contenente i risultati di alto livello di tutte le attività svolte ed eventuali suggerimenti al fine di mitigare i rischi derivanti dalle problematiche riscontrate;
Report tecnico: reportistica contenente i risultati tecnici di dettaglio, oltre che la spiegazione puntuale di tutti gli step intrapresi per ottenere i risultati presentati

15. PRESENZA DI ULTERIORI FUNZIONALITA' AGGIUNTIVE

Si conferma la presenza contemporanea delle funzionalità di; ✓"Geo-IP filtering e Geo-Blocking" per il servizio "Next Generation Firewall" per consentire la creazione di regole di policy da applicare a specifici paesi e/o regioni geografiche); ✓raccolta ed utilizzo delle informazioni secondo profili di utenza diversi, tramite un'interfaccia grafica oppure tramite API per il Servizio "Gestione continua delle vulnerabilità di sicurezza"; ✓utilizzo dei formati STIX/TAXII per l'integrazione con il sistema SIEM per il servizio "Threat Intelligence e Vulnerability Data feed".

16. PORTALE DELLA FORNITURA

Il RTI predisporrà un Portale della Fornitura, raggiungibile tramite Internet, a disposizione delle singole PA per il governo dei servizi, nel rispetto dei requisiti descritti nel Capitolato Tecnico Generale (cfr. §9.1).
Più in generale, il portale previsto dal RTI offrirà servizi: a Consip, per il governo dell'AQ nel suo complesso; alle singole Amministrazioni contraenti per il governo dei Contratti esecutivi affidati al RTI; a tutti gli utenti per la fruizione degli strumenti offerti e la condivisione delle informazioni di interesse.
Il Portale della Fornitura è anche il punto di accesso per i team del RTI per il popolamento dei contenuti e per la normale condivisione della conoscenza.

Figura 44 – Schema del Portale della Fornitura

16.1. SOLUZIONI TECNOLOGICHE E FUNZIONALITÀ DEL PORTALE DELLA FORNITURA

La soluzione proposta deriva dalle esperienze maturata dalle aziende del RTI nella realizzazione di analoghe piattaforme a supporto della gestione di forniture su analoghi contesti di servizio.

La soluzione tecnologica scelta dal RTI per la realizzazione del Portale della Fornitura è basata su uno stack di prodotti prevalentemente open source. In particolare, adotta la piattaforma **Liferay Digital Experience Platform** (Liferay DXP), leader di mercato, che supporta diversi standard d'interoperatività (JSR168, JSR170, JSR160, FTP, WebDAV, CIFS/SMB, Microsoft SharePoint, Web Services, REST API, RSS) consentendo di: ✓accedere ai contenuti attraverso API Standard Content Repository for Java Technology; ✓integrare attraverso WebDAV l'accesso ai contenuti con sistemi Desktop ✓fornire attraverso Web Service un accesso a tutti i servizi della componente di base del sistema portale; ✓scambiare in modo semplice ed efficace contenuti web con altri portali attraverso la tecnologia RSS.

L'adozione della piattaforma Liferay DXP permette al RTI di realizzare il portale in ottica responsive e multi-device in osservanza dei principi di accessibilità definiti dalla Legge Stanca (n.4/2004) e successivi aggiornamenti (come, ad esempio il D.lgs. n. 106/2018) e alle 'Linee guida di design per i servizi web della PA' tracciate da AgID. Il Portale consente l'accesso, in modalità multicanale, a tutti gli strumenti operativi e di governo, in modalità profilata e selettiva: ✓ai referenti dell'Amministrazione per la rispettiva area di competenza, ✓al Management delle aziende del RTI, ✓a tutte le risorse dei Team di presidio e operanti presso le sedi di erogazione, ✓ad eventuali soggetti terzi. Di seguito la descrizione delle principali Aree in cui è strutturato il portale, schematizzate nell'immagine a lato.

Per garantire la completa copertura delle necessità previste dagli atti di gara, il Portale della Fornitura prevede le seguenti funzionalità, ottenute integrando strumenti dedicati: ✓Controllo accessi e gestione identità; ✓Governo fornitura; ✓Gestione della Conoscenza; ✓Analisi dati e reporting; ✓Comunicazione e collaborazione in chiave "social"**.**

Controllo accessi e gestione identità

L'accesso ad alcune sezioni del Portale è possibile previa autenticazione.

Attraverso funzionalità dedicate, è possibile profilare gli utenti, definendone i diritti di accesso. Sono previste, quindi, le principali seguenti categorie di utenti:

1. **Utente Non autenticato**: utente generico del World Wide Web (WWW);
2. **Utenti autenticati** Utente Amministrazione: utente accreditato appartenente ad uno dei soggetti che ha aderito ai servizi della fornitura - Utente Organismi di coordinamento: utente con profilo specifico per l'esecuzione delle attività di Governance della fornitura, con abilitazioni differenziate fra Organismo Tecnico e Organismo strategico - Utente RTI: utenti accreditati rappresentanti il RTI nel presente lotto di fornitura e in dettaglio: Responsabile del contratto (RUAC AQ e RUAC CE), Responsabili Tecnici per l'erogazione dei servizi, e altre figure di riferimento del RTI - Utente Osservatori e CONSIP: utenti accreditati che svolgono le funzioni di monitoraggio della qualità e della sicurezza sulla fornitura.

Governo fornitura

Le funzionalità di Governo della fornitura, in termini di Program e Project Management (PPM), garantiscono un punto di accesso unico per il governo dei progetti e la gestione dei piani e della documentazione a diverso livello di dettaglio (AQ, Contratto Esecutivo e singole iniziative progettuali), profilato secondo gli specifici ruoli dei diversi fruitori: una sezione a livello di AQ offrirà una visione complessiva del contratto mentre sottosezioni specifiche permetteranno di avere le informazioni a livello di singolo CE.

Il RTI prevede di utilizzare, quale piattaforma di PPM, la soluzione basata sulla suite **Microsoft Project**, **Planner**, **Power Automate** integrata in maniera nativa con gli strumenti di Intelligenza Artificiale, denominati Microsoft PowerBI.

La soluzione permette di visualizzare lo stato della "domanda" (fabbisogni delle Amministrazioni) e della "risposta" (CE e relativi progetti), pianificandone l'andamento e monitorarne i progressi in modo centralizzato. Il Portale della Fornitura darà quindi supporto all'intero processo di project management nelle sue "capabilities" chiave:

- Demand management con cui si garantisce una condivisione fra gli attori durante tutto il processo di gestione della domanda;
- Gestione delle risorse, dei costi e del tempo con predisposizione e condivisione del planning e dell'effort complessivo. Il monitoraggio di soglie specifiche permetterà anche di anticipare e segnalare con alert puntuali le situazioni di criticità;
- Workflow personalizzabile relativo a rischi, problemi, decisioni, azioni e cambiamenti per automatizzare e semplificare il lavoro. È possibile, per ciascuno dei ruoli definiti nell'organizzazione, seguire e automatizzare l'intero processo di governo del progetto dall'attivazione alla chiusura delle diverse iniziative;
- Cruscotti e reportistica: si prevedono viste destinate a utenti diversificati nel ruolo:
  - dashboard di AQ, di CE e di progetto che offriranno viste a diverso livello di dettaglio permettendo una valutazione dell'efficacia delle attività svolte in relazione a specifici KPI quali tempi, stato delle attività e obiettivi raggiunti, qualità dei risultati, costi e risorse (umane e no) con valori personalizzabili;
  - grafici interattivi che tracciano il progresso anche di singoli obiettivi o di un gruppo di essi.
- Documentazione operativa: una specifica sottosezione documentale permetterà, nel rispetto agli standard di qualità, di tracciare in maniera strutturata e condividere note di lavoro significative, punti di attenzione, criticità di progetto anche sincronizzandosi con altre fonti dati.

Gestione della Conoscenza

L'area del **Knowledge** è dedicata agli strumenti per la gestione della conoscenza in grado di alimentare, sulla base delle esperienze pregresse e nel corso della fornitura, il cospicuo patrimonio informativo a disposizione del RTI (esperienze, framework per la stesura di componenti di offerta, metodologie e tecniche, white paper, ricerche di mercato, studi sull'evoluzione dei trend tecnologici/normativi). Tale Area permette di poter accedere agli strumenti integrati tra loro e descritti di seguito.

- Knowledge Management System (KMS): il sistema proposto garantisce la condivisione della conoscenza, a supporto delle diverse strutture organizzative coinvolte nella fornitura. Il sistema di KM, basato sull'utilizzo della piattaforma Liferay DXP, garantisce la governance dell'informazione salvaguardandone i contenuti. Tutti i tipi di informazioni / documenti trattati siano tracciati e ricercabili attraverso metadati che ne identifichino la

sorgente, le responsabilità, le modifiche apportate etc. Il sistema di KMS è articolato nelle seguenti aree principali: ✓Article: consente di aggiungere, modificare ed eliminare articoli di tipo knowledge; ✓News: permette di aggiungere, modificare ed eliminare articoli di tipo news; i ✓Libreria Metodologie / Best Practice: adibita alla raccolta di documentazione informativa sulle Metodologie e Best Practice utilizzate dal RTI nell'AQ ✓Q&A: permette di moderare sessioni Q&A tra gli utenti Hot Topics Analytics; permette di analizzare i quesiti e le richieste degli utenti, come pure i tipi di informazione che gli utenti ricercano ✓disponibilità di Strumenti di Collaboration.

- Base documentale (Knowledge Base Management System) Costituisce il repository centralizzato dove archiviare, classificare ed organizzare, i documenti di carattere generale della fornitura riguardanti sia il contesto dell'Appalto Specifico, le finalità e i risultati della fornitura sia i dettagli relativi ai servizi erogabili inclusa la relativa documentazione tecnica di supporto. La categorizzazione documentale è suddivisa in tre aree:
  - **Area Comunicazione**, di libero accesso ai Referenti dell'Amministrazione, ospita i documenti di interesse generale riguardanti il contesto del Contratto Quadro e le specificità dell'Appalto Specifico, le finalità e i risultati della fornitura e i dettagli relativi ai servizi erogabili
  - **Area Informativa**, contiene i documenti relativi alla gestione tecnica dell'Appalto Specifico come ad esempio, documentazione tecnica di supporto, aggiornamento degli asset relativo al parco applicativo e delle informazioni, FAQ, soluzioni degli Incident, Piani di Lavoro, verbali, etc.
  - **Area Deliverable**, dedicata alla raccolta di tutti i deliverable richiesti dall'Amministrazione.

Lo strumento KBMS dotato di un Workflow engine che consente di definire l'iter approvativo per i documenti di fornitura e di un Motore di ricerca semantico: intelligente e personalizzato, che permette di ritrovare documenti di interesse.

16.2. STRUMENTI DI ANALISI DEI DATI E REPORTING

Per le funzionalità di analisi dei dati e reporting il RTI prevede l'uso di **MS Power BI** che tramite report statici e dinamici, offre ai diversi stakeholders la possibilità di effettuare analisi multidimensionali su tutti i parametri caratteristici dell'AQ: dati di qualità e sicurezza; customer satisfaction misurata con la soluzione **LimeSurvey**; livelli di servizio e indicatori di qualità e di digitalizzazione, valori economici dei CE sottoscritti, etc.. Particolare attenzione è rivolta alla realizzazione dei cruscotti di monitoraggio relativi ai Piani dei Fabbisogni, Piani Operativi e CE. In accordo con Consip, report statici relativi ad avanzamenti delle iniziative contrattuali, numerosità delle iniziative attive e concluse, indicatori di digitalizzazione, potranno essere resi disponibili nelle aree Comunicazione (area pubblica) e Informativa. In generale, sono offerte agli utenti del portale funzioni per > ricevere periodicamente versioni aggiornate di uno o più report nella propria casella e-mail ed > essere informati della disponibilità di nuove versioni dei report (WhatsApp, Telegram), anche senza accedere alla piattaforma. In questo modo sarà possibile tenere sotto controllo anche offline un particolare aspetto dei CE attivi, senza la necessità di dover accedere alla piattaforma.

