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

- **Accenture S.p.A.**, sede legale in Milano, Via Privata Nino Bonnet n. 10, capitale sociale Euro 1.843.248,60=, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. MI-1652886, P. IVA 13454210157, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti:
- **Fastweb S.p.A.** con sede legale in Milano, Piazza Adriano Olivetti n.1, capitale sociale Euro 12.000.000,00=, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. MI-1591912, P. IVA 12878470157;
- **Fincantieri NextTech S.p.A**., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, capitale sociale Euro 12.000.000,00=, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. MI-2073993, P. IVA 00890740111;
- **DEAS- Difesa e Analisi Sistemi S.p.A**., con sede legale in Roma Via della Colonna Antonina n. 46, capitale sociale Euro 150.000,00=, iscritta al Registro delle Imprese di Roma al n. RM-1558212, P. IVA 14961281004

giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott.ssa Paola Cardelli repertorio n. 27351 del 10 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 PAL 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 PAL 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 Deutsche Bank ed avente n. 896BGI2200580 per un importo di Euro 400.000,00=(quattrocentomila/00) a garanzia dell'adempimento delle obbligazioni contrattuali nascenti dall'Accordo Quadro;

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

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

l) che risulta allo stato pendente, innanzi al T.A.R. del Lazio, 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.r.l., Reevo S.p.A., KPGM 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 (di seguito "**Ricorso Leonardo**"). All'udienza del 20 aprile 2022, fissata per la trattazione dell'istanza cautelare, Leonardo ha rinunciato alla sospensiva. Il Tribunale ha fissato per la trattazione del merito del giudizio l'udienza del 22 giugno 2022 con rinvio alla successiva udienza fissata per il 13 luglio 2022, con rinuncia delle parti ai termini a difesa rispetto ai ricorsi incidentali di Telecom e Accenture. Nella seduta del 13 luglio 2022 la causa è stata trattenuta in decisione. Per tale motivo la Consip S.p.A. procede nella sottoscrizione del presente atto.

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 PAL:** 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 PAL) 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).
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 PAL) 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 280.800.000,00=(duecentoottantamilioni ottocentomila), IVA esclusa (attribuzione della quota massima al Fornitore graduato primoo nella graduatoria di merito).
2. Qualora, anteriormente alla scadenza del termine di durata dell'Accordo Quadro, anche eventualmente prorogata, il valore relativo ad un Contratto esecutivo raggiunga il valore stimato dell'Accordo Quadro medesimo oppure lo

ecceda (comunque fino a una soglia massima del 20%), Consip considererà quest'ultimo come giunto a scadenza e di conseguenza non potranno essere affidati ulteriori Contratti esecutivi. La regola sopra illustrata opera sul massimale della quota di AQ stipulato con il Fornitore.

3. Il presente Accordo Quadro è concluso con il Fornitore aggiudicatario della procedura aperta di cui in premessa, il quale con la sottoscrizione del presente atto, si impegna a dare esecuzione ai Contratti esecutivi che si perfezioneranno all'esito dell'approvazione del Piano operativo, quale affidamento in favore del Fornitore del Contratto esecutivo basato sulle condizioni stabilite nel presente Accordo Quadro e relativi Allegati.
4. L'affidamento del Contratto esecutivo da parte della singola Amministrazione avverrà in favore del Fornitore che sottoscrive il presente contratto in ragione del fatto che la medesima appartiene alla PAL 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.

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 PAL", 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 PAL 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 14 e 15, 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 PAL).
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. 000012807025, intestato al Fornitore Accenture S.p.A. presso Bank of America, Codice IBAN IT48Z0338001600000012807025;
    - n. 100000064266, intestato al Fornitore Deas – Difesa e Analisi Sistemi S.p.A. presso Intesa San Paolo S.p.A, Codice IBAN IT73N0306905020100000064266;

- n. 000000770001, intestato al Fornitore Fastweb S.p.A. presso Deutsche Bank, Codice IBAN IT41F0310401607000000770001;
- n. 000041368809, intestato al Fornitore Fincantieri NextTech S.p.A. presso Unicredit S.p.A., Codice IBAN IT33Q0200805364000041368809.

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

16. Il Fornitore si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i alle Amministrazioni all'atto dell'accettazione del Piano dei Fabbisogni secondo le modalità indicate all'art.6.
17. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto nell'art. 5 del D.Lgs. 9 ottobre 2002, n. 231.
18. Il Fornitore, sotto la propria esclusiva responsabilità, renderà tempestivamente noto alle Amministrazioni e alla Consip S.p.A., per quanto di propria competenza, le variazioni che si verificassero circa le modalità di accredito indicate nell'Accordo Quadro e nei singoli Contratti esecutivi; in difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, il Fornitore non potrà sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.
19. Nel caso in cui risulti aggiudicatario dell'Accordo Quadro un R.T.I., le singole imprese costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione Contraente, dovranno provvedere ciascuna alla fatturazione delle sole attività effettivamente svolte, corrispondenti alle attività dichiarate in fase di gara risultanti nell'atto costitutivo del Raggruppamento Temporaneo di Imprese, che il Fornitore si impegna a trasmettere in copia, ove espressamente richiesto dall'Amministrazione Contraente. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi e/o forniture cui si riferisce.
20. Il R.T.I. avrà facoltà di scegliere se: i) il pagamento da parte delle Amministrazioni Contraenti dovrà essere effettuato nei confronti della mandataria che provvederà poi alla redistribuzione dei corrispettivi a favore di ciascuna mandante in ragione di quanto di spettanza o ii) se, in alternativa, il pagamento dovrà essere effettuato dalle Amministrazioni Contraenti direttamente a favore di ciascun membro del RTI. La predetta scelta dovrà risultare dall'atto costitutivo del RTI medesimo. In ogni caso, la società mandataria del Raggruppamento medesimo è obbligata a trasmettere apposito prospetto riepilogativo delle attività e delle competenze maturate dalle singole imprese membri del RTI e, in maniera unitaria, le fatture di tutte le imprese raggruppate e prospetto riepilogativo delle attività e delle competenze maturate da ciascuna. Resta in ogni caso fermo quanto previsto dall'art. 48, comma 13, del D.Lgs. n. 50/2016.
21. Resta tuttavia espressamente inteso che in nessun caso il Fornitore potrà sospendere la prestazione dei servizi e, comunque, delle attività previste nell'Accordo Quadro e nei singoli Contratti esecutivi, salvo quanto diversamente previsto nell'Accordo Quadro medesimo.
22. Qualora il Fornitore si rendesse inadempiente a tale obbligo, i singoli Contratti esecutivi e/o l'Accordo Quadro si potranno risolvere di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi tramite pec o con lettera raccomandata A/R, rispettivamente dalle Amministrazioni Contraenti e dalla Consip S.p.A., ciascuno per quanto di propria competenza.
23. E' ammessa la cessione dei crediti maturati dal Fornitore nei confronti dell'Amministrazione a seguito della regolare e corretta esecuzione delle prestazioni oggetto del Contratto esecutivo, nel rispetto dell'art. 106, comma 13, del D.Lgs. n. 50/2016. In ogni caso, è fatta salva ed impregiudicata la possibilità per l'Amministrazione Contraente di opporre al cessionario tutte le medesime eccezioni opponibili al Fornitore cedente. Le cessioni dei crediti devono essere stipulati mediante atto pubblico o scrittura privata autenticata e devono essere notificate alla Amministrazione Contraente. Si applicano le disposizioni di cui alla Legge n. 52/1991. Resta fermo quanto previsto

in tema di tracciabilità dei flussi finanziari di cui al successivo articolo 25.

24. Ai fini del versamento dell'IVA per cessione di beni e prestazioni di servizi a favore delle Pubbliche Amministrazioni, si applica quanto previsto dall'art. 17-ter del d.P.R. n. 633 del 1972 ("split payment"), introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96, e le relative disposizioni di attuazione tra le quali il DM 23 gennaio 2015 come modificato dal DM 27 giugno 2017.
25. In caso di pericolo di insolvenza di Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, diversi dalle società pubbliche inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, a totale partecipazione pubblica diretta o indiretta, è facoltà del Fornitore non inadempiente richiedere di prestare idonea garanzia per l'adempimento dell'obbligazione di pagamento relativa al contratto esecutivo; tale garanzia dovrà essere rilasciata per un importo pari al 20% del valore del Contratto esecutivo. La garanzia dovrà essere richiesta dal Fornitore entro il termine di 4 giorni lavorativi dalla ricezione dell'ordine e l'Amministrazione dovrà rilasciarla entro 30 giorni dalla ricezione della richiesta. Il Fornitore non inadempiente è legittimato a sospendere l'esecuzione della fornitura fino ad avvenuta ricezione della garanzia richiesta. Decorso inutilmente il termine per il rilascio della garanzia e ferma restando la facoltà di sospensione dell'esecuzione, è facoltà del Fornitore, ai sensi dell'art. 1454 c.c., diffidare per iscritto l'Amministrazione ad adempiere entro 15 giorni, decorsi inutilmente i quali il contratto s'intenderà risolto di diritto. Resta salva la facoltà dell'Amministrazione di recedere dal contratto esecutivo in caso di sospensione.
26. In caso di Contratti esecutivi effettuati da Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, verso i quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato del presente AQ o in precedenti rapporti contrattuali, il Fornitore è legittimato a sospendere l'esecuzione del Contratto esecutivo fino ad avvenuta ricezione della comprova del pagamento per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dei suddetti soggetti di recedere dal contratto esecutivo in caso di sospensione.
27. Fermo restando quanto stabilito al precedente comma, in caso di Contratti esecutivi effettuati da Amministrazioni verso le quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato nel presente Accordo Quadro ovvero in precedenti rapporti contrattuali relativi alla fornitura di beni o servizi ricompresi nell'oggetto dell'Accordo Quadro, il Fornitore è legittimato a sospendere l'esecuzione del contratto esecutivo fino ad avvenuta ricezione della comprova del pagamento/stanziamento di fondi per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione all'Amministrazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dell'Amministrazione di recedere dal contratto esecutivo in caso di sospensione.
28. Gli Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, nel Contratto esecutivo, accettano preventivamente la cessione dei crediti ai sensi e per gli effetti di cui all'art. 106, comma 13 del D.Lgs. n. 50/2016.
29. Ove applicabile in considerazione della natura e tipologia di prestazioni, ai sensi dell'art. 35, comma 18, del Codice, così come novellato dal D.L. 32/2019, il fornitore può ricevere, entro 15 giorni dall'effettivo inizio delle prestazioni oggetto del Contratto esecutivo un'anticipazione del prezzo pari al 20 per cento del valore del Contratto esecutivo stesso. Tale percentuale può essere aumentata dall'Amministrazione Contraente fino ad un massimo del 30% al ricorrere dei presupposti di cui all'art. 207 del D.L. 34/2020.

    L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa

in favore dell'Amministrazione beneficiaria della prestazione, rilasciata dai soggetti indicati all'art. 35, comma 18, del Codice, di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma (o altro documento equivalente tipo SLA) della prestazione che sarà indicato nel Piano dei Fabbisogni .

30. L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento delle prestazioni, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.
31. Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione delle prestazioni, non procede, per ritardi a lui imputabili, secondo il cronoprogramma concordato. Sulle somme restituite sono dovuti gli interessi legali con decorrenza dalla data di erogazione della anticipazione.
32. Laddove in relazione al singolo contratto esecutivo ricorrano i presupposti soggettivi ed oggettivi, le Amministrazioni Contraenti e il Fornitore sono tenuti all'applicazione delle disposizioni di cui all'art. 17-bis del D.lgs. 241/1997 in materia di ritenute e compensazioni in appalti e subappalti.

ARTICOLO 11 - COSTI DELLA SICUREZZA

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

ARTICOLO 12 - PENALI

1. Si applicano le penali previste nell'appendice 1 al Capitolato Tecnico Speciale (che deve intendersi in questa sede integralmente trascritta), nonché quelle di seguito indicate. È sempre fatto salvo il risarcimento del maggior danno. In caso di penali da ritardo, deve considerarsi ritardo anche il caso in cui il Fornitore esegua il servizio in modo anche solo parzialmente difforme rispetto alle disposizioni di cui al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto esecutivo, nonché alla propria Offerta Tecnica. In tal caso le Amministrazioni applicheranno al Fornitore la suddetta penale sino alla data in cui il servizio inizierà ad essere eseguito in modo effettivamente conforme al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto esecutivo, all'Offerta Tecnica, fatto salvo il risarcimento del maggior danno.
2. In caso di invio della documentazione necessaria all'attivazione dell'Accordo Quadro (ivi compreso il Piano di Qualità Generale) in ritardo rispetto ai termini previsti nel presente Accordo Quadro e relativi allegati o di ritardo nell'attivazione del portale della fornitura, per cause non imputabili a Consip ovvero a forza maggiore o caso fortuito, Consip avrà la facoltà di applicare una penale pari a 1.000,00 euro per ogni giorno solare di ritardo, fatto salvo il risarcimento del maggior danno subito.
3. In caso di invio della documentazione prodromica alla stipula di ciascun Contratto Esecutivo (ivi compreso il Piano Operativo e relativi allegati e i riferimenti del RUAC del Contratto Esecutivo) in ritardo rispetto ai termini previsti nel presente Accordo Quadro e relativi allegati o comunque concordati con l'Amministrazione, per cause non imputabili a Consip, all'Amministrazione ovvero a forza maggiore o caso fortuito, Consip, anche su segnalazione dell'Amministrazione, avrà la facoltà di applicare una penale pari a 1.000,00 euro per ogni giorno solare di ritardo, fatto salvo il risarcimento del maggior danno subito.
4. Per ogni giorno di ritardo del Fornitore, non imputabile a Consip S.p.A. ovvero a forza maggiore o caso fortuito, nell'adempimento all'obbligo previsto al precedente articolo 8, comma 1, lettere a), b) e c) per la presentazione della documentazione ivi indicata, il Fornitore è tenuto a corrispondere a Consip S.p.A. una penale pari a euro 100,00 = (cento/00), fatto salvo il risarcimento del maggior danno.
5. Per ogni giorno di ritardo non imputabile all'Amministrazione, ovvero a forza maggiore o caso fortuito, i) rispetto ai

previsti tempi di effettuazione delle verifiche di conformità; ii) di ripetizione delle prove di collaudo in caso di esito negativo delle verifiche di conformità; l'Amministrazione potrà applicare al Fornitore una penale pari allo 0,3 (ovvero in caso di Contratti esecutivi cd. PNRR o PNC si intenderà 0,6) per mille del valore del Contratto esecutivo, fatto salvo il risarcimento del maggior danno.