Figura 45 – Dashboard di reportistica

Sono messi a disposizione report che monitorano l'andamento generale dell'AQ tramite parametri quali, in via esemplificativa: ✓numero dei Piani di Fabbisogni realizzati con il dettaglio del loro stato (numero CE associati, percentuale CE completati/attivi, budget consumato) e con drill down sul dettaglio dei CE associati; ✓andamento e stato dei Piani Operativi; ✓numero e volumi di CE, con drill down sulla distribuzione territoriale e per tipologia di PA; ✓numero dei servizi/sottoservizi/interventi con il dettaglio del loro stato di avanzamento e del budget assegnato, consumato e residuo.

MS Power BI è totalmente integrato con MS Excel: è pertanto facile effettuare degli export sia in formato Excel che nei formati più comuni (es. csv, json, xls etc.). Il meccanismo permette di salvare periodicamente e in maniera automatica un determinato set di report all'interno della piattaforma SharePoint online, dove resterà disponibile per i diversi stakeholder.

16.3. SOLUZIONI, PROCESSI E STRUMENTI DI COMUNICAZIONE E DI COLLABORAZIONE IN CHIAVE "SOCIAL" CON LE AMMINISTRAZIONI CONTRAENTI

Come soluzioni e strumenti di comunicazione e di collaborazione in chiave "social" il RTI adotta due componenti della piattaforma Microsoft 365: **MS Teams** e **MS Yammer**.

Microsoft Teams è una App di messaggistica che consente di condividere uno spazio di lavoro per la collaborazione e la comunicazione in tempo reale, le riunioni, la condivisione di file fra tutti i membri di un gruppo di lavoro. Permette di comunicare con la massima efficacia, creare team di lavoro con chat di gruppo, organizzare riunioni on line, chiamate, conferenze e condividere documenti.

MS Teams sarà dedicato alla collaborazione nell'ambito dei progetti, sia internamente al RTI, sia per migliorare l'efficacia delle interazioni fra i membri dei gruppi di lavoro del raggruppamento e i referenti delle Amministrazioni contraenti, facilitare e velocizzare le iterazioni.

Le caratteristiche del sistema consentono ai Referenti Tecnici di configurare, modificare e gestire l'organizzazione di "working room" virtuali, in modo semplice ed efficace.

Infatti il sistema consente: ✓la creazione di "stanze virtuali" per le riunioni, dotate della documentazione utile per le fasi preparatorie degli incontri e per la discussione vera e propria. In questo spazio è possibile, inoltre, creare una sorta di blog in cui i partecipanti possono relazionarsi e chiarire eventuali dubbi pre-riunione allo scopo di fare della riunione in presenza un momento di eccellenza e di sintesi; ✓funzioni di video conferenza, per eventuali partecipanti a distanza;

✓funzioni di messaggistica on line con cui la community dei responsabili della fornitura potrà fare domande e fornire risposte in qualunque momento.

MS Teams potrà essere utilizzato nel corso della fornitura per mantenere costantemente aggiornati gli stakeholders dei progressi della migrazione, condividere eventuali criticità ed i punti di attenzione. Potranno essere costituiti Team specifici fra RTI, Amministrazione con canali dedicati al progetto di migrazione oppure dedicati alle attività di revisione degli Indicatori di digitalizzazione congiuntamente con gli Organismi di coordinamento e controllo.

MS Yammer è un Enterprise Social Network (ESN), invece orientato alla comunicazione "esterna". Consente di costituire comunità su scala più ampia tra le diverse organizzazioni coinvolte dall'iniziativa, condividendo e sfruttando le conoscenze e le esperienze maturate nei diversi progetti di migrazione. L'ambito di utilizzo di Yammer si distingue da quello di Teams per la gestione di conversazioni che non passano esclusivamente da meccanismi di chat istantanea, ma che conservano validità per gli appartenenti alla "comunità" anche per periodi più lunghi, come nel caso della condivisione delle esperienze.

17. INNOVAZIONE

Per garantire un elevato livello di innovazione nell'erogazione dei Servizi di gara il RTI propone l'adozione di soluzioni e modalità operative, facendo leva su un approccio organico che valorizza tutti gli elementi distintivi e di unicità del RTI, in termini di:

- **Metodologie, soluzioni organizzative e strumenti operativi** proposti per gestire, per l'intera durata dell'AQ, tutte le attività necessarie a promuovere e diffondere l'innovazione in ciascun ambito dei servizi richiesti e sul singolo CE;
- **Presenza di numerose e complementari strutture operative innovative** (cfr. cap.1 - Ecosistema dell'Innovazione) che saranno coinvolte dall'Innovation Hub e utilizzate sul singolo CE, con ruoli, competenze e attività specifiche assegnate (come illustrato nel seguito del paragrafo), al fine di apportare *know-how* e soluzioni innovative e consistenti per rispondere alle esigenze di trasformazione delle PA aderenti all'AQ.

17.1. METODOLOGIE, SOLUZIONI ORGANIZZATIVE E STRUMENTI ADOTTATI

Per diffondere l'innovazione all'interno dell'Amministrazione, il RTI propone l'adozione di un approccio metodologico di Innovation management "proattivo" e "reattivo" che consentirà di: ✓disporre, sin dalla stipula dell'AQ, di **strutture operative preposte alla gestione dell'innovazione**; ✓utilizzare **modalità operative snelle e flessibili** che permettano di individuare la struttura operativa dell'Ecosistema dell'Innovazione più idonea alle esigenze della singola PA. In tale ottica, l'Innovation Hub assume un ruolo centrale come unità operativa che presidierà, a livello di AQ, tutte le tematiche connesse all'innovazione, gestendo direttamente un framework metodologico e organizzativo pensato appositamente per la presente Fornitura (schematizzato a lato) che: ✓**valorizza le organizzazioni interne dei componenti del RTI** (es. *competence center*, osservatori, *innovation lab*, centri di ricerca e start-up innovative) e dei relativi *network* ed ecosistemi di innovazione presidiati (es. incubatori e acceleratori, *network* di *start-up* e PMI innovative con cui gli operatori economici collaborano stabilmente); ✓**individua e disciplina puntualmente soluzioni organizzative e strumenti operativi** da adottare in ogni fase del *funnel* (imbuto) di innovazione, massimizzando il contributo innovativo da parte di ciascuna struttura operativa ingaggiata in tutti i servizi proposti. In particolare, il *framework* organizzativo e metodologico proposto è articolato nelle seguenti fasi:

FASE 1 (F1): Approach to Innovation Gestita secondo due approcci complementari e sinergici:

- **Approccio proattivo**: le strutture innovative presenti all'interno dell'Ecosistema dell'innovazione implementano un processo virtuoso di monitoraggio dei *trend* di mercato relativi a soluzioni innovative e tecnologie emergenti in ambito della Sicurezza che possono essere oggetto di potenziale interesse per l'evoluzione e innovazione dell'Amministrazione. Tale attività consente al RTI di "anticipare i bisogni di innovazione";
- **Approccio reattivo**: i professionisti del RTI che interagiscono con l'Amministrazione rilevano "sul campo" uno o più bisogni specifici di innovazione direttamente espressi e/o correlati alle richieste di supporto indicate dall'Amministrazione.

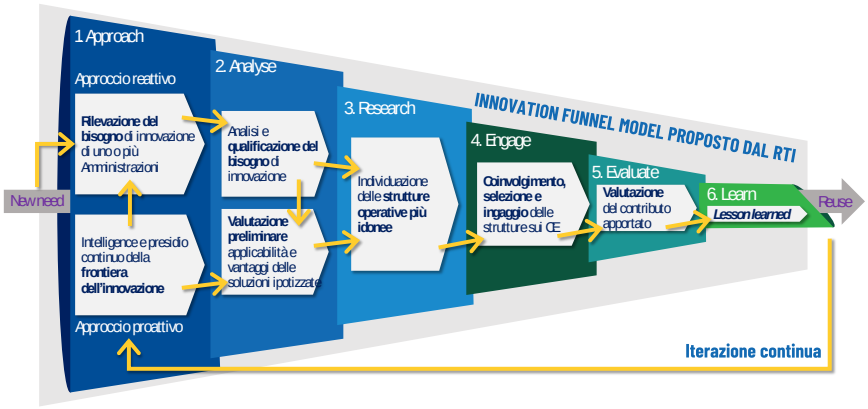

Figura 46 – Innovation Funnel Model

FASE 2 (F2): Analysis Rilevato il bisogno di innovazione, l'Inn-Hub attiverà, coinvolgendo le strutture dell'Ecosistema dell'Innovazione competenti per ambito, una fase di analisi approfondita e qualificazione del bisogno espresso/rilevato sul singolo CE, con la finalità di mappare e declinare puntualmente: ✓**Obiettivi e risultati attesi** dall'Amministrazione; ✓**Soluzioni e tecnologie abilitanti** già esistenti sul mercato per rispondere al bisogno di innovazione ed eventuali *benchmark* e *best practice* da "riusare", sviluppate in ambito pubblico su scala globale; ✓***Stakeholder* da coinvolgere** in fase di progettazione e implementazione della soluzione innovativa; ✓***Key User* e *task owner* dei Servizi e processi** dell'Amministrazione impattati dall'introduzione della soluzione; ✓**Servizi di gara da attivare**.

FASE 3 (F3): *Research* Sulla base delle evidenze raccolte in fase 2, l'Inn-Hub valuta la necessità e le modalità di coinvolgimento, all'interno dei gruppi di lavoro impiegati sui singoli CE, di: ✓**Livello 1**: Strutture operative innovative che fanno parte delle organizzazioni interne degli operatori economici del RTI (es. *competence center*, *tech-labs*, centri di ricerca e sviluppo, osservatori tematici). Esse forniscono ai *team* operativi RTI tutto il *know-how* necessario per la progettazione di soluzioni ad elevato contenuto innovativo; ✓**Livello 2**: Incubatori e acceleratori di innovazione che collaborano stabilmente con il RTI. Tali strutture supportano l'Inn-Hub e le strutture innovative del RTI nell'individuazione delle migliori soluzioni da proporre all'Amministrazione; ✓**Livello 3**: Start-up e PMI innovative che saranno in grado di apportare *know-how* a valore aggiunto e soluzioni ad elevato contenuto innovativo.

La selezione delle strutture da coinvolgere sul singolo CE, è definita di volta in volta dall'Inn-Hub, basandosi sulla valutazione integrata di 5 *driver* di selezione (D): ✓**D1–Innovatività delle soluzioni proposte** ✓**D2–Applicabilità delle soluzioni alle PA italiane**;✓**D3–Tempistiche di ingaggio delle strutture**; ✓**D4–scalabilità e riuso delle soluzioni**; ✓**D5-presenza sul territorio.**

FASE 4 (F4): *Engage* Nell'ambito di tale fase, l'Inn-Hub gestisce il processo di contatto, coinvolgimento e ingaggio delle strutture innovative individuate in Fase 3. In particolare, il modello organizzativo proposto prevede differenti modalità di ingaggio, quali: ✓**Strutture innovative interne**: strutture già integrate nel RTI che coprono a 360 gradi le competenze tematiche, funzionali, metodologiche e tecnologiche relative al contesto di gara, rispetto alle quali è richiesta l'introduzione di soluzioni innovative; ✓**Start-up**: strutture in grado di proporre soluzioni operative e tecnologiche ad elevato contenuto innovativo (soluzioni

disruptive), capaci di avviare all'interno delle PA percorsi di accelerazione dell'innovazione e di trasformazione digitale di Servizi erogati e processi gestiti; ✓**PMI innovative:** strutture presenti sul territorio, capaci di generare innovazione facendo leva sulla conoscenza di esigenze e bisogni specifici del territorio all'interno del quale operano le Amministrazioni; ✓**Ingaggio delle strutture operative individuate:** Le strutture interne sono rapidamente attivate dall'Inn-Hub, andando a completare e integrare i team di intervento con competenze peculiari in linea con l'esigenza espressa dall'Amministrazione. *Start-Up* e PMI innovative sono ingaggiate secondo un modello operativo articolato in più *step*: **1)** preselezione di un *cluster* del *set* di strutture individuato in Fase 3; **2)** contatto, valutazione e selezione di una *short list* di operatori per la definizione di prototipi e/o lo sviluppo di soluzioni-pilota. Gli operatori saranno confrontati in base alle peculiarità specifiche, utilizzando anche modalità di valutazione innovative (es. *Call4Ideas*, *Hackaton*); **3)** integrazione della struttura selezionata all'interno dei *team* di intervento che erogano i Servizi oggetto di fornitura.