6. Nel caso in cui, come previsto nell'atto di nomina a responsabile del Trattamento allegato all'Accordo Quadro, all'esito delle verifiche, ispezioni e audit e assessment compiuti dall'Amministrazione o da terzi autorizzati, le misure di sicurezza adottate dal Responsabile primario/Sub responsabile 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 07/03/2022 dalla Deutsche Bank avente n. 896BGI2200580 di importo pari ad Euro 400.000,00=(quattrocentomila/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 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 10 e 11;
l) nell'ipotesi di non veridicità delle dichiarazioni rese dal Fornitore ai sensi del D.p.r. n. 445/00, fatto salvo quanto previsto dall'art. 71, del medesimo D.P.R. 445/2000;
m) nell'ipotesi di irrogazione di sanzioni interdittive o misure cautelari di cui al D. Lgs. n. 231/01, che impediscano all'Impresa di contrattare con le Pubbliche Amministrazioni;
n) in caso di avvalimento, ove a fronte delle segnalazioni delle Amministrazioni contraenti ed in ragione di quanto dichiarato dal Fornitore, risultasse la violazione dell'art. 89, comma 9, del d. lgs. n. 50/2016 e s.m.i.;
o) nei casi di cui all'articolo 3 e 5 del Patto di integrità.

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

2. Consip e/o le Amministrazioni Contraenti, per quanto di rispettiva competenza, devono risolvere l'Accordo Quadro e il singolo Contratto esecutivo senza bisogno di assegnare alcun termine per l'adempimento, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art.1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
   a) qualora nei confronti del Fornitore sia intervenuto un provvedimento definitivo che dispone l'applicazione di una o più misure di prevenzione di cui al codice delle leggi antimafia e delle relative misure di prevenzione, fatto salvo quanto previsto dall'art. 95 del D. Lgs. n. 159/2011, o nel caso in cui gli accertamenti antimafia presso la Prefettura competente risultino positivi oppure sia intervenuta sentenza di condanna passata in giudicato per i reati di cui all'articolo 80 del D. Lgs. n. 50/2016 e s.m.i.;
   b) qualora fosse accertato il venir meno dei requisiti richiesti dalla legge;
3. Inoltre, Consip S.p.a. si impegna ad avvalersi della clausola risolutiva espressa di cui all'art. 1456 c.c. ogni qualvolta nei confronti del Fornitore o dei componenti la propria compagine sociale, o dei dirigenti dell'impresa con funzioni specifiche relative all'affidamento alla stipula e all'esecuzione dell'Accordo Quadro sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317 cp 318 cp 319 cp 319 bis cp 319 ter cp 319 quater 320 cp 322 cp 322 bis cp 346 bis cp 353 cp 353 bis cp. La risoluzione di cui al periodo precedente è subordinata alla preventiva comunicazione all'ANAC, cui spetta la valutazione in merito all'eventuale prosecuzione del rapporto contrattuale, al ricorrere delle condizioni di cui all'art. 32 del dl. 90/2014 convertito in legge 114 del 2014.
4. Il Fornitore accetta le cause di risoluzione previste nell'atto di nomina a Responsabile/sub Responsabile del Trattamento allegato al presente Accordo quadro, che devono intendersi integralmente trascritte.
5. Consip e/o le Amministrazioni Contraenti, quando accertino un grave inadempimento del Fornitore ad una delle obbligazioni assunte con l'Accordo Quadro e/o con i Contratti esecutivi tale da compromettere la buona riuscita delle prestazioni, formuleranno la contestazione degli addebiti al Fornitore e contestualmente assegneranno un termine, non inferiore a quindici giorni, entro i quali il Fornitore dovrà presentare le proprie controdeduzioni. Acquisite e valutate negativamente le controdeduzioni ovvero scaduto il termine senza che il Fornitore abbia risposto, Consip e/o le Amministrazioni Contraenti hanno la facoltà, per quanto di rispettiva competenza, di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei Contratti esecutivi, di incamerare la garanzia ove essa non sia stata ancora restituita ovvero di applicare una penale equivalente, nonché di

procedere all'esecuzione in danno dell'Impresa; resta salvo il diritto al risarcimento dell'eventuale maggior danno.

6. Qualora il Fornitore ritardi per negligenza l'esecuzione delle prestazioni rispetto alle previsioni dell'Accordo Quadro e dei Contratti esecutivi, Consip e/o le Amministrazioni contraenti assegnano un termine che, salvo i casi d'urgenza, non può essere inferiore a 10 (dieci) giorni, entro i quali il Fornitore deve eseguire le prestazioni. Scaduto il termine assegnato, e redatto processo verbale in contraddittorio con il Fornitore, qualora l'inadempimento permanga, Consip e/o le Amministrazioni contraenti potranno risolvere l'Accordo Quadro e/o i Contratti esecutivi, fermo restando il pagamento delle penali.
7. In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con la stipula dell'Accordo Quadro e dei Contratti esecutivi che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato tramite pec dalla Consip e/o dall'Amministrazione Contraente, per quanto di propria competenza, per porre fine all'inadempimento, la Consip e/o l'Amministrazione Contraente hanno la facoltà di considerare risolti di diritto l'Accordo Quadro e/o i Contratti esecutivi e di ritenere definitivamente la garanzia ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.
8. In caso di risoluzione anche di uno solo dei Contratti esecutivi, Consip S.p.A. si riserva di risolvere il presente Accordo Quadro. La risoluzione dell'Accordo Quadro legittima la risoluzione dei singoli Contratti esecutivi a partire dalla data in cui si verifica la risoluzione dell'Accordo Quadro. La risoluzione dell'Accordo Quadro è, pertanto, causa ostativa all'affidamento di nuovi Contratti esecutivi e può essere causa di risoluzione dei singoli Contratti esecutivi, salvo che non sia diversamente stabilito nei medesimi e salvo, in ogni caso, il risarcimento del danno.
9. In tutti i casi di risoluzione dell'Accordo Quadro e dei Contratti esecutivi, Consip S.p.A. e/o l'Amministrazione Contraente, avranno diritto di escutere la garanzia prestata per l'intero importo della stessa o per la parte percentualmente proporzionale all'importo del/i Contratto/i esecutivo/i risolto/i. Ove l'escussione non sia possibile sarà applicata una penale di equivalente importo, che sarà comunicata al Fornitore via pec. In ogni caso, resta fermo il diritto della medesima Amministrazione Contraente e/o di Consip S.p.A. al risarcimento dell'ulteriore maggior danno.
10. La Consip S.p.A., fermo restando quanto previsto nel presente articolo e nei casi di cui all'art. 110 del D.Lgs. n. 50/2016, potrà interpellare progressivamente gli operatori economici che hanno partecipato all'originaria procedura di gara e risultanti dalla relativa graduatoria al fine di stipulare un nuovo Accordo Quadro per l'affidamento del completamento delle prestazioni contrattuali alle medesime condizioni già proposte dall'aggiudicatario in sede di offerta.

ARTICOLO 15 - RECESSO

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

   Si conviene che per giusta causa si intende, a titolo meramente esemplificativo e non esaustivo:
   - qualora sia stato depositato contro il Fornitore un ricorso ai sensi della legge fallimentare o di altra legge applicabile in materia di procedure concorsuali, che proponga lo scioglimento, la liquidazione, la composizione amichevole, la ristrutturazione dell'indebitamento o il concordato con i creditori, ovvero nel caso in cui venga

designato un liquidatore, curatore, custode o soggetto avente simili funzioni, il quale entri in possesso dei beni o venga incaricato della gestione degli affari del Fornitore, resta salvo quanto previsto dall'art. 110, comma 3, del D.Lgs. n. 50/2016;

- in qualsiasi altra fattispecie che faccia venire meno il rapporto di fiducia sottostante il presente Accordo Quadro o i Contratti esecutivi.

2. In caso di mutamenti di carattere organizzativo interessanti l'Amministrazione che abbiano incidenza sull'esecuzione della fornitura o della prestazione dei servizi, la stessa Amministrazione potrà recedere in tutto o in parte unilateralmente da Contratto esecutivo, con un preavviso almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore tramite pec.
3. Fermo restando quanto previsto dagli artt. 88, comma 4-ter, e 92, comma 4, del D.Lgs. 159/2011, Consip S.p.A. e/o l'Amministrazione ai sensi dell'art. 109 comma 1 del Codice potrà recedere dall'Accordo Quadro e/o da ciascun singolo contratto esecutivo, in qualunque momento, con preavviso non inferiore a 20 (venti) giorni solari, previo il pagamento da parte delle Amministrazioni delle prestazioni oggetto di Contratto esecutivo eseguite a regola d'arte, nonché del valore dei materiali utili esistenti in magazzino (ove esistenti), oltre al decimo dell'importo delle opere, dei servizi o delle forniture non eseguite, ai sensi dell'art. 109 comma 2 del Codice, rinunciando espressamente il Fornitore, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso e/o indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ..
4. Qualora la Consip receda dall'Accordo Quadro, non potranno essere affidati nuovi Contratti esecutivi da parte delle Amministrazioni e le singole Amministrazioni potranno a loro volta recedere dai singoli Contratti esecutivi, con un preavviso di almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore tramite pec..

ARTICOLO 16 - OBBLIGHI DERIVANTI DAL RAPPORTO DI LAVORO

1. Il Fornitore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, in materia previdenziale e infortunistica, assumendo a proprio carico tutti i relativi oneri. In particolare, il Fornitore si impegna a rispettare nell'esecuzione delle obbligazioni derivanti dall'Accordo Quadro e dai singoli Contratti esecutivi le disposizioni di cui al D.Lgs. 9 aprile 2008 n. 81.
2. Il Fornitore si obbliga altresì ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, le condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi ed integrativi di lavoro applicabili alla data di stipula dell'Accordo Quadro alla categoria e nelle località di svolgimento delle attività, nonché le condizioni risultanti da successive modifiche ed integrazioni, anche tenuto conto di quanto previsto all'art. 95, comma 10 e all'art. 97 del D. Lgs. n. 50/2016.
3. Il Fornitore si obbliga, altresì, fatto in ogni caso salvo il trattamento di miglior favore per il dipendente, a continuare ad applicare i suindicati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione.
4. Gli obblighi relativi ai contratti collettivi nazionali di lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui questi non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità dell'Accordo Quadro e dei singoli Contratti esecutivi.
5. Restano fermi gli oneri e le responsabilità in capo al Fornitore di cui all'art. 105, comma 9, del D. Lgs. n. 50/2016 in caso di subappalto.

ARTICOLO 17 - TRASPARENZA

1. Il Fornitore espressamente ed irrevocabilmente:

a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione dell'Accordo Quadro;
b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione dell'Accordo Quadro stesso;
c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione dell'Accordo Quadro rispetto agli obblighi con esso assunti, né a compiere azioni comunque volte agli stessi fini;
d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.lgs. 50/2016 al fine di evitare situazioni di conflitto d'interesse.

2. Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse per tutta la durata dell'Accordo Quadro gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma, lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'articolo 1456 cod. civ., per fatto e colpa del Fornitore, con facoltà di Consip S.p.A. di incamerare la garanzia prestata.
3. Il Fornitore si impegna al rispetto di tutte le previsioni di cui al Patto di integrità.

ARTICOLO 18 - RISERVATEZZA

1. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi compresi quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione dell'Accordo Quadro e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
2. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione dell'Accordo Quadro e degli Contratti esecutivi; tale obbligo non concerne i dati che siano o divengano di pubblico dominio.
3. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza anzidetti.
4. In caso di inosservanza degli obblighi di riservatezza, le Amministrazioni e/o Consip S.p.A. hanno la facoltà di dichiarare risolto di diritto, rispettivamente, il singolo Contratto esecutivo ovvero l'Accordo Quadro, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare alle Amministrazioni e/o a Consip S.p.A..
5. Il Fornitore potrà citare i contenuti essenziali dell'Accordo Quadro e dei Contratti esecutivi affidati in proprio favore nei casi in cui ciò fosse condizione necessaria per la partecipazione del Fornitore medesimo a gare e appalti.
6. Resta fermo quanto previsto nel successivo articolo 23.

ARTICOLO 19 - RESPONSABILE UNICO DELLE ATTIVITA CONTRATTUALI (RUAC)

1. Il Responsabile Unico delle Attività Contrattuali (RUAC), nominato dal Fornitore è il Dott.Marco Molinaro.
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 avviene in pendenza della definizione del giudizio di cui in premessa, iscritto al Tar Lazio Roma al numero di RG 3738/2022 relativamente al quale, senza concedere misure cautelari, all'udienza del 20 aprile 2022, il Tribunale ha rinviato per la trattazione del merito all'udienza del 22 giugno 2022 con successivo rinvio alla udienza del 13 luglio 2022, con rinuncia delle parti ai termini a difesa rispetto ai ricorsi incidentali di Telecom e Accenture. qualora all'esito del predetto giudizio, o degli eventuali giudizi instaurati a seguito 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

_____

ALLEGATO A – OFFERTA TECNICA DEL FORNITORE

Gara a procedura aperta per la conclusione di un accordo quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

07/10/2021

ID 2296 - **LOTTO** 1

AQ SICUREZZA

accenture | FASTWEB un passo avanti | FINCANTIERI NexTech | DEAS

SOMMARIO

1 PREMESSA

L'innovazione tecnologica avvenuta nell'ultimo decennio, e le nuove necessità causate dall'avvento della pandemia iniziata nel 2020, hanno generato il bisogno di un'accelerazione nella digitalizzazione della Pubblica Amministrazione (PA). Ciò ha contribuito all'aumento del rischio di esposizione alle **minacce di tipo cibernetico**, rischio accentuato dal fatto che non tutte le organizzazioni ad oggi possiedono adeguate capacità di difesa nei confronti delle minacce emergenti.

L'**aumento della superficie di attacco** ha portato al proliferare di azioni offensive ai danni di aziende, enti pubblici e governi, perpetrate principalmente tramite campagne di phishing e ransomware, che hanno portato l'estorsione online ad un nuovo livello, trasformando in poco tempo il crimine informatico in uno dei modelli di business più redditizi e scalabile.