FASE 5 (F5): *Evaluate,* al termine delle attività svolte dalla struttura operativa ingaggiata, l'Inn-Hub effettua una valutazione del contributo fornito, con l'obiettivo di valorizzare l'esperienza, in termini di criticità riscontrate e superate, *lesson learned*, *best practices* da poter riusare all'interno dell'AQ. Tale valutazione permette di agevolare eventuali ingaggi futuri della struttura e tiene conto di: ✓***rating*** dell'Amministrazione in termini di soddisfazione rispetto al bisogno di innovazione iniziale; ✓***feedback*** del Responsabile Tecnico del Servizio sul coinvolgimento della struttura in termini di efficacia nelle attività operative; ✓livello di **soddisfazione** espresso direttamente dalla struttura stessa ingaggiata, rispetto alle attività svolte sul progetto.

FASE 6 (F6): *Learn,* L'ultima fase dell'Innovation Funnel Model proposto prevede una fase di sistematizzazione del materiale illustrativo delle soluzioni innovative sperimentate e introdotte sulla singola Amministrazione, con l'obiettivo di condividere i processi digitali a disposizione con tutte le Amministrazioni interessate ad avviare percorsi di innovazione tecnologica e trasformazione digitale.

17.2. SOGGETTI COINVOLTI E PRINCIPALI CARATTERISTICHE

Si riporta di seguito una sintetica descrizione dei Centri di Ricerca, delle PMI e Start-up innovative con cui il RTI collabora per portare valore aggiunto ai servizi erogati.

Il Center for Cyber Security and International Relations Studies (CCSIRS), è parte del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università degli Studi di Firenze e analizza l'influenza del cyberspazio sulla sicurezza nazionale italiana. Il Centro mira ad accrescere e approfondire lo studio delle dinamiche della dimensione cyber attraverso un approccio *policy oriented*. Il suo approccio **multidisciplinare** garantisce l'integrazione dei tradizionali ambiti delle Scienze Sociali (politologia, economia, giurisprudenza, studi strategici e militari), con le discipline proprie dell'Ingegneria Informatica. Inoltre, la fiducia nella ricerca del Centro si traduce in un significativo investimento nel settore R&D, con l'obiettivo di restare sempre aggiornati sugli ultimi sviluppi tecnologici, regolativi e politici, sia in Italia che nel resto del mondo. Questa missione si concretizza non solo con pubblicazioni, documenti di ricerca e analisi indipendenti, ma anche con la partecipazione alle maggiori conferenze relative ai temi di interesse, funzionali agli obiettivi dell'Amministrazione che richiede un **costante aggiornamento**, anche in tempo reale, per erogare servizi coerenti con le novità del settore, attrarre consenso e accrescere competitività.

Cyber Guru, startup innovativa che offre servizi formativi volti a diffondere le buone pratiche per prevenire ed evitare gli attacchi hacker attraverso un sofisticato portale e-learning che consente di incidere in modo concreto ed efficace su attitudini e comportamenti, trasformando le persone in "agenti attivi" del sistema di Cyber Defense. La soluzione permette di **aumentare la consapevolezza** (awareness) degli utenti rispetto ai rischi che si corrono nell'interazione con le tecnologie digitali e con il Web e **di influenzare i comportamenti degli utenti,** per renderli adeguati alle necessità di protezione delle organizzazioni e dei dati aziendali critici e personali, oltre che alle sfide imposte dall'evoluzione del crimine informatico.

Gli **Insights Centre** di KPMG sono importanti showcase hub, localizzati in tutto il Mondo, in ambito di Data & Analytics e Technology Innovation. L'Insight Centre italiano, posto al 9° piano del Building KPMG a Milano, fa parte di un network globale in espansione, con sedi a Tokyo, Londra, Parigi, Madrid, New York, Francoforte, Zurigo, Melbourne, Sydney, Hong Kong, Vancouver e molti altri, si tratta di un'area di circa 500 metri quadri in cui sono concentrate le più importanti tecnologie Data Driven che permettono di gestire, interagire e analizzare i dati per valorizzarne il significato trasformandolo in conoscenza e abilitando nuove soluzioni e modelli di business.

Haruspex, PMI innovativa, nata nel 2016; offre una soluzione di Cyber Security in grado di prevedere, in base al livello di confidenza desiderato, come potrebbe essere attaccata un'infrastruttura ICT, prima che si verifichino gli attacchi, fornendo così soluzioni per neutralizzare gli aggressori. Haruspex utilizza un motore di intelligenza artificiale per costruire un "*digital twin*" degli attaccanti e della struttura, effettuando milioni di simulazioni di attacco e abilitando quindi anche scenari what-if e la security-by-design.

ReeVo, PMI innovativa fondata nel 2003; è il cloud provider italiano focalizzato sui servizi di Cyber Security e archiviazione che consente alle aziende e alle Amministrazioni di proteggere e custodire il vero patrimonio aziendale rappresentato dai dati. ReeVo, oltre a custodire i dati attraverso risorse e piattaforme tecnologiche, analizza le minacce, le vulnerabilità e i rischi dei servizi del cloud e delle reti clienti al fine di proteggerli da attacchi esterni ed interni. Infine, ReeVo dispone di Centri di Competenza distribuiti sul territorio nazionale specializzati nella ricerca di soluzioni innovative specializzate sulla Cyber Security.

Boolebox, PMI innovativa fondata nel 2011; dispone di una suite di applicazioni per la protezione dei dati aziendali che preservano l'integrità e la riservatezza dei dati da qualsiasi accesso non autorizzato, interno o esterno all'azienda, grazie alla crittografia di grado militare e garantendo così i più elevati standard di cifratura per proteggere i dati sensibili dagli attacchi informatici.

Bluenet PMI innovativa che sviluppa nuovi programmi di ricerca e sviluppo di carattere scientifico e tecnologico nei campi dell'informatica e dell'elettronica. Con una consolidata esperienza in applicazioni di controllo accessi, identità legata a documenti elettronici, sistemi operativi per microcontrollori, smart card ed applicazioni NFC, con brevetti e tecnologie innovative già mature. In particolare, Bluenet dispone di una piattaforma di timbro digitale con elevato valore di efficienza, gestione di impronte digitali e riconoscimento facciale.

17.3. AMBITO DI INTERVENTO E VALORE AGGIUNTO CONCRETAMENTE APPORTATO IN TERMINI DI INNOVAZIONE E INCREMENTO DELLE QUALITÀ

Di seguito sono descritti **gli ambiti di intervento** dei Centri di Ricerca, delle PMI e delle Start-up innovative e **il valore aggiunto** concretamente apportato nell'esecuzione delle prestazioni in termini di **innovazione e incremento della qualità**.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Attraverso l'accesso al **know-how**, alle **metodologie** e agli **strumenti** largamente sperimentati, il RTI può conferire un taglio innovativo concreto a molti dei servizi offerti: dalla **formazione**, alle attività di **vulnerability assessment,** alla **gestione del rischio**, alla **configurazione delle strutture organizzative dei diversi servizi**. Inoltre, il Centro mette a disposizione dei team di intervento del RTI know-how verticale a garanzia dell'innovazione dei Servizi di gara erogati; offre contributi tecnico-metodologici (best practice, studi e analisi) rispetto alle soluzioni più innovative e sperimentali proposte dal mercato; collabora all'ideazione e progettazione di soluzioni innovative, con stima di tempi, costi e benefici degli interventi, nonché definizione di nuovi processi e procedure e relativo impatto sui sistemi delle Amministrazioni; contribuisce all'utilizzo di modalità innovative di assessment (ad es. mediante logiche di crowd-testing); dispone di benchmark con realtà assimilabili in contesti nazionali e internazionali. A livello tecnico e pratico, il Centro si pone come obiettivo lo **sviluppo, la produzione e la diffusione di servizi e soluzioni innovative ad alto valore tecnologico**, ad esempio: ✓**Cyber Threat Intelligence,** piattaforma con funzionalità di info-sharing per la gestione dei dati classificati. Il software punta a collezionare, gestire e processare le informazioni non classificate, attraverso l'emissione di report semi-automatici, con elevati standard di qualità garantiti da analisti e componenti AI/ML; ✓**Cyber Human Factor,** l'assessment del livello di esposizione al fattore umano legato al rischio cyber. Il servizio valuta le capacità di risposta, in relazione ai cambiamenti della minaccia e ai rischi cyber correlati con il fattore umano; ✓**Cyber Maturity Assessment,** l'assessment del livello di maturità tecnologica sui più importanti temi della cyber security, sia in termini di tecnologie che di processi interni e/o esterni; ✓**Framework Compliance Tool,** strumento in grado di determinare un piano per ottenere la piena conformità ai maggiori standard dell'IT security. Il software analizza e compara automaticamente più di una decina di riferimenti internazionali (es. ISO, NIST, CMMC), valutando in maniera automatizzata i processi dell'organizzazione e stabilendo le azioni da attuare per colmare i gap identificati. In ultimo, il RTI può attingere al **network di partnership** pubbliche e private di cui gode il CCSIRS e ai costanti aggiornamenti diffusi da questo su diverse tematiche di ricerca come: il Cyber Warfare, la Cyber Diplomacy, la Cyber Security, la Cyber Law, La Cyber Intelligence e il Cyber Terrorism.

CYBER GURU

L'ambito di intervento della start up è focalizzato **nell'erogazione dei servizi di formazione sulla "Security Awareness".** Attraverso un approccio sinergico fra formazione e verifica, Cyber Guru permette al RTI di implementare il servizio di "Security Awareness" su piattaforma digitale, assicurando **metodologie innovative,** e di aggiornare ed arricchire gli argomenti trattati in base alle minacce cyber più rilevanti del momento e/o al maggiore impatto per l'Amministrazione, permettendo la creazione di test di verifica puntuali e concreti. Infine, Cyber Guru offre **sistemi di reportistica** in grado di soddisfare le esigenze di tutte le figure professionali coinvolte a vario titolo nei programmi formativi e addestrativi. Dunque, attraverso il coinvolgimento della Start-up, il RTI garantisce, con particolare riferimento al servizio di "Security Awareness", che:

- gli argomenti trattati siano aggiornati ed arricchiti regolarmente in base alle minacce cyber più rilevanti del momento e/o dal maggiore impatto per le diverse organizzazioni e figure aziendali;
- vengano affrontate nel dettaglio tematiche relative alla Social Engineering (inclusi Phishing, Smishing, Vishing, Fake News, Truffe Telefoniche), alla protezione delle informazioni (inclusi Gestione delle Password, Privacy & GDPR, Utilizzo dei Social Media, Email security, Classificazione delle Informazioni, Dati Personali Identificativi, Navigazione sul Web, Clean Desk, Lavoro Remoto) e alla conoscenza e al corretto utilizzo delle tecnologie informatiche (Dispositivi Mobili & App, Memorie USB, Browser Web, Dispositivi IoT, E-Commerce, Cyber Hygiene, Backup & Restore);
- sia assicurata una efficiente e aggiornata condivisione di buone pratiche.

INSIGHTS CENTRE DI KPMG

L'Insights Centre rappresenta un fattore chiave della strategia di innovazione che trasforma il modo di lavorare, rendendo le persone attive protagoniste, fornendo loro strumenti e un mindset per pensare in modo diverso e supportandole nelle sfide più critiche. La missione del Centro è quella di creare valore tramite insights, facilitation e thought leadership. L'Insights Centre è dunque un importante showcase hub in ambito di Data & Analytics e Technology Innovation e può, quindi, fornire supporto, in fase di erogazione dei servizi di AQ, in svariati ambiti, ad es. nella gestione del rischio e nell'analisi dei dati e supporta i team di intervento nello sviluppo di soluzioni innovative per la digitalizzazione dell'Amministrazione; contribuisce all'utilizzo di strumenti sofisticati di analisi; supporta l'utilizzo di strumenti innovativi. L'Insights Centre ha infatti consolidato nel tempo varie tecniche di facilitazione, pensiero visivo e attività di co-progettazione partecipativa di cui il RTI fa uso per implementare i servizi richiesti, dall'identificazione delle possibili vulnerabilità, alla gestione dei centri servizi e SOC, etc. Inoltre, **gli spazi degli Insights Centre**, qualora richiesto, **possono essere messi a disposizione dell'Amministrazione** per riunioni, meeting e servizi di formazione.

REEVO

Nell'ambito del RTI, ReeVo garantisce esperienza e competenza in ambito Cyber Security e conferisce un taglio innovativo ai servizi erogati, con particolare riferimento alla protezione, vigilanza e gestione dei dati. ReeVo ha realizzato una piattaforma proprietaria per l'orchestrazione e l'automazione degli elementi di Cyber Security. In tale ambito, grazie alle competenze specialistiche di ReeVo, il RTI potrà beneficiare del know how necessario per la realizzazione di playbook innovativi a supporto dell'integrazione e dell'automazione dei servizi di sicurezza nell'ambito della salvaguardia delle informazioni e nel monitoraggio costante della superficie di attacco.

HARUSPEX

L'innovazione portata dalla soluzione Haruspex all'intero processo di **Cyber Risk Assessment, Management e Remediation** consta di una piattaforma predittiva (H-PAR - Predict, Assess, Remediate), capace di identificare tutti i percorsi di attacco e di definire il numero minimo di contromisure per neutralizzare tutti i rischi, e di una soluzione H-CAP (Correlate, Attribute and Predict), che adotta una logica di monitoraggio continuo in grado di proteggere in modo proattivo un'infrastruttura da attacchi in corso. Nello specifico, la piattaforma H-CAP applica tecniche di **intelligenza artificiale** e **big data** per

fondere le informazioni che provengono dai sensori di intrusione, ad esempio SIEM e IDS, con quelle sui percorsi di attacco che sono calcolate proattivamente dalla piattaforma H-PAR. Dunque, la tecnologia messa a disposizione da Haruspex permette di fornire un taglio innovativo ai servizi SOC. Infatti, la fusione precedentemente descritta produce informazioni che consentono al SOC di prevedere i prossimi attacchi, anticipare l'obiettivo degli attacchi in corso e suggerire contromisure dinamiche per ridurre al minimo il rischio. Utilizzando H-CAP, il SOC può implementare dinamicamente contromisure solo quando e se sono necessarie per ridurre al minimo sia il rischio sia l'investimento in sicurezza. Grazie alla conoscenza dei percorsi di attacco, H-CAP può anche scoprire gli attaccanti che stanno sfruttando vulnerabilità 0-day e suggerire in tempo reale le contromisure in grado di proteggere le risorse critiche. Inoltre, H-CAP, integrando AI e digital twin, riduce drasticamente il numero di falsi positivi.

BOOLEBOX

Boolebox rappresenta un attore cruciale per la strategia della protezione dei dati sensibili con particolare riferimento alla protezione dei dati degli endpoint. Come descritto nel capitolo 13, il RTI ha maturato una consolidata esperienza nell'erogazione di servizi di protezione degli endpoint sia nel comparto della PA che nel mondo privato. Boolebox, pertanto, garantisce al RTI un taglio innovativo e strategico di rilievo nella protezione dei dati sensibili. Specificatamente, il RTI, avvalendosi di Boolebox, e delle soluzioni di "Data centric protection", che uniscono logiche di DRM (Digital Right Management), di DLP (Data Loss Prevention), di Encryption, Classification (Cifratura e classificazione dei dati) e funzionalità di CCP (Content Collaboration Platform), integra il processo di gestione sicura dei dati confidenziali degli endpoint delle Control Room del Centro Servizi.

BLUENET

Bluenet, grazie alla sua tecnologia innovativa, supporta il RTI nella predisposizione del servizio di timbro digitale proposto. Il timbro digitale di BlueNet, grazie ad un innovativo algoritmo di compressione e ad un sofisticato software di cifratura, rappresenta il riferimento di mercato per le soluzioni 2D Code con la maggiore densità di dati. BLUeCODE™ è la tecnologia brevettata della startup innovativa Bluenet s.r.l. che permette di creare un "codice bidimensionale" non falsificabile, stampabile con estrema semplicità, facile da apporre in documenti digitali. Di fatto, il BLUeCODE™ può essere utilizzato per memorizzare al suo interno informazioni destinate ad essere consultate e verificate rapidamente con uno smartphone, un tablet o PC. Può contenere una fotografia, testo, dati biometrici (impronta digitale, riconoscimento facciale) o altri tipi di dati, garantendo la protezione delle informazioni. Il BLUeCODE™ si propone come timbro elettronico di certificazione dei dati e allo stesso tempo strumento di protezione e verifica.

17.4. MODALITÀ ORGANIZZATIVE DEL COINVOLGIMENTO, IN TERMINI DI TEMPISTICHE DI INGAGGIO E MODALITÀ DI RELAZIONE CON LE AMMINISTRAZIONI

Il RTI prevede un coinvolgimento continuativo delle realtà innovative sopracitate per l'intera durata contrattuale attraverso un processo di interazione continua con l'Amministrazione che prevede tra l'altro:

- **L'organizzazione di allineamenti mensili tra l'Amministrazione, i soggetti coinvolti e il RTI volti a** garantire un **corretto flusso comunicativo** e un **costante aggiornamento dei temi, delle attività e delle eventuali criticità rilevate**. Agli allineamenti, effettuati in **modalità online**, partecipano **il referente dell'Amministrazione, un referente del RTI e i rappresentanti dei Centri coinvolti a livello di Contratto Esecutivo**. Il fine dell'allineamento non è semplicemente quello di valutare le attività in essere, ma di **riflettere su eventuali estensioni dell'attività** in diversi ambiti al fine di garantire una **contaminazione coerente** tra gli ambiti di interesse per la stessa Amministrazione. Per ogni allineamento viene predisposta **un'agenda del giorno** preventivamente concordata con l'Amministrazione.
- **Allineamenti bisettimanali on-line** della durata di venti minuti **con i soggetti coinvolti e il RTI.** Per **garantire l'apporto di un concreto valore aggiunto attraverso il coinvolgimento delle realtà proposte.** In tale contesto, vengono valutati **eventuali elementi rilevanti da sottoporre all'attenzione delle Amministrazioni contraenti**.

Lo scopo degli allineamenti è quello di **garantire la continua e costante innovazione** su specifiche fasi di erogazione dei servizi e di creare un flusso comunicativo quanto più aggiornato possibile. Le **tempistiche e i luoghi di esecuzione** degli allineamenti potranno variare secondo le necessità dell'Amministrazione e del RTI. I soggetti coinvolti garantiscono massima disponibilità al RTI e all'Amministrazione, assicurando l'ingaggio immediato ogni qualvolta ritenuto necessario dalle Parti.

Le start-up innovative Cyber Guru e Bluenet hanno già in essere dei rapporti continuativi di collaborazione con le aziende del RTI, operando in modo integrato con i Competence Center e le factory del RTI,

Le Boolebox e Haruspex sono state selezionate seguendo il processo del Funnel Model descritto al §17.1.

18. MIGLIORAMENTO SOGLIE INDICATORI DI QUALITA' - TIIS – TEMPO DI PRIMA INVESTIGAZIONE PER INCIDENTI DI SICUREZZA

Il RTI dichiara l'impegno a garantire i seguenti valori di soglia: ✓Gravità Alta, **TIIS <=2 ore solari**; ✓Gravità Media, **TIIS <=4 ore solari**.

19. MIGLIORAMENTO SOGLIE INDICATORI DI QUALITA' - TCIS – TEMPO DI PRIMO CONTENIMENTO PER INCIDENTI DI SICUREZZA

Il RTI dichiara l'impegno a garantire i seguenti valori di soglia: ✓Gravità Alta, **TCIS <=6 ore solari**; ✓Gravità Media, **TCIS <=10 ore solari**.

20. ASSUNZIONE DELLE RISORSE PROFESSIONALI

Il RTI dichiara l'impegno ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione dei contratti esecutivi o per la realizzazione di attività ad essi connessi o strumentali, in una quota, 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, **maggiore del 35%.**

acquistinretepa.it
Il Portale degli acquisti della Pubblica Amministrazione

Offerta economica relativa a:	
Numero Gara	2860125
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 Capitolato d'Oneri - Documento
Criterio di Aggiudicazione	Gara ad offerta economicamente più vantaggiosa
Lotto	1 (Servizi di sicurezza da remoto)

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	TELECOM ITALIA SPA (mandataria) Società per Azioni
Partita IVA	00488410010
Codice Fiscale Impresa	00488410010
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	00488410010
Codice Ditta INAIL	3441073
n. P.A.T.	08315476
Matricola aziendale INPS	7036858465

CCNL applicato	IMPRESE ESERCENTI SERVIZI DI TELECOMUNICAZIONE
Settore	TELECOMUNICAZIONI
Indirizzo sede legale	VIA GAETANO NEGRI, 1 - MILANO (MI)
Telefono	800333666
Fax	800333669
PEC Registro Imprese	GESTIONE.CONVENZIONI@PEC.TELECOMITALIA.IT
Ragione Sociale	ALMAVIVA - THE ITALIAN INNOVATION COMPANY S.P.A. (mandante) Società per Azioni
Partita IVA	08450891000
Codice Fiscale Impresa	08450891000
Provincia sede registro imprese	RM
Numero iscrizione registro imprese	08450891000
Codice Ditta INAIL	14143831
n. P.A.T.	92251495/18 - 020520624/97 - 92631330/36 - 91784932/98 - 020914283/58 - 20969526/53 - 92772483/20 - 21270646/68 - 21270645/11 - 21271086/36
Matricola aziendale INPS	7051122457 - 7051122255 - 7052668664 - 7058273176 - 7058882329
CCNL applicato	METALMECCANICI
Settore	INDUSTRIA
Indirizzo sede legale	VIA DI CASAL BOCCONE 188/190 - ROMA (RM)
Telefono	0639931
Fax	0639935266
PEC Registro Imprese	ALMAVIVA@PEC.ALMAVIVA.IT
Ragione Sociale	KPMG ADVISORY SPA (mandante) Società per Azioni
Partita IVA	04662680158
Codice Fiscale Impresa	04662680158
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	04662680158
Codice Ditta INAIL	5164646/69
n. P.A.T.	10917335/59 (VIDEO TERMINALI) - 06382739/04