In questo contesto gli enti regolatori europei e nazionali hanno avviato molte iniziative volte a offrire regolamentazioni e best practice nell'ambito della sicurezza informatica, come cardine imprescindibile per la transizione digitale. In particolar modo per la PA il quadro si compone dei seguenti principali elementi:

- il **Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020–2022**, nato per guidare operativamente la trasformazione digitale della PA e che trova nella sicurezza informatica un elemento determinante;
- il **Piano Nazionale di Ripresa e Resilienza** (**PNRR**), che identifica la "digitalizzazione, innovazione e **sicurezza nella PA**" come la prima delle missioni del piano con ingenti investimenti dedicati alla sicurezza cibernetica;
- il **Perimetro di sicurezza nazionale cibernetica,** instituito con lo scopo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, dal cui malfunzionamento o interruzione possa derivare un pregiudizio per la sicurezza nazionale;
- la nascita dell'**Agenzia per la Cybersicurezza Nazionale** (**ACN**), che funzionerà da interlocutore unico per i soggetti pubblici e privati in tema di misure di sicurezza nazionali.

La presente iniziativa **Sicurezza da remoto** si inserisce all'interno di questo scenario, che sta delineando l'approccio italiano alla minaccia cibernetica, e consentirà di migliorare la **capacità di resilienza del paese**.

Il costituendo Raggruppamento Temporaneo d'Impresa (in seguito indicato dalla sigla RTI o semplicemente dall'uso della prima persona plurale) formato da Accenture S.p.A. (Accenture) in qualità di mandataria e da Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri) e Difesa e Analisi Sistemi S.p.A. (DEAS) costituisce una compagine in grado di permettere il pieno raggiungimento degli obiettivi prefissi dall'AQ, in quanto:

- **Accenture** è il più grande operatore di servizi di sicurezza al mondo; l'unità operativa dedicata Security ha più di 9.000 professionisti dedicati alla protezione dello spazio cibernetico, più di 1.000 in Italia. Opera da più di 20 anni per oltre 2.900 clienti in 67 paesi differenti; oltre ad avere un'ampia esperienza nell'erogazione dei servizi di sicurezza gestiti, sia nel privato che nel settore pubblico, è riconosciuta per la sua capacità di innovarne la modalità di erogazione, grazie alla sua rete globale di Centri di Ricerca, Sviluppo e Innovazione;
- **Fastweb** è il primo fornitore della PA in Italia di servizi avanzati di telecomunicazioni e di ICT, con più di 15 anni di esperienza, potendo vantare la presenza in una pluralità di enti della Pubblica Amministrazione Centrale (PAC) e Locale (PAL) essendo aggiudicataria di numerose Convenzioni e Accordi Quadro quali, ad esempio, SPC Cloud Lotto 2 Sicurezza, SPC 2 Connettività, SGM, Infrastrutture Condivise SPC, TF5, CT5, AQ DTO3, AQ System Management;
- **Fincantieri NexTech** è una società tecnologica, appartenente al Gruppo Fincantieri, che opera principalmente per lo sviluppo di soluzioni nei settori della sicurezza e della protezione di informazione, rappresentando il centro di competenza tecnologico del Gruppo Fincantieri, con la capacità di supportare lo sviluppo e l'integrazione sia di soluzioni "Legacy" che "innovative";
- **DEAS** è una PMI innovativa che ha scelto la Sicurezza come ambito di ricerca e sviluppo per un'offerta innovativa già apprezzata nella PAC.

I **valori** (competenze, esperienze, migliori pratiche, beni) che il nostro RTI mette a disposizione della Fornitura in oggetto possono essere classificati in relazione agli **obiettivi** che tale Fornitura si pone: **Continuità**, **Evoluzione** e **Innovazione**. La seguente tabella illustra una sintesi di tali valori, più ampiamente descritti al §3.2.

Obiettivi	Competenze e asset messi a disposizione della Fornitura
Continuità	**Fastweb** è aggiudicataria del Contratto Quadro "Servizi di Gestione delle Identità Digitali e Sicurezza Applicativa" (SPC Cloud L2) che ha permesso di sviluppare **esperienze** in numerosi progetti pubblici anche tramite una **copertura capillare delle PA**. **Accenture** è il primo fornitore di servizi in ambito sicurezza in Italia, erogandoli sia da remoto sia on-site tramite la struttura **Managed Security Services** e **il Cyber Fusion Center di Napoli**. **Fincantieri** e **DEAS** garantiscono continuità specifica nel critico **settore Difesa**.
Evoluzione	**Accenture** ha realizzato il modello **Cyber Defense Operating Model** che facilita la presa in carico dei servizi di un nuovo cliente, l'erogazione dei servizi stessi per la protezione dei sistemi informativi, il monitoraggio e miglioramento continuo per raggiungere il livello di Sicurezza auspicato. È inoltre **partner dell'anno dei maggiori vendor di tecnologia in ambito Sicurezza** senza legarsi a nessuno di essi (**technology agnostic**) e opera da **system integrator** per valorizzare le diverse tecnologie nell'interesse dei clienti. Rende, inoltre, disponibili asset distintivi descritti nel documento, tra cui: servizio di Intelligence iDefense, piattaforma di Intelligence TIS, piattaforma di Security Awareness, ecc. **Fincantieri** mette a disposizione esperienze distintive maturate nel settore militare e della **cyber security.**

	DEAS, grazie alle competenze nel settore **Difesa**, garantisce una continua **evoluzione verticale dei servizi**.
Innovazione	**Accenture** apporta ✓il contributo di una **rete globale di centri di ricerca e sviluppo** (*Cyber Labs*), di **erogazione dei servizi di sicurezza da remoto** (*Cyber Fusion Center*) e di **poligoni cibernetici** (*Cyber Range*) sia in Italia che nel resto del mondo (50+ Centri, di cui 2 in Italia) ✓il valore del **continuo investimento in acquisizioni di società specializzate** in servizi di cyber security (es. Maglan, FusionX, iDefense, Syman-tec e Contex-IS specializzata in ambito Governativo e Difesa in UK). ✓la **più grande rete globale di *threat intelligence*** con specialisti che coprono più di 39 lingue parlate e casi di successo internazionali a difesa di numerosi governi esteri. **Fastweb** mette a disposizione laboratori di sicurezza equipaggiati con **tecnologie all'avanguardia** per l'analisi di apparati embedded, strumentazioni di test e misura, centri dedicati a **collaudi e prove tecniche per la certificazione** di servizi e prodotti di sicurezza per la PA. **Fincantieri** apporta il valore della sua fitta **rete di collaborazione con le principali università e centri di ricerca** la **partecipazione a progetti di ricerca nazionali e internazionali** sui temi della sicurezza per ambienti **militari e della difesa**. **DEAS** mette a disposizione know how e strumenti per l'**applicazione dell'Intelligenza Artificiale (AI) ai Big Data** generati dall'erogazione dei servizi di Sicurezza.

Il **fattore unificante e acceleratore** della messa in opera ed erogazione dei servizi di sicurezza da remoto è il **Cyber Defense Operating Model (CDOM)**, un modello operativo proprietario messo a disposizione da Accenture per la Fornitura. Grazie alle sue componenti (Modello Operativo, Libreria di Procedure, Funzioni Fondamentali e Interfacce Chiave, Workflow, ecc.) oltre a garantire un'erogazione della **fornitura rapida, standardizzata e di qualità**, agisce come elemento omogeneizzante creando un'organizzazione di Fornitura coesa e integrata che alimenta un processo di **miglioramento incrementale continuo**. Tale modello – il cui schema di alto livello è rappresentato in Figura 1 - è basato sul National Institute of Standards and Technology (**NIST**) **Cyber Security Framework** (principale standard di sicurezza in ambito cyber, anche il framework nazionale si basa su di esso), arricchito dai principali standard e best practice di settore (ISO 27001, NERC-CIP, MITRE ATT&CK, ISF, SANS, ITIL e COBIT); integra i requisiti normativi cogenti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al **Framework Nazionale per la Cybersecurity e la Data Protection**, che rappresenta un punto di riferimento adatto a realtà fortemente eterogenee, dalla grande PAC alla piccola PAL. Proponiamo, quindi, un approccio globale e collaborativo che non definisce solo le competenze chiave di un **Security Operation Center**, SOC (i.e. *Threat Intelligence*, *Vulnerability Management*, *Threat Monitoring*, *Threat Hunting, IIdentity Management, Application Security, Threat Response e Active Defence*) ma rappresenta anche le funzioni chiave complementari (i.e. *Breach Prevention & Readiness*, *Governance*, *Gestione prestazioni del servizio*, *Automazione e Orchestrazione, Machine Learning (ML), Miglioramento Continuo* e servizi trasversali), che sono fondamentali per un'efficace gestione dei servizi gestiti di sicurezza (MSS, Managed Security Services) oggetto di tale fornitura.

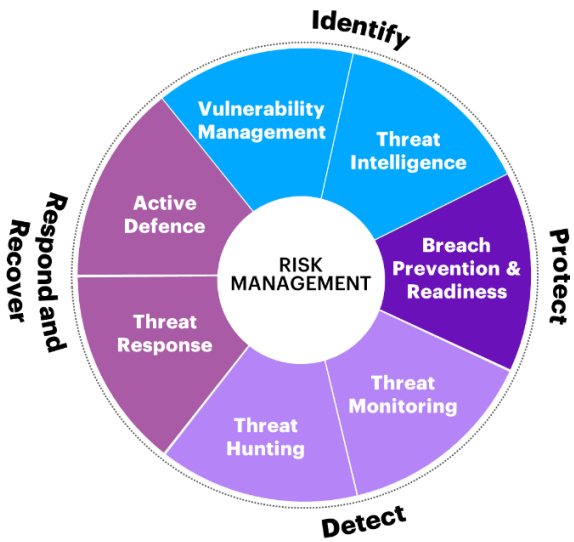


Figura 1 - Schema del CDOM

In Figura 2 mostriamo come le componenti del CDOM sono pienamente aderenti allo schema dei servizi previsti dalla presente Fornitura. Ad esempio, sotto la macrofunzione NIST Identify il CDOM prevede il dominio di sicurezza Vulnerability Management che include 4 sotto-servizi che rispondono pienamente ai requisiti del servizio L1-S4 Gestione continua delle vulnerabilità di sicurezza, facilitando la riduzione del rischio.

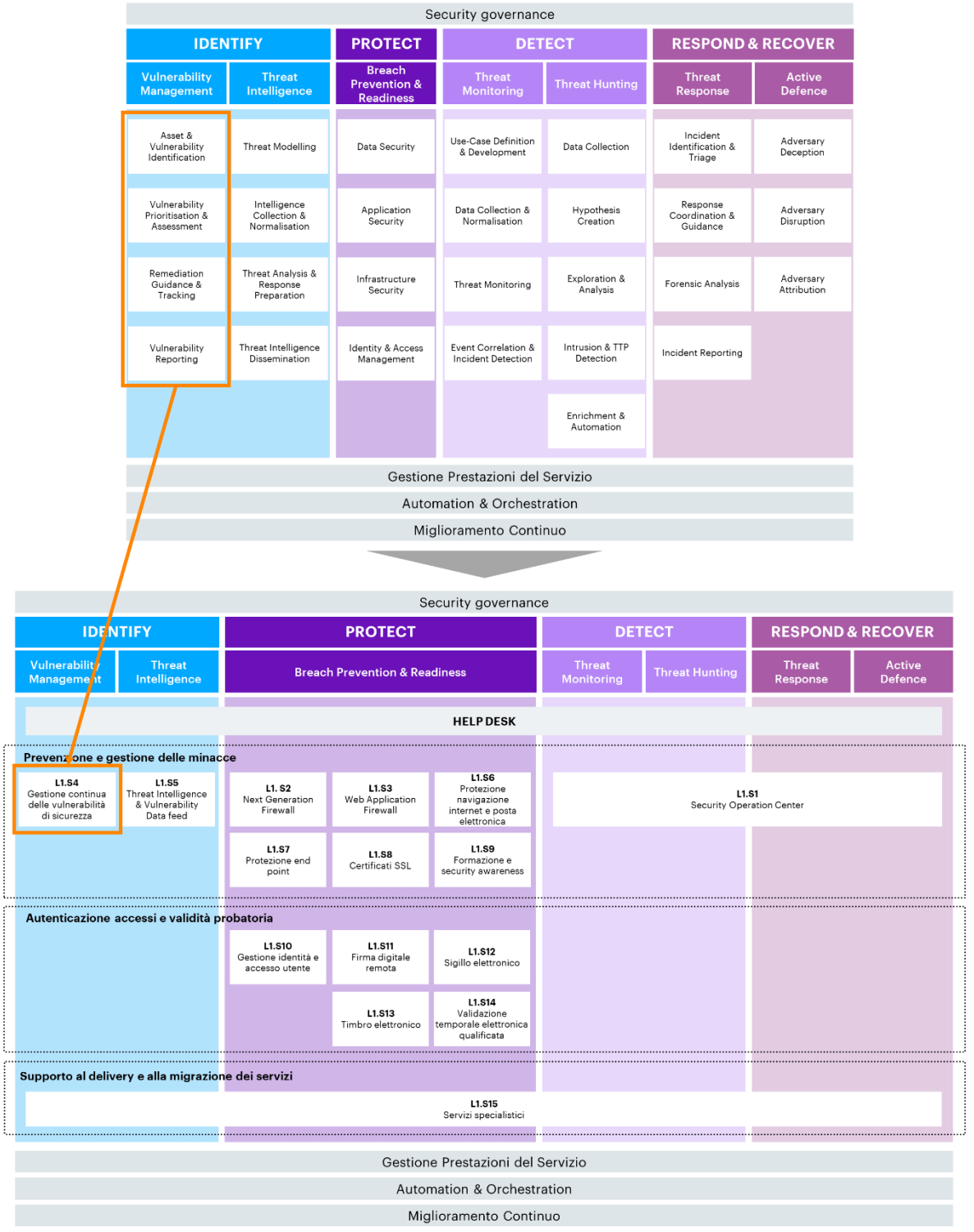


Figura 2– Aderenza tra CDOM e servizi della Fornitura

Il valore aggiunto della metodologia proposta è dato dalla disponibilità di linee guida, processi, esempi e template organizzati gerarchicamente secondo tre livelli: 1. **Framework dei servizi di sicurezza** (cfr. fig. 3): costituisce la rappresentazione di alto livello della metodologia, che esprime l'articolazione della stessa in 4 macro funzioni (es. in figura "*Identify* "), 7 domini di sicurezza, che costituiscono il focus di "Cosa" si deve fare per la metodologia in esame in riferimento a uno specifico servizio (es. "*Vulnerability Management*") e 28 sotto-servizi, che costituiscono il focus di "Come" si deve operare in riferimento a uno specifico servizio (es "*Asset & Vulnerability Identification*"); 2. **Caratteristiche dei servizi**: raccolta di Libreria di Procedure, Funzioni Fondamentali, Playbook, template di servizio, Architetture di riferimento, Knowledge Base, Workflow, KPI di servizio, frutto di esperienze e best practice, che mettono a disposizione un patrimonio informativo esaustivo e fondamentale per accelerare l'avvio e l'erogazione del servizio per ogni tipologia di PA. A titolo esemplificativo, la seguente figura illustra la "navigazione" all'interno del framework metodologico proposto relativamente al servizio di Vulnerability Management. 3. **Sviluppo di una caratteristica:** foglie terminali del framework che mostrano come le caratteristiche del servizio si sviluppano in attività da svolgere, loro sequenza e flussi di dati (ad es. la figura mostra lo sviluppo del flusso di lavoro del Processo di Gestione continua delle Vulnerabilità di sicurezza.

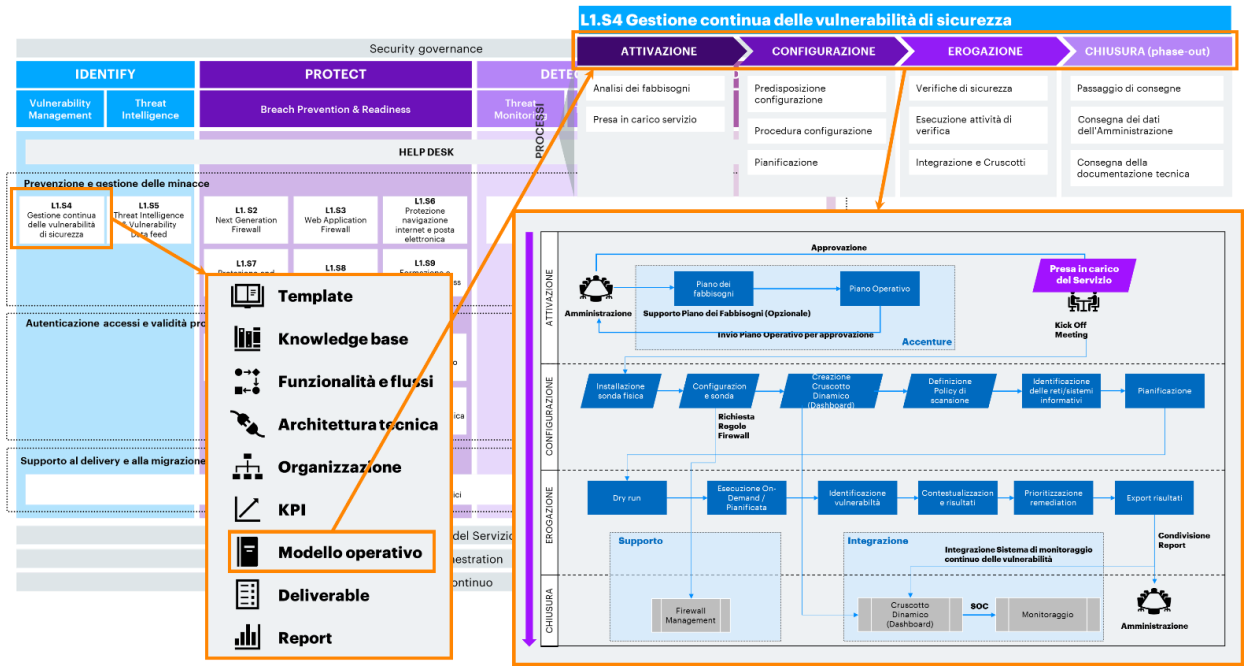


Figura 2 - Struttura e componenti del CDOM

Oltre la classificazione dei servizi, il modello CDOM fornisce una visione e guida complessiva alle interazioni tra i diversi servizi, come illustrato in figura.

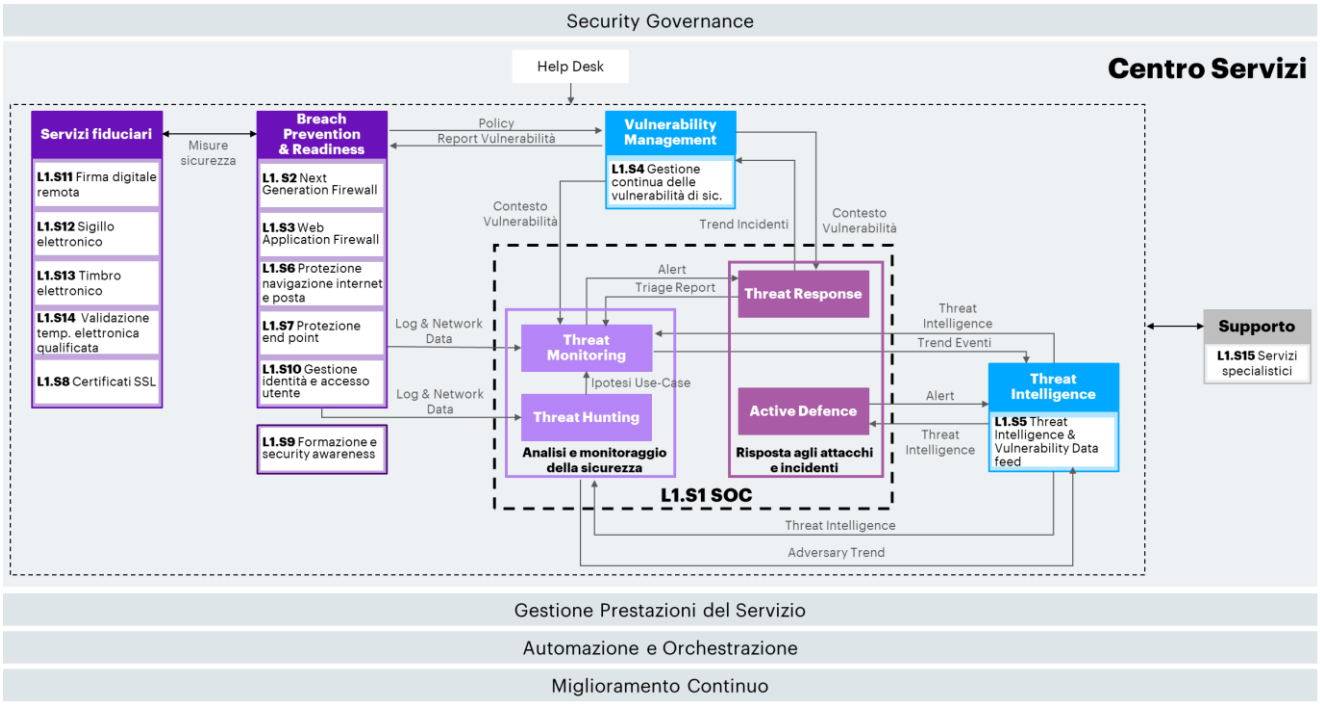


Figura 3 - CDOM - Sistema di interazioni tra i servizi

Infine, useremo il CDOM come **mappa logica di navigazione della presente relazione tecnica**, dal momento che rappresenta un utile strumento per dare evidenza degli elementi progettati a garanzia dell'omogeneità del servizio.

2 PRESENTAZIONE E DESCRIZIONE OFFERENTE

Nell'ambito dell'omonimo Gruppo internazionale, Accenture S.p.A. offre servizi di consulenza direzionale, realizzazione di sistemi e consulenza tecnologica e servizi alle imprese. Il gruppo impiega nel mondo più di 600 mila professionisti, è presente con uffici e sedi operative in più di 200 città di 51 Paesi e serve 5.000 clienti in oltre 120 Paesi nel mondo. In Italia, nell'esercizio 2020 ha sviluppato un fatturato di oltre 1,949 miliardi di Euro lavorando per oltre 300 clienti, tra i quali più di 30 clienti della Pubblica Amministrazione e gli enti di interesse pubblico (INPS, INAIL, Consip, Sogei, Ministero dell'Economia e delle Finanze, Ministero della Salute, Ministero degli Affari Esteri e della Cooperazione Internazionale, Ministero dell'Interno, Ministero dello Sviluppo Economico, AIFA, Regione Sardegna, Regione Lazio, Regione Toscana, Regione Lombardia, Roma Capitale, Poligrafico e GSE) e le più grandi aziende di tutti i settori industriali, finanziari e assicurativi (es. TIM, Vodafone, Mediaset, Unicredit, Fiat, Enel, ENI).

Accenture ritiene la Security una delle sue offerte più strategiche, sia nell'ambito dei programmi di trasformazione digitale che nell'ambito dell'erogazione dei servizi gestiti (Managed Security Services) per numerosi clienti nazionali e internazionali (es. Sogei, Senato, Min. Interno, Regione Sardegna, Comune Roma, ENEL, ENI, Intesa San Paolo, NEXI, Poste Italiane, PostePay, SNAM). L'**unità operativa Security** è la più ampia practice italiana in ambito, in grado di coprire end-to-end i servizi di sicurezza ed è riconosciuta come leader di mercato sia per i servizi di sicurezza gestiti che di consulting a livello globale e locale/europeo (Forrester, IDC). Accenture Security si avvale di:

- oltre 2.100 certificazioni professionali di processo e sicurezza (ISO27001, CISA, CISM, ISO22301, OPST, CSSLP, CRISC, CIPP, ABCP, CBCP, GCIH, GREM, GCFA, GMOB, GWAPT SSCP, CCSP, OSCP, CEH, GSEC, GCIA, GCED, GPPA, GMON, GCCC, ITIL, CISSP, etc.) e certificazioni specifiche di prodotto;
- strutture e capacità certificate in tutto il mondo (comprendenti ISO 9001, ISO 14001, ISO 20000, ISO 27001, CREST-CBEST, CMMI, CSA STAR ecc.);
- continuo investimento in acquisizioni di società specializzate in materia cybersecurity tra cui FusionX, Maglan, iDefense , Symantec, Context-IS (UK), OpenMinded (Francia) e Sentor (Svezia).

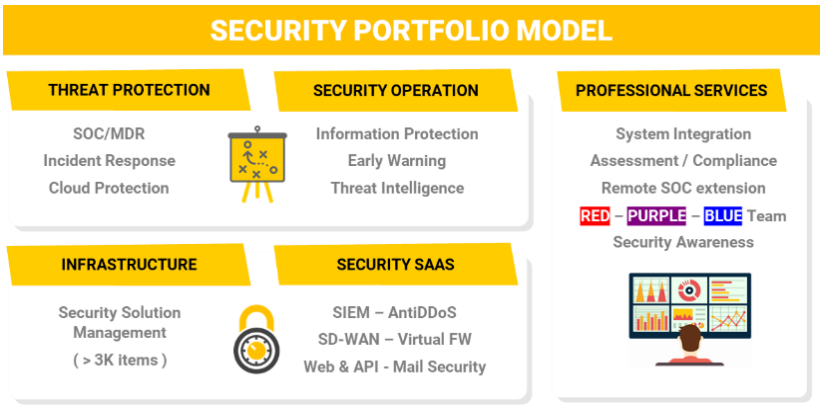
Vendor	Livello di Partnership (selezione)
Symantec	Platinum Global System Integrator
TrendMicro	Gold Reseller
Fortinet	Global Partner
CISCO	Gold Certified Cisco Channel Partner
Splunk	Elite Reseller, Managed Services, System Integrator
CyberArk	Advanced Reseller
SAP	SAP Service Partner Global VAR Platinum Level
RSA	System Integrator
IBM	IBM Platinum Business Partner
Palo Alto	Global System Integrator Partner
Microsoft	Gold Globally Recognized Partner
Oracle	Platinum Partner Global Cloud Elite
Citrix	Citrix System Integrator
ServiceNow	Global Strategic Partner
Suse	SUSE Accredited Partner
HPE	Global SI Alliance Partner
Netapp	Global System Integrator
Veritas	Veritas Platinum Tier partner

Accenture può vantare una vasta serie di alleanze e **partnership** strategiche con i principali Vendor in ambito sicurezza, volte a massimizzare la qualità dei servizi offerti pur mantenendo comunque un profilo indipendente e un insieme di asset, metodologie, framework e strumenti proprietari che consentono di garantire coerenza, uniformità ed efficacia alla gestione dell'intera Fornitura.

Fastweb, con più di 2,7 milioni di clienti (di cui 1,6 milioni collegati in tecnologie ultrabroadband, in crescita del 23% rispetto allo scorso anno), è uno dei principali operatori di telecomunicazioni in Italia. Parte del gruppo Swisscom dal settembre 2007, Fastweb offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese. Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultra-larga. Con un investimento di oltre 10 miliardi di euro, ha realizzato una rete in fibra ottica di nuova generazione che raggiunge ad oggi 55.500 km di tracciato, con oltre 4.000.000 di km di fibra (la più estesa d'Europa). Grazie all'espansione e al continuo potenziamento della rete ultra-broadband, Fastweb raggiunge oggi 22 milioni di abitazioni, di cui 8 con rete proprietaria, con velocità di collegamento fino a 1 Gigabit. La società offre inoltre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G, 4G Plus e 5G. Dall'ultimo osservatorio AGCOM, Fastweb è risultata essere leader per l'offerta di servizi con prestazioni superiori a 100 Mb/s con il 37,7% del mercato e primo operatore alternativo nel segmento dei grandi clienti pubblici e privati. Fastweb, inoltre, secondo l'indagine realizzata dall'Istituto Tedesco di Qualità e Finanza in cooperazione con l'Università Goethe di Francoforte, è il miglior operatore in Italia per il servizio di connessione in fibra ottica Ftth (Fiber to the home) ed è risultata tra le aziende "Top" anche per il servizio di connessione ADSL. Contestualmente all'infrastruttura di rete, Fastweb ha sviluppato un'infrastruttura IT di eccellenza, attraverso Data Center di proprietà distribuiti sul territorio nazionale, che permettono di erogare i più avanzati e complessi servizi a valore aggiunto. Fastweb è stata inoltre la prima Azienda in Italia a dotarsi di un Data Center certificato TIER IV dall'UpTime Institute di New York, l'ente che valuta l'affidabilità e la continuità del servizio e delle architetture di ridondanza dei Data Center in tutto il mondo. Il **nuovo Data Center** di Milano è in grado di garantire la massima sicurezza per i dati delle Aziende Clienti ed è **integrato con il SOC (Security Operation Center)**, il centro di prevenzione dagli attacchi informatici costituito interamente da personale Fastweb altamente qualificato e operante 24 ore su 24 su 365 giorni. Grazie alle proprie infrastrutture, Fastweb dispone, quindi, di una gamma completa ed integrata di servizi TLC e ICT avanzati, come l'housing, il Cloud computing, la sicurezza e la comunicazione unificata, in grado di soddisfare le esigenze di tutti i segmenti di mercato e di Aziende di tutte le dimensioni, dalle start-up alle piccole e medie imprese, dalle società di

grandi dimensioni fino al settore pubblico.