	(AUTO)
Matricola aziendale INPS	4931133619 (PRINCIPALE) - 4957312542 - 4972845449
CCNL applicato	COMMERCIO
Settore	TERZIARIO
Indirizzo sede legale	VIA VITTOR PISANI N. 27 - MILANO (MI)
Telefono	02676431
Fax	0267643603
PEC Registro Imprese	KPMGADVISORYSPA.UFFICIOGARE@PEC.KPMG.IT
Ragione Sociale	NETGROUP SRL (mandante) Società a Responsabilità Limitata
Partita IVA	03008301214
Codice Fiscale Impresa	03008301214
Provincia sede registro imprese	NA
Numero iscrizione registro imprese	536345
Codice Ditta INAIL	4785898
n. P.A.T.	11304675 33; 20247259 95; 20423013 53; 21541970 32; 21556225; 20388131 60; 20168956 31; 20482609 93
Matricola aziendale INPS	5120114426
CCNL applicato	METALMECCANICO CONF.
Settore	PRODUZIONE SOFTWARE
Indirizzo sede legale	PONTECITRA,23 - MARIGLIANO (NA)
Telefono	0818856967
Fax	0818856194
PEC Registro Imprese	GMOCERINO@NETGROUP.IT
Ragione Sociale	REEVO SPA (mandante) Società per Azioni
Partita IVA	03888200965
Codice Fiscale Impresa	03888200965
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	1710741
Codice Ditta INAIL	013595018/28

n. P.A.T.	91024233/26
Matricola aziendale INPS	4965103549
CCNL applicato	COMMERCIO
Settore	COMMERCIO
Indirizzo sede legale	VIA DANTE, 4 - MILANO (MI)
Telefono	0392873925
Fax	0392875471
PEC Registro Imprese	REEVO@PEC.IT
Offerta sottoscritta da	**CAPPELLETTI ANDREA, AMATI ANTONIO, GESUELE SALVATORE, MATERAZZI MASSIMILIANO, SALVATORE GIANNETTO**

Scheda di Offerta	
Descrizione	Servizi di sicurezza da remoto - offerta economica
Offerta Economica	
Parametro Richiesto	**Valore Offerto**
1 - L1.S1 - Security Operation Center (SOC) - Fascia 1 - Fino a 300 Eps - Prezzo unitario offerto (€)	127,3
2 - L1.S1 - Security Operation Center (SOC) - Fascia 2 - Fino a 600 Eps - Prezzo unitario offerto (€)	283,2
3 - L1.S1 - Security Operation Center (SOC) - Fascia 3 - Fino a 1.200 Eps - Prezzo unitario offerto (€)	285
4 - L1.S1 - Security Operation Center (SOC) - Fascia 4 - Fino a 6.000 Eps - Prezzo unitario offerto (€)	260
5 - L1.S1 - Security Operation Center (SOC) - Fascia 5 - > 6.000 Eps - Prezzo unitario offerto (€)	250
6 - L1.S2 - Next Generation FW - Fascia 1 - Fino a 250 Mbps - Prezzo unitario offerto (€)	292,92
7 - L1.S2 - Next Generation FW - Fascia 2 - Fino a 2 Gbps - Prezzo unitario offerto (€)	846,29
8 - L1.S2 - Next Generation FW - Fascia 3 - Fino a 4 Gbps - Prezzo unitario offerto (€)	2375,95
9 - L1.S2 - Next Generation FW - Fascia 4 - Fino a 7 Gbps - Prezzo unitario offerto (€)	3919,51
10 - L1.S2 - Next Generation FW - Fascia 5 - Fino a 15 Gbps - Prezzo unitario offerto (€)	17666,41
11 - L1.S2 - Next Generation FW - Fascia 6 - > 15 Gbps - Prezzo unitario offerto (€)	45041,24
12 - L1.S3 - Web Application FW - Fascia 1 - Fino a 500 Mbps - Prezzo unitario offerto (€)	6964
13 - - Fascia 2 - Fino a 5 Gbps - Prezzo unitario offerto (€)	21000
14 - - Fascia 3 - > 5 Gbps - Prezzo unitario offerto (€)	34000
15 - L1.S4 -Gestione continua delle	34,87

vulnerabilità di sicurezza - Fascia 1 - Fino a 50 IP - Prezzo unitario offerto (€)	
16 - - Fascia 2 - Fino a 200 IP - Prezzo unitario offerto (€)	21,25
17 - - Fascia 3 - > 200 IP - Prezzo unitario offerto (€)	14,432
18 - L1.S5 -Threat Intelligence & Vulnerability Data Feed - Fascia 1 - fino a 10 datafeed - Prezzo unitario offerto (€)	361,24
19 - L1.S5 -Threat Intelligence & Vulnerability Data Feed - Fascia 2 - fino a 50 datafeed - Prezzo unitario offerto (€)	181,26
20 - L1.S5 -Threat Intelligence & Vulnerability Data Feed - Fascia 3 - > 50 datafeed - Prezzo unitario offerto (€)	125,95
21 - L1.S6 - Protezione navigazione Internet e Posta elettronica - Fascia 1 - Fino a 1.000 utenti - Prezzo unitario offerto (€)	2,75
22 - - Fascia 2 - Fino a 5.000 utenti - Prezzo unitario offerto (€)	1,78
23 - - Fascia 3 - Fino a 10.000 utenti - Prezzo unitario offerto (€)	1,83
24 - - Fascia 4 - Fino a 20.000 utenti - Prezzo unitario offerto (€)	1,59
25 - - Fascia 5 - > 20.000 utenti - Prezzo unitario offerto (€)	0,89
26 - L1.S7 -Protezione End point - Fascia 1 - Fino a 500 nodi - Prezzo unitario offerto (€)	26,124
27 - - Fascia 2 - Fino a 1.000 nodi - Prezzo unitario offerto (€)	24,097
28 - - Fascia 3 - Fino a 5.000 nodi - Prezzo unitario offerto (€)	19,783
29 - - Fascia 4 - > 5.000 nodi - Prezzo unitario offerto (€)	17,096
30 - L1.S8 -Certificati SSL - SSL OV - Prezzo unitario offerto (€)	22
31 - L1.S8 -Certificati SSL - SSL OV Wildcard - Prezzo unitario offerto (€)	74
32 - L1.S8 -Certificati SSL - SSL EV - Prezzo unitario offerto (€)	90
33 - L1.S8 -Certificati SSL - SSL DV - Prezzo unitario offerto (€)	16

34 - L1.S8 -Certificati SSL - SSL Code signing - Prezzo unitario offerto (€)	50
35 - L1.S8 -Certificati SSL - SSL Client Auth - Prezzo unitario offerto (€)	8
36 - L1.S9 -Formazione e security awareness - gg/p Team ottimale - Prezzo unitario offerto (€)	231
37 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 1 - Fino a 10.000 utenti - Prezzo unitario offerto (€)	0,399
38 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 2 - Fino a 100.000 utenti - Prezzo unitario offerto (€)	0,330
39 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 3 - Fino a 500.000 utenti - Prezzo unitario offerto (€)	0,249
40 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 4 - > 500.000 utenti - Prezzo unitario offerto (€)	0,154
41 - L1.S11 - Firma digitale remota - Fascia 1 - > 50 e fino a 200 utenti - Prezzo unitario offerto (€)	7,1
42 - L1.S11 - Firma digitale remota - Fascia 2 - > 200 e fino a 500 utenti - Prezzo unitario offerto (€)	6,8
43 - L1.S11 - Firma digitale remota - Fascia 3 - > 500 e fino a 1.000 utenti - Prezzo unitario offerto (€)	6,6
44 - L1.S11 - Firma digitale remota - Fascia 4 - > 1.000 utenti - Prezzo unitario offerto (€)	6,2
45 - L1.S11 - Firma digitale remota - Garantita - N. 1 firma - Prezzo unitario offerto (€)	5800
46 - L1.S11 - Firma digitale remota - Garantita - N. 5 firme aggiuntive - Prezzo unitario offerto (€)	13500
47 - L1.S12 -Sigillo elettronico - Garantita - N. 1 firma - Prezzo unitario offerto (€)	5800
48 - L1.S12 -Sigillo elettronico - Garantita - N. 5 firme aggiuntive - Prezzo unitario offerto (€)	13500

49 - L1.S13 - Timbro elettronico - Fascia 1 - Fino a 1.000 timbrature - Prezzo unitario offerto (€)	0,78
50 - L1.S13 - Timbro elettronico - Fascia 2 - Fino a 10.000 timbrature - Prezzo unitario offerto (€)	0,78
51 - L1.S13 - Timbro elettronico - Fascia 3 - Fino a 100.000 timbrature - Prezzo unitario offerto (€)	0,72
52 - L1.S13 - Timbro elettronico - Fascia 4 - Fino a 1.000.000 timbrature - Prezzo unitario offerto (€)	0,6
53 - L1.S13 - Timbro elettronico - Fascia 5 - Fino a 10.000.000 timbrature - Prezzo unitario offerto (€)	0,008
54 - L1.S13 - Timbro elettronico - Fascia 6 - > 10.000.000 timbrature - Prezzo unitario offerto (€)	0,007
55 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 1 - Fino a 1.000 Marcature - Prezzo unitario offerto (€)	0,05
56 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 2 - Fino a 10.000 Marcature - Prezzo unitario offerto (€)	0,04
57 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 3 - Fino a 100.000 Marcature - Prezzo unitario offerto (€)	0,027
58 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 4 - Fino a 1.000.000 Marcature - Prezzo unitario offerto (€)	0,009
59 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 5 - Fino a 10.000.000 Marcature - Prezzo unitario offerto (€)	0,005
60 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 6 - > 10.000.000 Marcature - Prezzo unitario offerto (€)	0,004
61 - L1.S14 - Validazione temporale elettronica qualificata - Garantita - N. 1 marcatura - Prezzo unitario offerto (€)	5000

62 - L1.S14 - Validazione temporale elettronica qualificata - Garantita - N. 1 marcatura aggiuntiva - Prezzo unitario offerto (€)	5000
63 - L1.S15 -Servizi specialistici - gg/p Team ottimale - Prezzo unitario offerto (€)	235
Ribasso medio ponderato - Calcolato dal Sistema	0,50523

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

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 1 - Servizi di sicurezza da remoto per le Pubbliche Amministrazioni Centrali (PAC)

Servizio	Voce economica	Id voce	Prezzo offerto
L1.S1 - Security Operation Center (SOC)	Fascia 1 - Fino a 300 Eps	1	€ 127,30
	Fascia 2 - Fino a 600 Eps	2	€ 283,20
	Fascia 3 - Fino a 1.200 Eps	3	€ 285,00
	Fascia 4 - Fino a 6.000 Eps	4	€ 260,00
	Fascia 5 - > 6.000 Eps	5	€ 250,00
L1.S2 - Next Generation FW	Fascia 1 - Fino a 250 Mbps	6	€ 292,92
	Fascia 2 - Fino a 2 Gbps	7	€ 846,29
	Fascia 3 - Fino a 4 Gbps	8	€ 2.375,95
	Fascia 4 - Fino a 7 Gbps	9	€ 3.919,51
	Fascia 5 - Fino a 15 Gbps	10	€ 17.666,41
	Fascia 6 - > 15 Gbps	11	€ 45.041,24
L1.S3 - Web Application FW	Fascia 1 - Fino a 500 Mbps	12	€ 6.964,00
	Fascia 2 - Fino a 5 Gbps	13	€ 21.000,00
	Fascia 3 - > 5 Gbps	14	€ 34.000,00
L1.S4 - Gestione continua delle vulnerabilità di sicurezza	Fascia 1 - Fino a 50 IP	15	€ 34,87
	Fascia 2 - Fino a 200 IP	16	€ 21,25
	Fascia 3 - > 200 IP	17	€ 14,432
L1.S5 - Threat Intelligence & Vulnerability Data Feed	Fascia 1 - fino a 10 datafeed	18	€ 361,24
	Fascia 2 - fino a 50 datafeed	19	€ 181,26
	Fascia 3 - > 50 datafeed	20	€ 125,95
	Fascia 1 - Fino a 1.000 utenti	21	€ 2,75