In ambito ICT, Fastweb ha recentemente acquisito Cutaway, società specializzata in progetti ICT, con l'obiettivo di rafforzare il proprio posizionamento di fornitore di servizi Cloud nel mercato Enterprise e proseguendo nella strategia di costante rafforzamento dell'offerta di Cyber Security ha acquisito una quota del 70% di 7Layers, società leader nei servizi per la sicurezza informatica inserita, dal 2017 al 2020, dal Financial Times nella classifica delle 1000 "fastest-growing companies" a livello Europeo. Nel segmento Enterprise, Fastweb è riconosciuta come fornitore d'eccellenza per affidabilità e competitività dei servizi ed è il primo fornitore della Pubblica Amministrazione in Italia, potendo vantare la presenza in una pluralità di enti della Pubblica Amministrazione Centrale e Locale essendo aggiudicataria di numerose Convenzioni e Accordi Quadro quali ad esempio, **SPC Cloud L2**, SPC 2 Connettività, SGM, Infrastrutture Condivise SPC, TF5, CT5, AQ DTO3, AQ System Management.



FINCANTIERI NexTech

Fincantieri NexTech S.p.A. è una società tecnologica, appartenente al Gruppo Fincantieri, che opera principalmente per lo sviluppo di soluzioni nei settori della sicurezza e della protezione di informazione, rappresentando il **centro di competenza tecnologico del Gruppo Fincantieri**. Fincantieri NexTech, grazie alle esperienze maturate nel settore militare e della sicurezza, alle competenze specifiche nell'analisi degli scenari operativi e alla capacità di realizzare dei sistemi complessi operanti in "ambienti ostili", è in grado di supportare lo sviluppo e l'integrazione sia di soluzioni "Legacy" che di infrastrutture di campo sia su piattaforme software tradizionali (SCADA) che con l'architettura SOA (Service Oriented Architecture) ed erogare servizi di SOC, le cui competenze e la territorialità gli permettono di erogare servizi di monitoraggio di sicurezza sia da remoto sia nella sede del cliente di primo e di secondo livello. Rappresenta una realtà di eccellenza tutta italiana capace di offrire prodotti e servizi nel campo dell'elettronica, della sistemistica avanzata, dell'Information Technology e della Cyber Security.

D E A S
DIFESA E ANALISI SISTEMI

Difesa e Analisi Sistemi S.p.A. (DEAS) è una PMI innovativa specializzata in Cyber Security e AI, in grado di fornire soluzioni tecnologiche con gli standard più alti del settore in ambito sicurezza informatica, intelligenza artificiale, GDPR, modelli di governance, soluzioni di continuità operativa. DEAS collabora con Grandi Aziende (Autostrade per l'Italia), Istituti bancari e Pubbliche Amministrazioni Centrali (Consip, Sogei, Agenzia delle Entrate, Ministero della Difesa, Camera dei Deputati, Senato della Repubblica, ISTAT, ecc.) e Locali (Regione Lazio, LazioCrea, ULSS).

Informazioni sui soggetti firmatari per il RTI

Franco Turconi, nato a [redacted] Procuratore della **Accenture S.p.A.**

Francesco Carrino, nato a [redacted] e **Riccardo Lodà**, nato a [redacted], Procuratori della **Fastweb S.p.A.**

Andrea Viero, nato a [redacted], Amministratore Delegato della **Fincantieri Nextech S.p.A.**

Stefania Ranzato, nata a [redacted] Amministratore Unico della **DEAS – Difesa e Analisi Sistemi S.p.A.**

Distribuzione dei servizi/attività tra le aziende partecipanti

La tabella riporta la distribuzione dei servizi/attività tra le aziende del RTI, secondo la notazione RACI; la A di Accountable non è stata inserita in quanto per definizione è sempre in capo alla mandataria e neanche la I di Informed in quanto pervasiva su tutte le aziende/servizi. La R indica Responsabilità ed esecuzione delle attività, mentre la C designa la collaborazione.

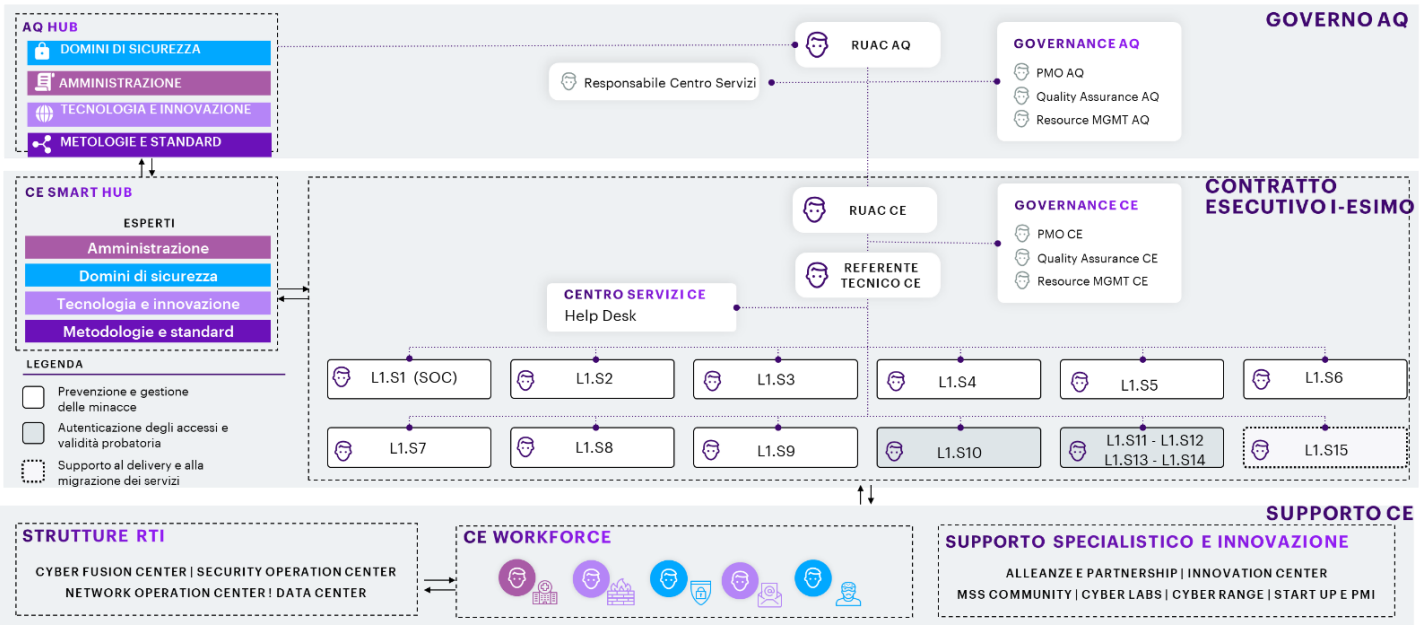
Servizi	Accenture	Fastweb	Fincantieri	DEAS
Governo della fornitura	R	C	C	C
Centri Servizi	R	R	C	C
Help Desk	R	C	C	C
Security Operation Center	R	R	C	C
Next Generation Firewall e Web Application Firewall	C	R	C	C
Gestione continua delle vulnerabilità di sicurezza	R	C	C	C
Threat Intelligence & Vulnerability Data Feed	R	C	C	C
Protezione navigazione Internet e Posta elettronica	C	R	C	C
Protezione end point	C	R	C	C
Certificati SSL e servizi di Validità Probatoria	R	C	C	C
Formazione e security awareness	R	C	C	C
Gestione dell'identità e l'accesso utente	R	C	C	C
Servizi specialistici	R	R	C	C

3 STRUTTURA ORGANIZZATIVA

La nostra proposta organizzativa è stata progettata per governare e indirizzare l'affidamento, nell'ambito del Lotto 1, dei **servizi di Sicurezza da remoto** delle PA. Si tratta di un contesto altamente critico e in continua evoluzione, rispetto al quale siamo in grado di garantire sia **continuità** dei servizi già previsti nella precedente iniziativa SPC Cloud L2 sia **approcci e tecnologie innovative** con l'obiettivo di migliorare la **resilienza delle PA contro le minacce informatiche**. L'organizzazione proposta **consolida** il meglio sia di quanto applicato per la **PA**, in particolare da Accenture e Fastweb, su altri Accordi Quadro Consip (compreso SPC Cloud L2) sia l'esperienza specifica in ambito **sicurezza** di grandi e complesse forniture realizzate per **clienti privati e infrastrutture critiche del Paese** (es. banche e servizi finanziari, telecomunicazioni, operatori energetici di produzione, trasmissione e distribuzione, infrastrutture e trasporti). L'organizzazione di seguito illustrata è reattiva e agile, e permette di gestire in maniera flessibile e scalabile l'erogazione dei servizi in base alle specifiche esigenze; è tale da garantire: ✓la **gestione dell'Accordo Quadro (AQ)** nel suo complesso, con ruoli di organizzazione, indirizzo e controllo dei diversi **Contratti Esecutivi (CE)** attivati (**Governo dell'AQ**); ✓il **coordinamento dei singoli CE** e l'erogazione dei servizi richiesti per ciascuno di essi (**Gestione dei CE**); ✓la capacità di adattarsi dinamicamente alle necessità della singola PA in base, ad esempio, alla maturità della stessa in ambito cybersecurity, alle dimensioni, al contesto tecnologico, alla tipologia di dati trattati, alla distribuzione geografica e all'appartenenza del Perimetro di Sicurezza Cibernetico Nazionale.

3.1 Modalità Organizzative e Organigramma

Il modello proposto si articola sui tre livelli rappresentati in figura:



- **Livello di Governo dell'AQ -** rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera Fornitura. Come anticipato, Accenture e Fastweb vantano una pluriennale esperienza di successo nella gestione di Accordi e Contratti Quadro di dimensioni e complessità analoghe al presente AQ, esperienza che ha consentito di raggiungere **livelli di eccellenza** sia nella capacità di **scalare rapidamente** in funzione delle richieste delle PA sia nella **capillarità** di presenza sul territorio nazionale, come dettagliato al §3.2. Ad esempio, **Accenture** nell'ambito di AQ/CQ di cui è stata assegnataria, è giunta ad erogare **62 contratti** in parallelo (anche di grandi dimensioni) con l'impegno di circa 1400 professionisti, e **Fastweb,** nell'ambito dei diversi AQ/CQ già citati in Premessa**,** nel periodo 2017-2021 ha operato su **circa di 6.800 CE**, ripartiti tra **PAC** e **PAL**. Per gli elementi concreti in termini di infrastrutture e risorse a dimostrazione di tale scalabilità e capillarità si rimanda ai dettagli forniti al §3.2. Il livello di Governo AQ è presieduto dal Responsabile unico delle attività contrattuali dell'AQ (**RUAC AQ**), che svolge un'azione di indirizzo e controllo strategico in ottica di gestione unitaria dei CE. Il RUAC AQ è designato dalla mandataria, presiede il **Comitato di Coordinamento del RTI** composto da figure manageriali delle nostre aziende e dal **Responsabile del Centro Servizi** (per la cui organizzazione si rimanda al §4), che insieme definiscono la strategia di AQ e assicurano una visione unica e integrata dell'andamento dei servizi oggetto di gara garantendo al tempo stesso la qualità complessiva dei CE per conseguire la piena soddisfazione delle PA. Il RUAC AQ è il principale riferimento del RTI per Consip, rappresenta inoltre il RTI all'interno dell'**Organismo Tecnico di Coordinamento e Controllo** ed è quindi la principale interfaccia verso i soggetti istituzionali su tutte le tematiche contrattuali. È supportato dal team di **Governance AQ** che include strutture/ruoli aggiuntivi (offerti senza oneri aggiuntivi) quali: Project Management Office, Quality Assurance e Resource Management (cfr. §3.3).
- **Livello dei Contratti Esecutivi -** è progettato per adattarsi alle diverse tipologie di PA che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi. A tale livello sono coordinati ed erogati i servizi previsti per ogni CE ed è prevista la presenza di: ✓un Responsabile unico delle attività contrattuali del CE (**RUAC CE**), ✓un **Referente Tecnico CE**, ✓un **team di Governance CE**, ✓un **Help Desk** dedicato all'assistenza dei Referenti identificati dall'Amministrazione, ✓**team** responsabili dell'**erogazione** dei servizi previsti. Il RUAC CE ha una responsabilità speculare a quella del RUAC AQ e rappresenta la principale interfaccia verso le singole PA per tutte le tematiche contrattuali, avendo allo stesso tempo compiti di raccordo tra i due livelli. Il Referente Tecnico CE è responsabile del corretto svolgimento delle attività e dei servizi e il relativo livello di qualità di erogazione per il singolo CE ed è supportato dal team di Governance CE (PMO CE, Quality Assurance CE e Resource Management CE). I Team responsabili dell'erogazione dei servizi, composti da professionisti di settore, hanno l'ulteriore supporto dei maggiori esperti di tematica del RTI (Subject Matter Expert) per assicurare omogeneità di metodologie e innovazione continua in base all'evoluzione del contesto.
- **Livello Supporto CE -** garantisce due tipi di supporto: ✓scalabilità, ✓supporto specialistico e innovazione. **SCALABILITÀ**: la **CE Workforce** comprende le strutture di appartenenza delle risorse assegnate ai CE, quali **Cyber Fusion Center/Security Operation Center/Network Operation Center/Data Center** (cfr. §4), la

cui dimensione garantisce flessibilità e scalabilità adeguata alle esigenze (es. aumento della domanda, complessità progettuale, contesto tecnologico, sensibilità dei dati). **SUPPORTO SPECIALISTICO E INNOVAZIONE:** comprende: ✓i **CdC tecnologici** (es. infrastruttura, rete, applicazioni, DB, S.O., sistemi di virtualizzazione e HW); ✓i **Cyber Labs** di Accenture, operanti a livello globale per introdurre nuove tecnologie di sicurezza tramite prove di laboratorio che ne facilitano l'integrazione sui sistemi cliente, e i **centri di ricerca e sviluppo in ambito cyber** di Fastweb, Fincantieri e DEAS; ✓il network di **start-up e PMI innovative**; ✓le **partnership** con i principali vendor in materia sicurezza; ✓le **MSS COMMUNITY**, specializzate per **ambito** (es. Application Security, Digital Identity, Threat Operations, Cloud Security, Continuous Risk Management), **tecnologia** delle soluzioni offerte e/o presenti presso le PA richiedenti, **tematica** (es. ambiti Difesa, Sanità); ✓i **Cyber Range** (Poligoni Cibernetici) di Accenture e DEAS; ✓i laboratori di **test plant** di Fastweb utilizzati per testare gli apparati di sicurezza, così come nella verifica della conformità dei prodotti effettuata dai CVCN (Centro di Valutazione e Certificazione Nazionale) e CV. In particolare, per la capacità del RTI di supportare Consip, le PA e gli organismi istituzionali (es. AgID, Agenzia per la Cyber Sicurezza Nazionale) in materia di Innovazione si rimanda al §17.

- **AQ HUB e CE SMART HUB** - Strutture aggiuntive composte da esperti di diversi ambiti, con il compito di stimolare e promuovere, rispettivamente a livello di AQ e di CE, l'innovazione e le competenze tecnologiche nell'erogazione dei servizi, rafforzare il livello di conoscenze nei vari domini di sicurezza e di awareness verso le PA anche rispetto alle opportunità offerte dal contratto, garantire la conformità a standard e best practice di settore. La forza degli HUB è quella di offrire un supporto qualificato e innovativo avvalendosi del network nazionale e internazionale garantito dalle aziende del RTI. Di seguito la loro descrizione.

Competenze a disposizione dell'Accordo Quadro e del Contratto Esecutivo

Gli HUB AQ e CE forniscono il supporto di esperti per rafforzare le competenze e le metodologie possedute dai team. L'AQ HUB opera trasversalmente su tutti i CE per garantire: ✓un livello di qualità dei servizi di sicurezza erogati elevato e uniforme, ✓la diffusione dell'innovazione, ✓il corretto riuso e l'omogeneità di approccio. L'Hub è strutturato in 4 ambiti di competenza identici a livello di AQ e di CE: **Domini di Sicurezza (DS), Amministrazione (AMM), Tecnologie e Innovazione (T&I), Metodologie e Standard (M&S)** con i seguenti compiti.

Ambito	Competenze e asset messi a disposizione della Fornitura
DS	Garantire l'omogeneità di erogazione dei servizi per **dominio/servizio** oggetto dell'AQ, fornendo una guida ai team di erogazione servizi. Infatti, ciascun servizio avrà, nell'AQ HUB, un **Referente di Dominio**, individuato come la persona del RTI con maggiore esperienza sullo specifico servizio. Oltre la **garanzia di uniformità e qualità** tra i diversi CE, tali referenti hanno l'importante ruolo di contribuire al **veloce avvio dei servizi**: fin dalla definizione dei fabbisogni lavorano alla configurazione del servizio avvalendosi ✓sia degli **standard tecnologici e procedurali** del Centro Servizi (cfr. anche il ruolo del modello CDOM ai §§1 e 3.3, modello rispetto a quale i Referenti di Dominio **assicurano aderenza** in ogni CE) ✓sia dei "**Managed Security Twin**", vale a dire configurazioni di servizio già applicate in realtà analoghe (per questo "gemelle") e raccolte anche per diffondere lessons learned, best practice e conoscenza messi a punto nel corso dell'AQ. Si sottolinea in particolare che, per la rilevanza del SOC, è previsto un ruolo di **Referente del Security Operation Center** che si occuperà anche di supportare le PA, in maniera uniforme, nel processo di notifica verso le Autorità Competenti (CSIRT Italia, Garante Privacy) in caso di rilevamento di incidenti di sicurezza e per il continuo miglioramento del servizio erogato.
AMM	Ascoltare le esigenze delle PAL o PAC e degli utenti finali, facilitare il confronto tra di esse, pubblicizzare i casi di successo per stimolare l'adesione all'AQ, favorire la cooperazione e la resilienza della macchina amministrativa, analizzare i fabbisogni e garantire la realizzazione di proposte innovative. L'ambito AMM, grazie alla conoscenza di contesto, indirizza l'innovazione tecnologica dei servizi affinché tengano conto delle peculiarità delle PA (es. difesa e sicurezza pubblica, sanità, municipalità). Tra gli esperti in questo ambito sono selezionati primariamente i RUAC di CE sulla base del contesto specifico della PA richiedente. Rientrano in questo ambito, a livello di AQ, anche gli **Account Territoriali** (uno per Regione/Provincia Autonoma) che apportano consapevolezza delle specificità regionali e promuovono la conoscenza dell'AQ sul territorio.
T&I	Assicurare le **competenze tecnologiche** sui trend innovativi legati alla sicurezza informatica, alla protezione dei dati personali e alle tecnologie emergenti: es. *Zero Trust, Sicurezza del Cloud, Sicurezza dell'Internet of Things, Artificial Intelligence, Autonomus Identity*. Il **Referente Tecnologia e Innovazione**, figura con esperienza nel contesto pubblico per la definizione di strategie di trasformazione digitale e cyber resilienza, è il punto di riferimento per i team dei servizi CE, coordinandone gli interventi per garantire unitarietà di approccio. L'innovazione è altresì garantita anche da un ampio ecosistema con i player tecnologici leader per i diversi servizi di alleanze (es. *Splunk, PaloAlto, Fortinet, Tenable, Qualys, Symantec, Crowdstrike, TrendMicro, CyberGuru, Forgerock, Okta, Oracle, Microsoft, IBM, Check Point)* e di continue acquisizioni da parte delle aziende componenti il RTI (*Maglan, FusionX, iDefense, Symantec, 7layers, e-phors, ecc.*). Il Referente Tecnologia e Innovazione è promotore dei lavori della **Cyber Security Room** strumento operativo per veicolare l'innovazione a livello di AQ e CE, descritta al §17. Inoltre, come da una **best practice** di Fastweb, sviluppata nel CQ SPC Cloud L2, nei casi d'integrazione dei sistemi del Fornitore con sistemi della PA, viene individuato un **Technical Account Manager (TAM)** per interfacciare direttamente il vendor di riferimento e ottimizzare le soluzioni applicate e i tempi di risoluzione di eventuali incidenti.
M&S	Garantire le **competenze su standard e metodologie** utili a gestire il programma nella sua interezza. Gli esperti Metodologie e Standard sono espressione di due diverse attività: 1) **continuo aggiornamento e recepimento** rispetto al panorama normativo e metodologico di riferimento, 2) **contributo diretto** alla definizione di linee guida, standard e best practice a livello nazionale e internazionale. **CONTINUO AGGIORNAMENTO E RECEPIMENTO** - Le aziende del RTI seguono un **processo strutturato di Aggiornamento e Recepimento** che garantisce alle PA sia la tempestiva individuazione di novità/aggiornamenti a livello nazionale e internazionale sia la proattività del RTI nel proporre soluzioni per il recepimento. Ad esempio, il perimetro di monitoraggio comprende: ✓Metodologie di riferimento su Modelli Operativi ✓Procedure per la erogazione dei Servizi e standard di sicurezza ✓Norme e Standard di Sicurezza per l'Accesso ai Dati Personali ✓Norme e Standard di Sicurezza per i servizi essenziali. **CONTRIBUTO DIRETTO** - ✓**Accenture** contribuisce direttamente alla definizione di linee guida, standard e best practice a livello internazionale (es NERC-CIP) e nazionale (es. a supporto del CERTFin); ha inoltre attivato collaborazioni con le primarie istituzioni, enti di ricerca e osservatori italiani in ambito cyber security tra cui il Politecnico di Milano, l'Associazione Bancaria Italiana (ABI), il Ministero innovazione tecnologica e transizione digitale (MITD), l'Agenzia per l'Italia Digitale (AgID); infine partecipa attivamente **principali osservatori e forum mondiali di settore** (es. WEF, FS-ISAC, ECSO come membro fondatore, etc)

✓**Fastweb** è l'unico operatore nazionale di TLC a contribuire attivamente con le proprie analisi al rapporto annuale CLUSIT sulla Sicurezza ICT in Italia (basata su oltre 35 milioni di eventi di sicurezza individuati) e collabora con l'Osservatorio Cybersecurity & Data Protection, promosso dalla School of Management del Politecnico di Milano; ✓**Fincantieri** partecipa attivamente al programma ECHO, tra le soluzioni studiate nel progetto si possono annoverare il quadro di valutazione multisettoriale, il sistema di allarme precoce, la federazione di Cyber Ranges, le roadmap tecnologiche intersettoriali, il Cyber Skills Framework e uno schema di certificazione della sicurezza informatica.

il Raggruppamento si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, almeno nella misura del **35,01%**.

3.2 Distribuzione delle responsabilità RTI

Con il nostro RTI mettiamo a disposizione della PA una **straordinaria complementarità**, fondata su 4 pilastri di eccellenza: ✓un player di **consulenza e tecnologia** a livello nazionale e internazionale ✓un primario operatore delle telecomunicazioni, protagonista di **grandi progetti infrastrutturali** ✓il primo gruppo italiano operante nei **settori difesa e sicurezza** ✓una PMI innovativa specializzata in **Cyber Security e AI** già apprezzata nel settore pubblico. Offriamo tra queste aziende una fote **sinergia** per realizzare una proposta efficace, efficiente e di qualità dei servizi offerti attraverso le **tre direttrici** di **continuità, evoluzione e innovazione**.

Continuità

Fastweb: ✓è uno dei principali interlocutori della PA nell'ambito della Cyber-sicurezza grazie alla titolarità di convenzioni come **SPC 2 Connettività** e **Contratto Quadro SPC Cloud L2**, ✓è fornitore ufficiale della PA da ben **15 anni** (SPC1/TF3 del 2006) con più di 5000 contratti attivati, ✓ha sviluppato un'**infrastruttura IT di eccellenza**, attraverso Data Center di proprietà distribuiti sul territorio nazionale, garantendo la connettività di rete SPC richiesta dalla fornitura, nonché tutti i servizi infrastrutturali che sottendono l'erogazione da remoto dal Centro Servizi del RTI, ✓ha profonda **penetrazione nel mercato PA**. A titolo esemplificativo citiamo: ✓convenzione SGM - gestiti circa 1.000.000 di apparati e 400.000 ticket nel 2019, di cui ca. 50.000 analoghi a quelli di cui al presente AQ; ✓SPC Cloud L2 - circa 30 contratti PAC e 100 PAL; ✓SPC 2 Connettività - oltre 300 PA servite su ca. 16.000 sedi).

Accenture: ✓l'unità operativa Security segue gli aspetti di sicurezza per tutti gli AQ e CQ di cui Accenture è titolare con servizi dedicati; la conoscenza riguarda più di **30 Amministrazioni Centrali** (Sogei, Min. Interno, Senato, Min. Esteri, Min. Salute, ecc.), con grande eterogeneità funzionale e dimensionale, nonché **PAL** quali Comuni di Roma e Milano, Regioni Lombardia e Sardegna; ✓è primo fornitore di servizi di sicurezza e Managed Security Services per le più importanti infrastrutture critiche del Paese, come istituti finanziari, assicurativi, operatori energetici e di telecomunicazioni operanti nel Perimetro di Sicurezza Nazionale (tra gli operatori italiani: i **6** principali istituti finanziari tra cui Intesa Sanpaolo e NEXI, i **6** principali operatori del settore energetico, oil & gas, tra cui ENI, ENEL e SNAM, **5** tra le principali aziende manufatturiere, **3** tra le principali aziende di telecomunicazioni, tra cui TIM) nonché per primari Enti della PA Centrale.

Fincantieri e **DEAS**: mettono a disposizione la loro esperienza di erogazione di servizi di Sicurezza in particolare per il **settore Difesa**.

Evoluzione

Accenture: ✓è il **più grande operatore mondiale e italiano di servizi di cyber security**, con 9.000 professionisti dedicati e oltre 1000 in Italia; ✓vanta un'offerta e una **copertura end to end in tutti i domini della sicurezza informatica**; ✓ha realizzato un modello operativo specifico per i servizi di sicurezza, il **CDOM descritto in Premessa e al §3.3**, che si **adatta perfettamente** al contesto di gara e alle esigenze delle diverse PA ✓è il **primo partner** di tutti i maggiori vendor di tecnologia in ambito Sicurezza, utili anche a valorizzare le tecnologie in uso presso le PA ✓ha **più di 500 asset proprietari**, **più di 400 brevetti** in ambito sicurezza e più di 15 acquisizioni di società specializzate in ambito cyber negli ultimi 5 anni (es. Maglan, iDefense, Symantec, FusionX), ✓opera per promuovere la security community nazionale di formazione e divulgazione per CISO, CRO e i principali stakeholder in ambito.

Fastweb: ✓è uno dei principali MSSP (Managed Security Service Provider) che eroga già servizi di sicurezza attraverso il suo Security Operation Center a numerose PA centrali e locali; ✓grazie alla sua **capillare distribuzione** sul territorio e la sua **catena logistica** consente una piena copertura delle potenziali esigenze di supporto richieste dalle PA; ✓è coadiuvato e supportato dal competence center e dall'osservatorio di sicurezza che si avvalgono di partnership consolidate con i maggiori player e vendor.