L1.S6 - Protezione navigazione Internet e Posta elettronica	Fascia 2 - Fino a 5.000 utenti	22	€ 1,78
	Fascia 3 - Fino a 10.000 utenti	23	€ 1,83
	Fascia 4 - Fino a 20.000 utenti	24	€ 1,59
	Fascia 5 - > 20.000 utenti	25	€ 0,89
L1.S7 - Protezione End point	Fascia 1 - Fino a 500 nodi	26	€ 26,124
	Fascia 2 - Fino a 1.000 nodi	27	€ 24,097
	Fascia 3 - Fino a 5.000 nodi	28	€ 19,783
	Fascia 4 - > 5.000 nodi	29	€ 17,096
L1.S8 - Certificati SSL	SSL OV	30	€ 22,00
	SSL OV Wildcard	31	€ 74,00
	SSL EV	32	€ 90,00
	SSL DV	33	€ 16,00
	SSL Code signing	34	€ 50,00
	SSL Client Auth	35	€ 8,00
L1.S9 - Formazione e security awareness	gg/p Team ottimale	36	€ 231,00
L1.S10 - Gestione dell'identità e l'accesso utente	Fascia 1 - Fino a 10.000 utenti	37	€ 0,399
	Fascia 2 - Fino a 100.000 utenti	38	€ 0,330
	Fascia 3 - Fino a 500.000 utenti	39	€ 0,249
	Fascia 4 - > 500.000 utenti	40	€ 0,154
L1.S11 - Firma digitale remota	Fascia 1 - > 50 e fino a 200 utenti	41	€ 7,10
	Fascia 2 - > 200 e fino a 500 utenti	42	€ 6,80
	Fascia 3 - > 500 e fino a 1.000 utenti	43	€ 6,60
	Fascia 4 - > 1.000 utenti	44	€ 6,20
	Garantita - N. 1 firma	45	€ 5.800,00
	Garantita - N. 5 firme aggiuntive	46	€ 13.500,00
L1.S12 - Sigillo elettronico	Garantita - N. 1 firma	47	€ 5.800,00
	Garantita - N. 5 firme aggiuntive	48	€ 13.500,00
	Fascia 1 - Fino a 1.000 timbrature	49	€ 0,78

L1.S13 - Timbro elettronico	Fascia 2 - Fino a 10.000 timbrature	50	€ 0,78
	Fascia 3 - Fino a 100.000 timbrature	51	€ 0,72
	Fascia 4 - Fino a 1.000.000 timbrature	52	€ 0,60
	Fascia 5 - Fino a 10.000.000 timbrature	53	€ 0,008
	Fascia 6 - > 10.000.000 timbrature	54	€ 0,007
L1.S14 - Validazione temporale elettronica qualificata	Fascia 1 - Fino a 1.000 Marcature	55	€ 0,05
	Fascia 2 - Fino a 10.000 Marcature	56	€ 0,04
	Fascia 3 - Fino a 100.000 Marcature	57	€ 0,027
	Fascia 4 - Fino a 1.000.000 Marcature	58	€ 0,009
	Fascia 5 - Fino a 10.000.000 Marcature	59	€ 0,005
	Fascia 6 - > 10.000.000 Marcature	60	€ 0,004
	Garantita - N. 1 marcatura	61	€ 5.000,00
	Garantita - N. 1 marcatura aggiuntiva	62	€ 5.000,00
L1.S15 - Servizi specialistici	gg/p Team ottimale	63	€ 235,00

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 1

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.

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.

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO F

ID 2296

SCHEMA DI CONTRATTO ESECUTIVO – LOTTO 1

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 1 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 6.4 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 7.3 del Capitolato Tecnico Speciale (2A).

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)

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 -

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 -

ACCORDO DI AVVALIMENTO

TRA

Telecom Italia S.p.A., con sede legale in Milano, Via Gaetano Negri 1, Codice Fiscale e Partita IVA ed iscrizione presso il Registro delle Imprese di Milano n. 00488410010, iscrizione al Registro A.E.E. n. IT08020000000799, rappresentata per la sottoscrizione del presente Accordo da Massimiliano Materazzi, in qualità di procuratore speciale, di seguito denominata per brevità "Telecom Italia" o “Impresa Ausiliata”

E

Telecom Italia Trust Technologies S.r.l., con sede legale in Pomezia (RM) S. R. 148 Pontina km 29,100, Codice Fiscale e Partita IVA ed iscrizione presso il Registro delle Imprese di Roma n. 04599340967, iscrizione REA n. RM - 1085826, rappresentata da Salvatore Nappi, in qualità di Amministratore Delegato e Rappresentante Legale, di seguito denominata per brevità "Impresa Ausiliaria” o “I.A.”;

(di seguito anche denominate collettivamente “le Parti”)

Premesso che

1. Telecom Italia è società che opera nel settore delle telecomunicazioni e che dispone pertanto di tutte le competenze ed il know-how necessario allo studio, progettazione e messa a punto di soluzioni tecnologiche avanzate, basati anche su applicativi software evoluti, che consentono prestazioni e funzionalità per servizi globali nel campo dell’innovazione tecnologica, nonché per erogare servizi di progettazione e affiancamento alla transizione digitale attraverso strumenti, consulenza e formazione;

2. I.A. è una società che si occupa dello sviluppo e l’integrazione delle soluzioni di identità e validazione digitale delle persone e delle cose e la gestione del ciclo di vita dei dati e dei documenti in modalità conformi alle normative Italiane ed Europee ed è società appartenente al Gruppo Telecom, controllata da Telecom Italia e sottoposta alla sua direzione e coordinamento;

3. l’Ente Appaltante Consip S.p.A. ha pubblicato su GUUE serie S n. 178 del 14/09/2021 e su GURI n. 108 del 17/09/2021 il bando di 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 Sigef 2296 CIG Lotto 1 88846293CA, CIG Lotto 2 8884642E81” (di seguito per brevità la “Gara”);

4. I.A. possiede i requisiti e le risorse previste, così come meglio descritte nel successivo Art. 2 “Oggetto dell’Accordo” idonei alla partecipazione della summenzionata Gara ed a tal fine rende contestualmente alla sottoscrizione del presente Accordo la “Dichiarazione Integrativa di Avvalimento” (allegata);

5. scopo del presente Accordo è dato dall’interesse di Telecom Italia a partecipare al Lotto 1 della Gara, avvalendosi delle risorse/certificazioni/requisiti dell’Impresa Ausiliaria in relazione a quanto previsto dal punto III.1.3) “Capacità professionale e tecnica” del bando di gara e dettagliato nel paragrafo 7.3, lettera d) “Requisiti di

capacità tecnica e professionale" del Capitolato d'oneri, ed in particolare al *"possesso di una valutazione di conformità del proprio sistema di gestione della sicurezza delle informazioni alla/e norma/e ISO 27001 nel settore/ambito IAF 33, idonea, pertinente e proporzionata al seguente ambito di attività: progettazione, realizzazione ed erogazione di servizi di sicurezza gestiti."*

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

Art. 1. Premesse ed allegati

Le Premesse e gli Allegati sono parte integrante e sostanziale del presente Accordo.

Art. 2. Oggetto dell'Accordo

2.1. Tra l'Impresa Ausiliata e l'Impresa Ausiliaria si stipula un contratto di avvalimento, in base all'art. 89 del D.Lgs. 18 aprile 2016 n. 50 e s.m.i., ai seguenti patti e condizioni:

L'impresa Ausiliaria, presa visione ed esatta conoscenza dei documenti di Gara, si impegna a mettere a disposizione dell'Impresa Ausiliata, dell'Ente Appaltante e delle Pubbliche Amministrazioni aderenti all'Accordo Quadro (di seguito "Amministrazioni Contraenti"), ai fini della partecipazione dell'Impresa Ausiliata alla Gara e, in caso di aggiudicazione, per tutta la durata dell'appalto di cui alla Gara, in riferimento al requisito di cui al § III.1.3.) del Bando di Gara la propria certificazione di conformità del sistema di gestione della sicurezza delle informazioni n. 9194.ITTM, conforme alle norme UNI EN ISO 27001:2013, in corso di validità, per le attività di progettazione, realizzazione ed erogazione di servizi di sicurezza gestiti, nonché tutte le strutture, le tecniche, i fattori della produzione e le risorse che, complessivamente considerati, le hanno consentito di acquisire la predetta certificazione tra cui know how, consulenza e formazione professionale da parte di personale qualificato, strutture tecnico-organizzative, tecniche operative, audit periodicamente effettuati e tutte le procedure di sistema messe in atto per conseguire e mantenere la validità della certificazione.

In particolare, l'Impresa Ausiliaria si impegna a mettere a disposizione dell'Impresa Ausiliata, dell'Ente Appaltante e delle Amministrazioni Contraenti la detta Certificazione conforme alla norma ISO 27001:2013 il cui scopo comprende la progettazione, realizzazione ed erogazione di servizi di sicurezza gestiti, specificatamente per "Progettazione, sviluppo, system integration, delivery ed esercizio – anche in modalità SaaS con l'utilizzo delle linee guida ISO/IEC 27017:2015 e ISOIEC 27018:2019 – di soluzioni e servizi informatici, anche basati sulle tecnologie di crittografia a chiave pubblica, ivi compresi firma elettronica, sigillo elettronico, conservazione a norma di documenti informatici, Posta Elettronica Certificata, identità digitale in ambito SPID e soluzioni di firma elettronica avanzata, anche basate su sistemi biometrici"

Ed in particolare verranno messi a disposizione i seguenti mezzi (e relativi siti di ubicazione) inclusi nel Certificato 9194.ITTM:

- *Sito di Pomezia (S.S Pontina Km 29,100 – 00097 Pomezia - RM): infrastrutture e sistemi*
    - Risorse computazionali: 1858GHz; RAM: 12Tb
    - Capacità Storage: NFS 1.1Pb, FC: 208Tb
    - Software di virtualizzazione: VmWare

- Console di monitoraggio e gestione
- Banda (front-end/back.end): 1Gbit/s

- *Sito Roma (Via Oriolo Romano 257 – 00189 Roma): infrastrutture e sistemi*
  - Risorse computazionali: 378GHz, RAM: 1Tb
  - Capacità Storage: NFS: 1.1Pb, FC: 400TB Free
  - Software di virtualizzazione: VmWare
  - Console di monitoraggio e gestione
  - Banda (front-end/back.end) : 1Gbit/s
  -

- Risorse Professionali:
  - N. 2 Professional di elevata specializzazione ed esperienza
  - N. 3 ICT System Architect Senior
  - N. 7 Specialista esperto di soluzioni informatiche
  - N. 4 Specialista di attività tecniche integrate
  - N. 2 Specialista di attività tecniche

L'Impresa Ausiliaria si impegna altresì:

- ad assicurare all'Impresa Ausiliata, all'Ente Appaltante ed alle Amministrazioni Contraenti la disponibilità delle risorse per attuare e monitorare i processi definiti per l'esecuzione e il controllo delle attività di progettazione, realizzazione ed erogazione di servizi di sicurezza gestiti funzionali alla fornitura ed all'erogazione dei servizi di gara secondo gli standard;
- ad assicurare all'Impresa Ausiliata, all'Ente Appaltante ed alle Amministrazioni Contraenti periodica attività di sensibilizzazione e a promuovere attività di formazione/addestramento;
- a definire i parametri di misurazione e controllo per le attività di monitoraggio, e analisi dei processi;
- a pianificare e ad eseguire periodicamente audit interni allo scopo di verificare la conformità dei processi aziendali rispetto ai requisiti delle norme di riferimento, di verificare il raggiungimento delle performance e degli obiettivi desiderati, nonché di fornire uno strumento sistematico di verifica e identificare le aree di potenziale miglioramento;
- nel caso di rilievo di anomalie a definire e a realizzare idonee azioni correttive relativamente alle carenze evidenziate.