Fincantieri: ✓mette a disposizione esperienze e progetti per sviluppare la difesa cibernetica delle infrastrutture critiche nazionali (es. porti).

In particolare, ai fini dell'analisi delle minacce informatiche, garantiamo l'**accesso alle informazioni di molteplici e variegati sorgenti, di livello nazionale e internazionale**, per abilitare le successive attività di **elaborazione e correlazione** e per **proporre** alle PA le azioni di contrasto e mitigazione più opportune.

Innovazione

Vantiamo una rete di **più di 30 centri di eccellenza** - tra cui centri di Ricerca e Sviluppo (Cyber Labs e Innovation Center), Cyber Range (Poligoni Cibernetici), Delivery Center e Cyber Fusion Center - da cui vengono erogati i servizi di sicurezza gestiti (Managed Security Services) in uno spazio di lavoro immersivo e dove collaboriamo anche per sviluppare nuove soluzioni, tecniche e strumenti per prevenire e gestire le minacce informatiche. Per dettagli sulle strutture messe a disposizione per l'innovazione si rimanda al §17.

Le sinergie tra le aziende sono assicurate dal **Comitato di coordinamento del RTI**, per garantire il massimo sostegno alle iniziative dell'AQ. Il Comitato – per semplicità espositiva non riportato nella figura rappresentante la struttura organizzativa - è composto da dirigenti delegati delle aziende coinvolte, dal RUAC AQ e dai RUAC e dai Referenti Tecnici dei più rilevanti CE in corso.

La modalità operativa proposta consente al team di AQ di: ✓adattarsi alle esigenze delle diverse tipologie di PA in termini di tematiche, tecnologie, evoluzioni progettuali e dimensioni, grazie all'impiego di esperti a livello di AQ che, intercettando in anticipo i potenziali fabbisogni, di concerto con i team di Resource Management, agilmente identificano le strutture più adatte da coinvolgere per la creazione dei CE ✓valorizzare il contributo delle diverse realtà aziendali a copertura

di tutte le competenze necessarie, grazie ad un approccio proattivo che cura lo sviluppo continuo degli skill in base alle esigenze previste o espresse.

La seguente tabella mostra la **ripartizione delle responsabilità** delle Aziende in RTI, considerando che Accenture, quale mandataria del RTI, esprime il ruolo di responsabile unica del risultato per l'AQ, assicurando trasversalmente il governo, il coordinamento e la qualità dell'iniziativa; contestualmente si esalta la complementarità delle competenze, che guidano l'assegnazione dei task di servizio, assegnandone la responsabilità (R) all'azienda più esperta per quella competenza.

Servizi	Accenture SC	Accenture MSS	Fastweb DC	Fastweb CC	Fincantieri	DEAS
Governo della fornitura	R	C	C	C	C	C
Centri Servizi	C	R	R	C	C	C
Help Desk	C	R	C	C	C	C
Security Operation Center	C	R	C	R	C	C
Next Generation Firewall e Web Application Firewall	C	C	C	R	C	C
Gestione continua delle vulnerabilità di sicurezza	C	R	C	C	C	C
Threat Intelligence & Vulnerability Data Feed	C	R	C	C	C	C
Protezione navigazione Internet e Posta elettronica	C	C	C	R	C	C
Protezione end point	C	C	C	R	C	C
Certificati SSL e servizi di Validità Probatoria	C	R	C	C	C	C
Formazione e security awareness	R	C	C	C	C	C
Gestione dell'identità e l'accesso utente	C	R	C	C	C	C
Servizi specialistici	R	C	C	R	C	C

Legenda: R=Responsabile dell'attività – C=Collaboratore | Accenture SC – U.O. di Security Consulting; Accenture MSS – U.O. di Managed Security Services; Fastweb DC – U.O. responsabile dei centri servizi e dei Data Center; Fastweb CC – U.O. Centro di Competenza Security

3.3 Aderenza al contesto e coerenza generale dei ruoli, risorse e strutture aggiuntivi proposti e interazioni con l'Amministrazione

Aderenza al contesto

Garantiamo la migliore combinazione in termini di **modello operativo**, **competenze tecniche** del personale, aspetti **organizzativi** e **logistici** per rispondere completamente alle esigenze espresse nel capitolato. Il fattore unificante per l'erogazione dei servizi è il **modello operativo CDOM** (cfr. Premessa) che **copre tutti i servizi richiesti**. Il CDOM offre un linguaggio e una modalità operativa standardizzata e comune per tutto il personale di Fornitura. In figura riportiamo i domini del modello CDOM da cui i servizi attingeranno i modelli organizzativi, operativi, di reporting, i processi, i casi d'uso e la knowledge base utili per: ✓una **rapida messa in opera abilitata da veri e propri "template di servizio"**; ✓un'**erogazione uniforme in termini di qualità e standard** (per i dettagli si rimanda ai §§ da 6 a 14). Il CDOM, concepito sulla base di riconosciuti standard e best practice di settore (NIST, ISO27001, ISO22301, ISO31000, ITIL, etc.) è allineato alle normative vigenti (eIDAS, NIS, GDPR, ecc.). CDOM è stato consolidato ed evoluto nel corso del tempo sulla base delle esperienze maturate in contesti di complessità analoga a quelle delle PA future contraenti (es. Intesa Sanpaolo, Unicredit, ENI, ENEL, NEXI, SNAM) e arricchito e integrato dalle competenze verticali ed esperienze di Accenture, Fastweb, Fincantieri e DEAS nella PA (es. Mini. Interno, Stato Maggiore Difesa, Senato, Sogei, INPS, INAIL, ISTAT, Regioni Sardegna, Lombardia, Liguria, nonché Governo U.S.A, Governo U.K.).

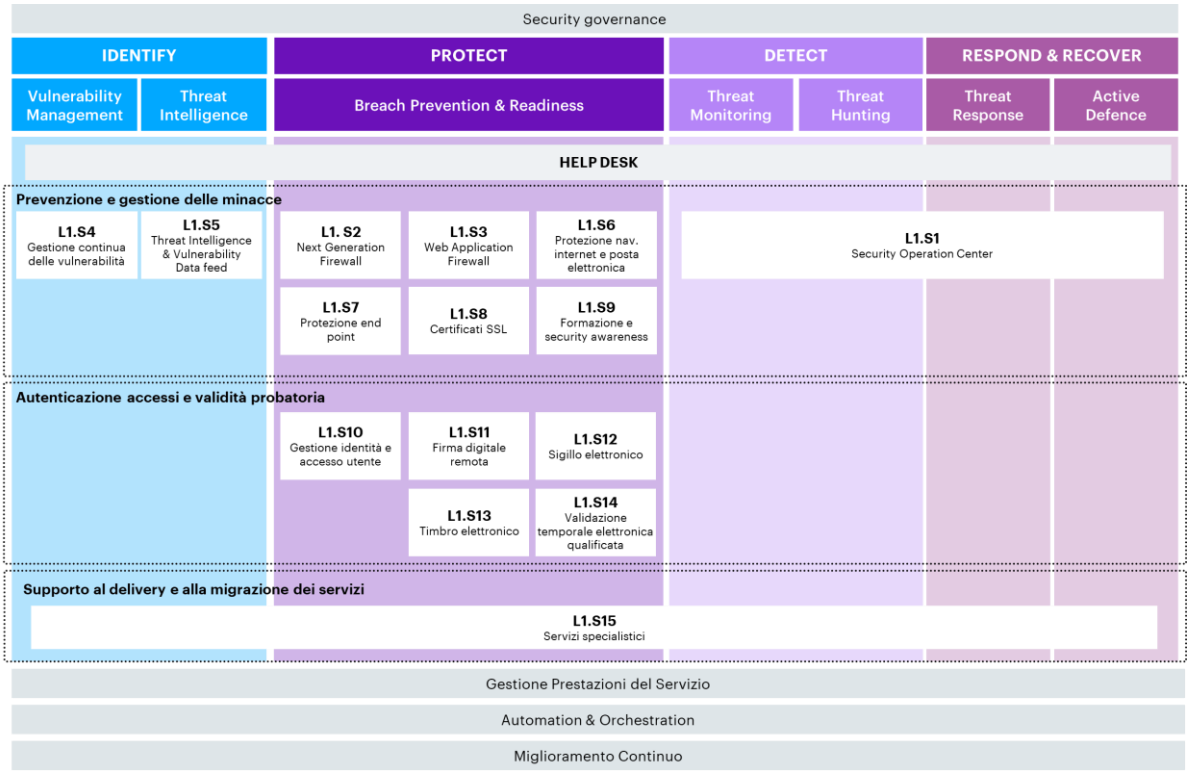
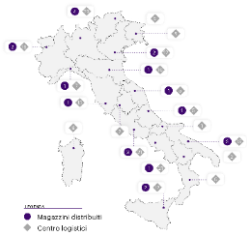


Figura 4 - CDOM

Competenze tecniche: ✓La mandataria Accenture ha nell'unità operativa Security una delle aree più strategiche della società in termini di programmi di trasformazione e servizi di sicurezza per i propri clienti in tutto il mondo; ✓Fastweb è riconosciuta come fornitore d'eccellenza per affidabilità e competitività dei servizi ed è il primo fornitore della PA in Italia; ✓Fincantieri e DEAS puntano proprio sull'innovazione tecnologica e una verticalizzazione in ambito difesa. In questo quadro le competenze tecniche sono il volano essenziale per offrire servizi di qualità; le aziende del RTI investono continuativamente in **formazione specialistica di settore** e i professionisti messi a disposizione dell'AQ hanno conseguito **più di 2.100 certificazioni** di processo e sicurezza (tra cui ISO 27001, ISO 22301, CISSP, CISM, CRISC, CEH, CSSLP, MBCP) e specifiche di prodotto (Splunk, IBM QRadar, Fortinet, PaloAlto, Oracle, FireEye, McAfee, Cisco, ecc.); inoltre DEAS dispone di un LVS (Laboratorio Valutazione Sicurezza) con **valutatori certificati** OCSI (Organismo di Certificazione della Sicurezza Informatica). Queste competenze sono poi **potenziate**

dal ricorso al ricco network di strutture del Supporto Specialistico e Innovazione, illustrato al §3.1.



Organizzazione e Logistica: garantiamo una **copertura completa** sul tutto il territorio nazionale, potendo vantare più di 40 tra **sedi** e **uffici in Italia,** e **una catena logistica con oltre 20 Centri Logistici e 168 Magazzini Distribuiti** e **personale distribuito** che consentono di fornire assistenza e servizi anche di prossimità in maniera **capillare** sia per la PAL che per la PAC (cfr. §2).

Ruoli, risorse e strutture aggiuntivi proposti per la gestione della fornitura e le modalità di interazione con l'Amministrazione

Per definire l'approccio generale di coordinamento e le modalità di interazione con le PA adottiamo l'Accenture Delivery Methods Program e Portfolio Management (ADM-PPM), il modello operativo proprietario coerente con le indicazioni del PMI, che raccoglie in una visione dinamica l'applicazione delle classiche aree di project management: ✓Strategia, Governo e Pianificazione; ✓Risorse e competenze; ✓Attività; ✓Rischio e Qualità; ✓Risultati. Di seguito, le fasi del modello con evidenza di azioni di Coordinamento e Interazione con PA e attori coinvolti.

1-PREDISPOSIZIONE/AGGIORNAMENTO RISORSE E STRUMENTI: la struttura del Resource Management, in collaborazione con l'AQ Hub, seleziona le risorse con le competenze più adeguate alle esigenze delle PA. La selezione è guidata dall'analisi del Piano dei Fabbisogni nonché dalla nostra esperienza in altri AQ/CQ. **2-PROMOZIONE AQ:** le risorse degli AQ HUB promuovono in modalità proattiva l'AQ tramite iniziative realizzate per lo più sul Portale della Fornitura, così da raggiungere il maggior numero di PA, cui si aggiungono le azioni di divulgazione della conoscenza dello strumento di AQ svolte sul territorio dai nostri Account Territoriali. **3-PREPARAZIONE CE:** la struttura del PMO AQ coordina le azioni per accompagnare le PA dal primo contatto fino alla stipula dei CE, avvalendosi anche di risorse provenienti dalle aziende del RTI per fornire consulenti esperti dei bisogni della specifica PA e in grado di anticiparne le necessità. Contattabile dal Portale, utilizza anche gli strumenti di collaboration per interagire con le PA. **4-ESECUZIONE CE:** fase operativa in cui sono erogati i servizi: ✓il Team di PMO CE coordina le attività di Project/Program Management e di Risk Management; ✓il Resource Manager e CE Smart Hub garantiscono lo staffing del CE con risorse del CE Workforce eventualmente integrate con PMI/start up/CdC; ✓i Responsabili Tecnici dei Servizi coordinano le attività richieste. **5-CONTROLLO E MONITORAGGIO:** le attività in esecuzione sono monitorate al fine di individuare criticità, attivare contromisure opportune e rendicontare ai Referenti della PA l'andamento dei servizi. In tale fase sono coinvolti i Responsabili Tecnici dei servizi nonché la struttura centrale di Governance CE, che forniscono supporto nella verifica degli SLA contrattuali e degli indicatori di digitalizzazione. **6-CHIUSURA FORMALE INTERVENTI E CE:** fase finale degli interventi/CE in cui si effettuano le verifiche formali del rispetto degli obblighi contrattuali. La struttura centrale di Governance CE aggiorna, inoltre, i dati a livello di AQ anche per consentire il controllo da parte degli Organismi di Coordinamento e Controllo. **7-CONDIVISIONE LESSONS LEARNED:** si opera per ✓condividere la conoscenza maturata sugli scenari di sicurezza delle singole PA, ✓analizzare situazioni di criticità e misure correttive adottate, ✓verificare l'opportunità di attività formative interne al RTI; protagonisti sono le strutture dell'AQ Hub e del Resource Management.

Inoltre, e come anticipato al §3.1, a livello organizzativo il **RUAC AQ** presiede il **Comitato di Coordinamento del RTI** per definire la strategia di business e assicurare omogeneità di erogazione ai CE ed è responsabile delle interazioni con Consip e gli **Organismi di Coordinamento**; in particolare con questi ultimi, l'interazione prevede uno **stato di avanzamento periodico**, almeno trimestrale, su: risultati raggiunti dalle forniture in corso, andamento dei contratti e attività di supporto alle PA. Di seguito un riepilogo di ruoli, risorse e strutture **aggiuntivi**.