2.2. L'Impresa Ausiliata è autorizzata ad utilizzare il requisito innanzi detto per partecipare alla Gara e, in caso di aggiudicazione, per eseguire le prestazioni oggetto del contratto.

2.3. L'I.A. si impegna a non mettere a disposizione di altri partecipanti alla medesima Gara i propri requisiti.

2.4. In conformità a quanto previsto dal comma 9 dell'Art. 89 del D. L.vo 18 aprile 2016 n. 50 e s.m.i., l'I.A. dà atto ed espressamente accetta che l'Ente Appaltante e le Amministrazioni Contraenti, per l'intera durata dell'Accordo Quadro eventualmente aggiudicato a Telecom Italia (di seguito il "Contratto") eseguiranno le verifiche

sostanziali circa l'effettivo possesso da parte dell'I.A. dei requisiti e delle risorse oggetto dell'avvalimento, nonché circa l'effettivo impiego delle risorse medesime nell'esecuzione dell'appalto. l'I.A. da' atto ed espressamente accetta che l'Ente Appaltante e le Amministrazioni contraenti possano accertare in corso d'opera che le prestazioni oggetto del Contratto siano svolte direttamente dalle risorse dell'I.A.

2.5. Resta espressamente inteso che Telecom Italia riconoscerà all'I.A., in caso di aggiudicazione in via definitiva della Gara e stipulazione del relativo contratto di appalto (di seguito "Contratto") il ruolo di Subfornitore/Subappaltatore in base alle norme applicabili, definendo anche i rapporti economici derivanti dagli obblighi di cui ai precedenti punti con separato specifico contratto di Subfornitura/subappalto, fermo restando che la messa a disposizione del requisito, risorse e mezzi avviene a titolo oneroso e che i corrispettivi saranno quindi determinati sulla base della prassi dei rapporti commerciali e di servizio già esistenti tra la capogruppo Telecom Italia e l'IA controllata e sottoposta alla sua direzione e coordinamento.

2.6. Ai fini di quanto previsto al precedente paragrafo 2.4, l'I.A. dichiara di non essere stata indicata come ausiliaria da altri concorrenti alla Gara e/o di non essersi impegnata ad assumere il ruolo di subappaltatore con nessun altro concorrente alla Gara.

2.7. L'Impresa Ausiliata e l'Impresa Ausiliaria sono responsabili in solido nei confronti dell'Ente Appaltante in relazione alle prestazioni oggetto del contratto.

Art. 3. Durata

3.1. Il presente Accordo decorrerà dalla data della sua sottoscrizione ed avrà efficacia per tutta la durata dell'appalto di cui al precedente punto 3 delle premesse, sino all'estinzione di tutte le obbligazioni pendenti tra le Parti e/o nei confronti dell'Ente Appaltante e/o delle Amministrazioni Contraenti in base all'Accordo Quadro stipulato tra Telecom Italia e l'Ente Appaltante medesimo.

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 da Telecom Italia;
- alla data dell'eventuale annullamento, in via definitiva e non soggetto ad impugnativa, della procedura di Gara;
- nel caso di aggiudicazione della Gara a Telecom Italia, 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, le Amministrazioni Contraenti e Telecom Italia stessa, ovvero qualora si verifichi altra causa di cessazione degli effetti giuridici o di estinzione del Contratto stipulato tra Telecom Italia e l'Ente Appaltante.

Art. 4. Proprietà Intellettuale

4.1. Le Parti convengono sin da ora che, compatibilmente con le previsioni della documentazione di Gara, 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.

4.2. Qualora nell'ambito delle attività previste nel presente Accordo ed in esecuzione dello stesso 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 Telecom Italia e dell' I.A. 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 anni 2.

5.3. Qualora la diffusione presso terzi di materiale o di informazioni ritenuti riservati, sia stato causato 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 Contratto, 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 Regolamento 2016/679/EU (Regolamento generale sulla protezione dei dati) e dell'ulteriore normativa applicabile sulla protezione dei dati

personali con modalità idonee a garantirne la sicurezza e la riservatezza.
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 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.

6.2. Nel rispetto di quanto previsto all'art. 89 del D.Lgsvo 50/2016 e dal punto 2.2 che precede, il presente Accordo non stabilisce alcuna esclusiva a carico delle Parti.

6.3. I.A si impegna a manlevare e tenere indenne Telecom Italia da qualsiasi conseguenza derivante dal mancato rispetto di quanto previsto nel presente Accordo.

6.4. Per tutto quanto non espressamente previsto dal presente Accordo, troveranno applicazione le disposizioni di cui all'Art. 89 del D.Lgsvo 50/2016 e s.m.i. .

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 e delle Amministrazioni contraenti.

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. Lgsvo 231/2001 dichiarano:

a) di essere a conoscenza della normativa in materia di responsabilità amministrativa delle società, ed in particolare di quanto stabilito al riguardo dal decreto del D. Lgs. n. 231/2001;

b) di essere a conoscenza dell'avvenuta adozione, da parte di entrambe, di un modello di organizzazione gestione e controllo ai sensi delle suddette disposizioni, reperibile sul seguente sito web
http://www.telecomitalia.com/tit/it/vendorshub/archivio-documenti.html

c) di essere a conoscenza dei contenuti e dei principi espressi nei rispettivi codice etici, che ne costituiscono parte integrante;

d) di obbligarsi a rispettare, nei rapporti reciproci, detti contenuti e detti principi;

Le Parti si obbligano perciò a non porre in essere, e a far sì che anche i propri dipendenti e/o collaboratori non pongano in essere, atti o comportamenti che rappresentino una violazione dei rispettivi codici etici, nonché più in generale atti o comportamenti che potrebbero condurre alla commissione, anche solo tentata, dei reati contemplati dal D.Lgs. 231/2001.

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 affinché 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 Contratto sarà competente in via esclusiva il Foro di Roma.

8.3. In ogni caso, anche nel caso di insorgenza di una controversia, l'I.A. si impegna a lasciare comunque a disposizione di Telecom Italia e dell'Ente Appaltante e delle Amministrazioni contraenti le proprie certificazioni e risorse oggetto del presente Accordo, salvo poi rivalersi nei confronti dell'Impresa Ausiliata.

Art. 9. Cessione e modifiche

9.1. Qualsiasi modifica, aggiunta o cancellazione a questo Accordo sarà valida ed effettiva solo previo pattuizione scritta tra i legali rappresentanti o persone munite dei necessari poteri di ciascuna delle Parti.

9.2. Le Parti non potranno cedere il presente Accordo.

Art. 10. Comunicazioni relative all'Accordo

Tutte le comunicazioni, notizie ed informazioni saranno comunicate per iscritto tra le Parti ai seguenti indirizzi:

Telecom Italia S.p.A.
CR.EM.PS.MC
Via di Val Cannuta 182

00166 ROMA
c.a. Massimiliano Materazzi
e-mail massimiliano.materazzi@telecomitalia.it
PEC massimiliano.materazzi@pec.telecomitalia.it

Telecom Italia Trust Technologies S.r.l.
S.R. 148 Pontina Km 29,100
00071 Pomezia (RM)
c.a. Marco Pitorri
e-mail marco.pitorri@telecomitalia.it
PEC ti.tt@ttpec.telecomitalia.it

Per Telecom Italia S.p.A. Per **Telecom Italia Trust Technologies S.r.l.**

Massimiliano Materazzi Salvatore Nappi

DOCUMENTO FIRMATO DIGITALMENTE

ACCORDO DI AVVALIMENTO

TRA

Telecom Italia S.p.A., con sede legale in Milano, Via Gaetano Negri 1, Codice Fiscale e Partita IVA ed iscrizione presso il Registro delle Imprese di Milano n. 00488410010, iscrizione al Registro A.E.E. n. IT08020000000799, rappresentata per la sottoscrizione del presente Accordo da Massimiliano Materazzi, in qualità di procuratore speciale, di seguito denominata per brevità "Telecom Italia" o “Impresa Ausiliata”

E

Noovle S.p.A. Società Benefit, con sede legale in Milano, Via Gaetano Negri 1, Codice Fiscale e Partita IVA ed iscrizione presso il Registro delle Imprese di Milano n. 11432040969, iscrizione REA n. MI - 2601962, rappresentata da Carlo D’Asaro Biondo, nella Sua qualità di Amministratore Delegato e Rappresentante Legale, di seguito denominata per brevità "Impresa Ausiliaria” o “I.A.”;

(di seguito anche denominate collettivamente “le Parti”)

Premesso che

1. Telecom Italia è società che opera nel settore delle telecomunicazioni e che dispone pertanto di tutte le competenze ed il know-how necessario allo studio, progettazione e messa a punto di soluzioni tecnologiche avanzate, basati anche su applicativi software evoluti, che consentono prestazioni e funzionalità per servizi globali nel campo dell’innovazione tecnologica, nonché per erogare servizi di progettazione e affiancamento alla transizione digitale attraverso strumenti, consulenza e formazione;

2. I.A. è una società appartenente al Gruppo Telecom, controllata da Telecom Italia e sottoposta alla sua direzione e coordinamento, operante nell’ambito dei servizi Cloud a supporto della trasformazione digitale delle aziende pubbliche e private italiane. I.A. è in grado di offrire risorse, servizi e soluzioni dall’infrastruttura all’applicazione, garantisce la realizzazione di soluzioni innovative private, hybrid, multicloud assicurando la gestione in sicurezza e localizzata in Italia dei dati pubblici e privati.

3. l’Ente Appaltante Consip S.p.A. ha pubblicato su GUUE serie S n. 178 del 14/09/2021 e su GURI n. 108 del 17/09/2021 il bando di 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 Sigef 2296 CIG Lotto 1 88846293CA, CIG Lotto 2 8884642E81” (di seguito per brevità la “Gara”);

4. I.A. possiede i requisiti e le risorse previste, così come meglio descritte nel successivo Art. 2 “Oggetto dell’Accordo” idonei alla partecipazione della summenzionata Gara ed a tal fine rende contestualmente alla sottoscrizione del presente Accordo la “Dichiarazione Integrativa di Avvalimento” (allegata);

5. scopo del presente Accordo è dato dall’interesse di Telecom Italia a partecipare al Lotto 1 della Gara avvalendosi delle risorse/certificazioni/requisiti dell’Impresa Ausiliaria in relazione a quanto previsto dal punto III.1.3) “Capacità professionale e

tecnica" del bando di Gara per il Lotto 1 e dettagliato nel paragrafo 7.3 del Capitolato d'Oneri punto d) e, precisamente, , essere in possesso di una certificazione di conformità del proprio sistema di gestione della sicurezza delle informazioni alle norme UNI EN ISO 27001:2013 in corso di validità, rilasciata da organismi accrediti in conformità alle norme vigenti.

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

Art. 1. Premesse ed allegati

Le Premesse e gli Allegati sono parte integrante e sostanziale del presente Accordo.

Art. 2. Oggetto dell'Accordo

2.1. Tra l'Impresa Ausiliata e l'Impresa Ausiliaria si stipula un contratto di avvalimento, in base all'art. 89 del D.Lgs. 18 aprile 2016 n. 50 e s.m.i., ai seguenti patti e condizioni:

L'impresa Ausiliaria, presa visione ed esatta conoscenza dei documenti di Gara, si impegna a mettere a disposizione dell'Impresa Ausiliata, dell'Ente Appaltante e delle Pubbliche Amministrazioni aderenti all'Accordo Quadro (di seguito "Amministrazioni Contraenti"), ai fini della partecipazione dell'Impresa Ausiliata alla Gara e, in caso di aggiudicazione, per tutta la durata dell'appalto di cui alla Gara, in riferimento al requisito di cui al § III.1.3.) del Bando di Gara, la propria certificazione di conformità del sistema di gestione della sicurezza delle informazioni alla/e norma/e ISO 27001 nel settore/ambito IAF 33 n. CERTCC2-003-2003-AIS-ROM-SINCERT, conforme alle norme UNI EN ISO 27001:2013, in corso di validità, perle attività di progettazione, realizzazione e gestione delle infrastrutture, piattaforme e servizi di ICT presso i Data Center e Centri servizi TIM anche in modalità Cloud e Virtuale per la realizzazione e l'erogazione dei servizi di sicurezza gestiti, nonché tutte le strutture, le tecniche, i fattori della produzione e le risorse che, complessivamente considerati, le hanno consentito di acquisire la predetta certificazione tra cui know how, consulenza e formazione professionale da parte di personale qualificato, strutture tecnico-organizzative, tecniche operative, audit periodicamente effettuati e tutte le procedure di sistema messe in atto per conseguire e mantenere la validità della certificazione.

In particolare, l'Impresa Ausiliaria si impegna a mettere a disposizione dell'Impresa Ausiliata, dell'Ente Appaltante e delle Amministrazioni Contraenti la detta Certificazione conforme alla norma ISO 27001:2013 specificatamente per "Progettazione, realizzazione e gestione delle infrastrutture, piattaforme e servizi di ICT presso i Data Center e Centri servizi TIM anche in modalità Cloud e Virtuale per la realizzazione e l'erogazione dei servizi di sicurezza gestiti", valida per il seguente campo applicativo:

Predisposizione, attivazione ed esercizio di infrastrutture, piattaforme e servizi di Information Communications Technology presso i Data Center e Centri Servizi TIM anche in modalità cloud e virtuale, attraverso
- la gestione di facilities e di impianti tecnologici;
- la gestione e assurance di infrastrutture, servizi di rete e firewall;
- la gestione della sicurezza fisica alle sale sistemi;
- la predisposizione e configurazione dei siti e sale sistemi;
- l'attivazione ed esercizio di piattaforme e servizi IT;
- la conduzione dei Sistemi Elaborativi.

Ed in particolare verranno messi a disposizioni i seguenti mezzi (e relativi siti di ubicazione) inclusi nel Certificato CERTCC2-003-2003-AIS-ROM-SINCERT:

DATA CENTER ROZZANO: Viale Toscana 3 – 20089 Rozzano (MI):

- 15 blade da 24 core fisici 2,2 Ghz e 256 GB
- 15 TB di SSD con backup delle VM con Veeam
- 1.700 TB di NAS SATA per NFS
- VDCN 5 Gbps

DATA CENTER ACILIA: Via di Macchia Palocco, 223/243 - 00125 Roma (RM)

- 15 blade da 24 core fisici 2,2 Ghz e 256 GB
- 15 TB di SSD con backup delle VM con Veeam
- 1.700 TB di NAS SATA per NFS
- VDCN 5 Gbps

Le seguenti risorse per le attività di conduzione e gestione della piattaforma:

- • N. 1 Responsabile di soluzioni informatiche
- • N. 1 Specialista esperto di soluzioni informatiche
- • N. 2 Addetto al supporto specialistico
- • N. 1 Specialista di attività tecniche integrate

L'Impresa Ausiliaria si impegna altresì:

- ad assicurare all'Impresa Ausiliata, all'Ente Appaltante ed alle Amministrazioni Contraenti la disponibilità delle risorse per attuare e monitorare i processi definiti per l'esecuzione e il controllo delle attività di progettazione, installazione e manutenzione dei sistemi di sicurezza ICT funzionali alla fornitura ed all'erogazione dei servizi di Gara secondo gli standard;
- ad assicurare all'Impresa Ausiliata, all'Ente Appaltante ed alle Amministrazioni Contraenti periodica attività di sensibilizzazione e a promuovere attività di formazione/addestramento;
- a definire i parametri di misurazione e controllo per le attività di monitoraggio, e analisi dei processi;
- a pianificare e ad eseguire periodicamente audit interni allo scopo di verificare la conformità dei processi aziendali rispetto ai requisiti delle norme di riferimento, di verificare il raggiungimento delle performance e degli obiettivi desiderati, nonché di fornire uno strumento sistematico di verifica e identificare le aree di potenziale miglioramento;
- nel caso di rilievo di anomalie a definire e a realizzare idonee azioni correttive relativamente alle carenze evidenziate.

2.2. L'Impresa Ausiliata è autorizzata ad utilizzare il requisito innanzi detto per partecipare alla Gara e, in caso di aggiudicazione, per eseguire le prestazioni oggetto del contratto.

2.3. L'I.A. si impegna a non mettere a disposizione di altri partecipanti alla medesima Gara

i propri requisiti.

2.4. In conformità a quanto previsto dal comma 9 dell'Art. 89 del D. L.vo 18 aprile 2016 n. 50 e s.m.i., l'I.A. da' atto ed espressamente accetta che l'Ente Appaltante e le Amministrazioni Contraenti, per l'intera durata dell'Accordo Quadro eventualmente aggiudicato a Telecom Italia (di seguito il "Contratto") eseguiranno le verifiche sostanziali circa l'effettivo possesso da parte dell'I.A. dei requisiti e delle risorse oggetto dell'avvalimento, nonché circa l'effettivo impiego delle risorse medesime nell'esecuzione dell'appalto. l'I.A. da' atto ed espressamente accetta che l'Ente Appaltante e le Amministrazioni contraenti possano accertare in corso d'opera che le prestazioni oggetto del Contratto siano svolte direttamente dalle risorse dell'I.A..

2.5. Resta espressamente inteso che Telecom Italia riconoscerà all'I.A., in caso di aggiudicazione in via definitiva della Gara e stipulazione del Contratto il ruolo di Subfornitore/Subappaltatore in base alle norme applicabili, definendo anche i rapporti economici derivanti dagli obblighi di cui ai precedenti punti con separato specifico contratto di subfornitura/subappalto, fermo restando che la messa a disposizione del requisito, risorse e mezzi avviene a titolo oneroso e che i corrispettivi saranno quindi determinati sulla base della prassi dei rapporti commerciali e di servizio già esistenti tra la capogruppo Telecom Italia e l'IA controllata e sottoposta alla sua direzione e coordinamento.

2.6. Ai fini di quanto previsto al precedente paragrafo 2.4, l'I.A. dichiara di non essere stata indicata come ausiliaria da altri concorrenti alla Gara e/o di non essersi impegnata ad assumere il ruolo di subappaltatore con nessun altro concorrente alla Gara.

2.7. L'Impresa Ausiliata e l'Impresa Ausiliaria sono responsabili in solido nei confronti dell'Ente Appaltante in relazione alle prestazioni oggetto del contratto.

Art. 3. Durata

3.1. Il presente Accordo decorrerà dalla data della sua sottoscrizione ed avrà efficacia per tutta la durata dell'appalto di cui al precedente punto 3 delle premesse, compresi eventuali rinnovi, sino all'estinzione di tutte le obbligazioni pendenti tra le Parti e/o nei confronti dell'Ente Appaltante e/o delle Amministrazioni contraenti in base all'Accordo Quadro stipulato tra Telecom Italia e l'Ente Appaltante medesimo.

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 da Telecom Italia;
- alla data dell'eventuale annullamento, in via definitiva e non soggetto ad impugnativa, della procedura di Gara;
- nel caso di aggiudicazione della Gara a Telecom Italia, 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, le Amministrazioni Contraenti e Telecom Italia stessa, ovvero qualora si verifichi altra causa di cessazione degli effetti giuridici o di estinzione del Contratto stipulato tra Telecom Italia e l'Ente Appaltante.

Art. 4. Proprietà Intellettuale

4.1. Le Parti convengono sin da ora che, compatibilmente con le previsioni della documentazione di Gara, 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.

4.2. Qualora nell'ambito delle attività previste nel presente Accordo ed in esecuzione dello stesso 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 Telecom Italia e dell' I.A. 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 anni 2.

5.3. Qualora la diffusione presso terzi di materiale o di informazioni ritenuti riservati, sia stato causato 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 Contratto, 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 Regolamento 2016/679/EU (Regolamento generale sulla protezione dei dati) e dell'ulteriore normativa applicabile sulla protezione dei dati personali con modalità idonee a garantirne la sicurezza e la riservatezza.
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 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.

6.2. Nel rispetto di quanto previsto all'art. 89 del D.Lgsvo 50/2016 e dal punto 2.2 che precede, il presente Accordo non stabilisce alcuna esclusiva a carico delle Parti.

6.3. I.A si impegna a manlevare e tenere indenne Telecom Italia da qualsiasi conseguenza derivante dal mancato rispetto di quanto previsto nel presente Accordo.

6.4. Per tutto quanto non espressamente previsto dal presente Accordo, troveranno applicazione le disposizioni di cui all'Art. 89 del D.Lgsvo 50/2016 e s.m.i. .

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 e delle Amministrazioni contraenti.

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. Lgsvo 231/2001 dichiarano:

a) di essere a conoscenza della normativa in materia di responsabilità amministrativa delle società, ed in particolare di quanto stabilito al riguardo dal decreto del D. Lgs. n. 231/200;

b) di essere a conoscenza dell'avvenuta adozione, da parte di entrambe, di un modello di organizzazione gestione e controllo ai sensi delle suddette disposizioni, reperibile sul seguente sito web
http://www.telecomitalia.com/tit/it/vendorshub/archivio-documenti.html

c) di essere a conoscenza dei contenuti e dei principi espressi nei rispettivi codice etici, che ne costituiscono parte integrante;

d) di obbligarsi a rispettare, nei rapporti reciproci, detti contenuti e detti principi;

Le Parti si obbligano perciò a non porre in essere, e a far sì che anche i propri dipendenti e/o collaboratori non pongano in essere, atti o comportamenti che rappresentino una violazione dei rispettivi codici etici, nonché più in generale atti o comportamenti che potrebbero condurre alla commissione, anche solo tentata, dei reati contemplati dal D.Lgs. 231/2001.

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 affinché 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 Contratto sarà competente in via esclusiva il Foro di Roma.

8.3. In ogni caso, anche nel caso di insorgenza di una controversia, l'I.A. si impegna a lasciare comunque a disposizione di Telecom Italia e dell'Ente Appaltante e delle Amministrazioni contraenti le proprie certificazioni e risorse oggetto del presente Accordo, salvo poi rivalersi nei confronti dell'Impresa Ausiliata.

Art. 9. Cessione e modifiche

9.1. Qualsiasi modifica, aggiunta o cancellazione a questo Accordo sarà valida ed effettiva solo previo pattuizione scritta tra i legali rappresentanti o persone munite dei necessari poteri di ciascuna delle Parti.

9.2. Le Parti non potranno cedere il presente Accordo.

Art. 10. Comunicazioni relative all'Accordo

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

seguenti indirizzi:

Telecom Italia S.p.A.
CR.EM.PS.MC
Via di Val Cannuta 182
00166 ROMA
c.a. Massimiliano Materazzi
e-mail massimiliano.materazzi@telecomitalia.it
PEC massimiliano.materazzi@pec.telecomitalia.it

Noovle S.p.A.
Via Gaetano Negri n. 1
20123 Milano
c.a Paolo Mesuraca
email paolo.mesuraca@noovle.com
pec:noovlespa@timpec.it

Per Telecom Italia S.p.A.

(Massimiliano Materazzi)

Per Noovle S.p.A. Società Benefit

(Carlo D'Asaro Biondo)

DOCUMENTO FIRMATO DIGITALMENTE