Ruoli, risorse e strutture aggiuntivi	Descrizione
HUB di AQ e CE SMART HUB	Si rimanda per la descrizione al §3.1
Project Management Office di AQ (PMO AQ) e di CE (PMO CE)	Assicura un costante monitoraggio dell'avanzamento dell'AQ e dei CE, gestendo centralmente aspetti quali la pianificazione delle attività della fornitura e delle risorse, (Program Management) e la gestione della conoscenza (Knowledge Management)
Quality Assurance AQ e CE	Assicura il rispetto dei livelli di qualità richiesti durante la fornitura (Quality Assurance) e incentiva l'utilizzo di standard e metodologie uniformi in ottica di riuso e razionalizzazione
Resource Management AQ e CE	Valuta gli skill delle nostre risorse da dedicare all'erogazione dei servizi, sotto il profilo delle competenze tematiche, funzionali, metodologiche e tecnologiche.

Per i **ruoli aggiuntivi**: **Responsabile del Centro Servizi, Referenti di Dominio, Referente del Security Operation Center, Referente Tecnologia e Innovazione, Technical Account Manager, Account Territoriali** si rimanda alle descrizioni fornite al §3.1.

4 PROPOSTA PROGETTUALE PER I "CENTRI SERVIZI"

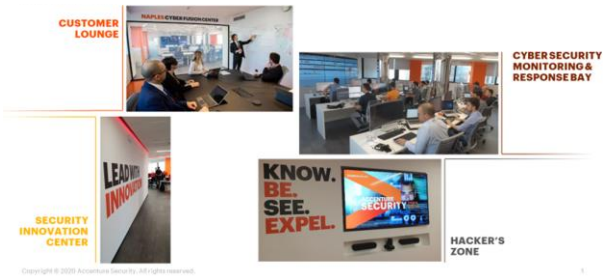
4.1 Descrizione del Centro Servizi

Il RTI eroga i servizi richiesti tramite il **Centro Servizi** che costituisce la struttura unica abilitante i servizi di fornitura e che tramite il servizio di Help Desk fornisce un punto unico di contatto alle PA. Il Centro Servizi (CS) si compone delle singole sedi operative appartenenti alle nostre Aziende che, operando in **modalità federata** e adottando **processi operativi univoci**, garantiscono l'erogazione di servizi (**Delivery Center**) e di gestione dei sistemi informatici (**Data Center**) secondo un modello disegnato per garantire scalabilità, performance e resilienza ad uso delle PA. Le singole sedi possono essere utilizzate da personale appartenente a ciascun componente del RTI così da rendere disponibili le migliori competenze necessarie all'erogazione dei servizi. Di seguito le sedi operative che costituiscono il CS.

Sede operativa	Tipologia	Indirizzo
Accenture Cyber Fusion Center Napoli (ACFC-N)	Delivery Center	Via Porzio, 6, 80143 Napoli (NA)
Accenture Assago (AAS)	Delivery Center	Strada 4, 4, 20089 Assago (MI)
Fastweb Caracciolo (FWCA)	Delivery Center & Data Center	Via Caracciolo, 51, 20155 Milano (MI)

Fastweb Bernina (FWB)	Data Center	Via Bernina, 6, 20158 Milano (MI)
Fastweb Omodeo (FWO)	Delivery Center	Via Adolfo Omodeo, 49, 70125 (BA)
Fastweb Polo Tiburtino (FWPT)	Data Center (Sito di Disaster Recovery)	Via Giacomo Peroni, 292, 00143 Roma (RM)

✓La sede **Accenture di Napoli** ospita il Cyber Fusion Center ovvero la struttura Accenture che concentra le attività di gestione, monitoraggio e innovazione in ambito Cyber Security. La struttura è operativa in modalità 24x7, conta su oltre 100 dipendenti specializzati e certificati sulle tecnologie da utilizzare per l'erogazione dei servizi e gestisce servizi per oltre 40 Clienti italiani ed europei. Il Cyber Fusion Center si inserisce in un network di centri presenti in tutto il mondo, dove vengono combinati servizi di sicurezza gestiti, tecnologie di automazione intelligenti e servizi integrati di difesa informatica per aiutare le organizzazioni a innovarsi e combattere il cyber-crime. Consente quindi di offrire ai nostri clienti un accesso diretto ai servizi più avanzati a livello mondiale, e allo stesso tempo, un punto di riferimento locale per la protezione del proprio business digitale. Il centro si sviluppa su una superficie di oltre 600mq e monitora oltre **224 miliardi di log** di sicurezza al giorno, gestisce **8.000 eventi** di sicurezza e oltre **200 incidenti** al giorno con grande potenziale di scalabilità. Inoltre il Centro riunisce le nostre capacità di gestione della sicurezza end-to-end, consentendo ai clienti di eseguire il monitoraggio degli eventi di sicurezza, fornisce assistenza dedicata per un'efficace gestione delle crisi attraverso l'adozione di azioni appropriate per rispondere a frodi e incidenti di sicurezza e lavora a stretto contatto con il Cliente, inviando avvisi tempestivi in caso di problemi di sicurezza e segnalando periodicamente lo stato dei servizi monitorati ✓La sede **Accenture di Assago** costituisce uno dei principali siti di delivery di Accenture a livello nazionale e ospita oltre 400 dipendenti specializzati nell'implementazione e gestione di tecnologie di sicurezza per clienti italiani ed europei. ✓La sede **Fastweb Caracciolo**, che impiega 420 dipendenti specializzati, ospita il Data Center che costituisce il sito primario di erogazione dei servizi di sicurezza grazie alla possibilità di ospitare i sistemi di elaborazione, connettività e storage in un **ambiente certificato** "**Tier IV – Constructed Facility**" dal Uptime Institute. Il Data Center è stato costruito e viene gestito con l'obiettivo di garantire il massimo livello di disponibilità dei servizi di elaborazione e connettività (garantita al 99,997%) grazie alla totale ridondanza delle infrastrutture di supporto. La sede ospita inoltre il SOC Enterprise di Fastweb, operativo in modalità 24x7 e disegnato per garantire la fornitura di Servizi Gestiti di Sicurezza alle grandi realtà Aziendali e Organizzazioni nazionali ed internazionali. ✓La sede **Fastweb Bernina** costituisce il secondo sito di erogazione dei servizi informativi ospitando i sistemi in ambienti certificati Tier III in grado di garantire una disponibilità dei servizi di elaborazione e connettività al 99,98%. ✓La sede **Fastweb Omodeo** ospita una ulteriore unità organizzativa adibita a Security Operation Center, che fornisce un presidio in h24 e costituisce un ulteriore back up alla sede Accenture di Napoli e Fastweb Caracciolo. ✓La sede **Fastweb Polo Tiburtino** costituisce il sito di Disaster Recovery per i servizi informatici, ospitando la terza copia dei dati di produzione (in aggiunta a quelle presenti a Caracciolo e Bernina) e le infrastrutture di connettività e di elaborazione necessarie alla loro messa in opera in caso di emergenza.



Il CS e, in particolare le relative sedi operative, utilizzano **servizi di connettività** garantiti da Fastweb assicurando i massimi livelli di servizio grazie a un'architettura di rete di backbone gerarchica, costantemente monitorata per verificare lo stato di occupazione di tutti i link. I collegamenti sono adeguati dinamicamente al superamento di valori di soglia rimodulati nel tempo. La **scalabilità dell'infrastruttura è stata confermata** in occasione del recente lockdown nazionale in cui Fastweb ha assorbito picchi di incremento del traffico sulla rete fino al 40% non pregiudicando la qualità del servizio erogata ai clienti sia Enterprise che Privati.

La **continuità operativa** dei servizi di elaborazione e connettività del CS è garantita dai **due Data Center Fastweb di Milano** (Caracciolo e Bernina) da cui erogare servizi basandosi sui paradigmi della virtualizzazione estesa e del Cloud Computing che, in perdita della disponibilità del sito primario, assicurano tempi di RTO e RPO prossimi allo zero. La robustezza della soluzione è ampiamente collaudata, essendo in uso da anni sui due Data Center Fastweb per l'erogazione di servizi verso enti pubblici e grandi aziende private. La soluzione proposta prevede, inoltre, il sito di **Disaster Recovery presso il Data Center Fastweb di Roma** (Polo Tiburtino) tale da garantire l'erogazione dei servizi anche a fronte di eventi catastrofici estesi che rendano indisponibili i 2 data center di Milano.

Il CS è in grado di erogare servizi in modalità sinergica tra le varie sedi operative, che già oggi operano con SLA superiori alla media di mercato e prevede, in aggiunta alla ridondanza garantita per i servizi elaborazione e connettività, anche la disponibilità di soluzioni per garantire l'operatività delle risorse in caso di **indisponibilità/inaccessibilità delle sedi operative adibite a Delivery Center**, ivi incluso il Cyber Fusion Center di Napoli. In tal senso, ogni sede è dotata di sistemi di connettività e alimentazione ridondati e ogni servizio viene erogato da almeno 2 sedi distinte come riportato in tabella.

A ulteriore garanzia del livello di sicurezza e di qualità del CS si riportano di

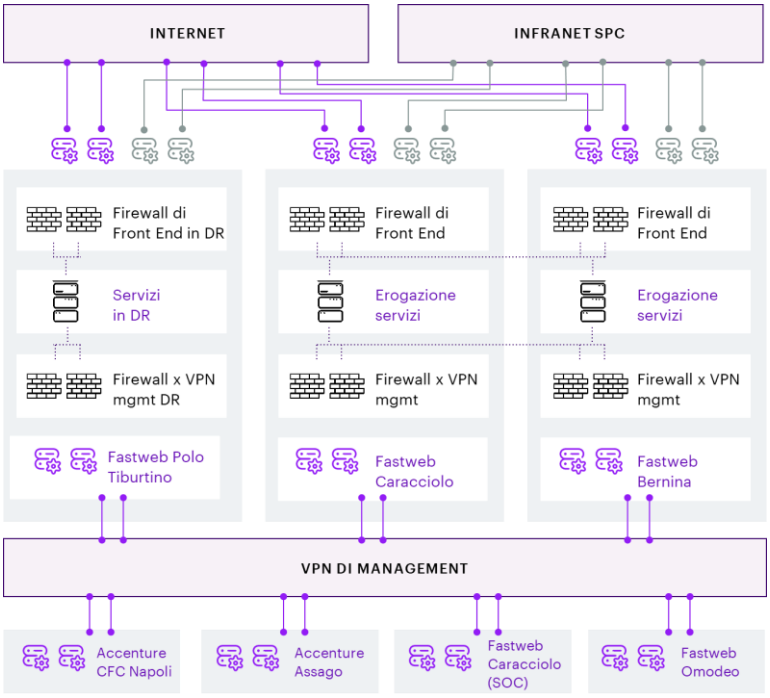


Figura 5 - Architettura tecnica del Centro Servizi

SERVIZIO	SOP	SOS
Help Desk	ACFC-N	AAS
L1.S1 – Security Operation Center	ACFC-N	FWCA
L1.S1 – Next Generation Firewall	FWCA	ACFC-N
L1.S3 – Web Application Firewall	FWCA	ACFC-N
L1.S4 – Gestione continua delle vulnerabilità	FWCA	ACFC-N
L1.S5 – Threat intelligence & vulnerability data feed	ACFC-N	FWO
L1.S6 – Protezione nav. internet e posta elettronica	FWCA	ACFC-N

seguito le relative **certificazioni di riferimento**: ✓CMMI - Capability Maturity Model Integration for System Development (DEV) and Service Management (SVC) ✓ISO 9001- Quality Management System ✓ISO 14001 - Environmental Management System ✓ISO 20000 - IT Service Management ✓ISO 27001 - Information Security Management System ✓ISO 27701 - Privacy Information Management System ✓ISO 22301 Business Continuity Management System ✓ISO 45001 - Occupational Health and Safety Management System ✓Tier IV – Constructed Facility dal Uptime Institute (Data Center Caracciolo) ✓CREST Cyber security incident response (CSIR). Per quanto concerne l'erogazione dei servizi fiduciari, l'architettura è costituita da un layer di front end costituito dal software applicativo da cui le PA possono richiedere i servizi e da un layer di back end che comprende gli HSM e altri sistemi funzionali all'erogazione dei servizi.

L1.S7 – Protezione end point	FWCA	ACFC-N
L1.S8 – Certificati SSL	ACFC-N	FWCA
L1.S9 – Formazione e security awareness	ACFC-N	FWO
L.1.S10 – Gestione identità e accesso utente	ACFC-N	FWCA
L.1.S11 – Firma digitale remota	ACFC-N	FWCA
L1.S12 – Sigillo elettronico	ACFC-N	FWCA
L1.S13 – Timbro elettronico	ACFC-N	FWCA
L1.S14 – Valid. temporale elettronica qualificata	ACFC-N	FWCA
L1.S15 - Servizi specialistici	ACFC-N	FWCA
Legenda: **SOP** *Sede operativa primaria,* **SOS** *Sede operativa secondaria*		

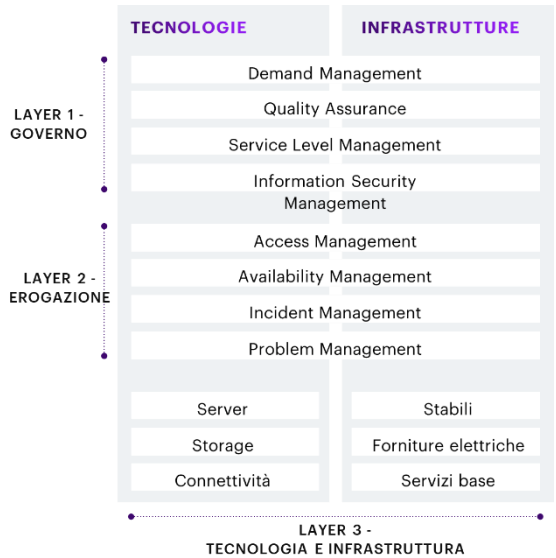
4.2 Modello organizzativo

Il CS viene coordinato da uno specifico Responsabile che opera a livello "Governo AQ" in accordo all'organigramma riportato al §3.1 secondo un modello definito, in accordo ai seguenti criteri: ✓**struttura organizzativa unica** che assume la responsabilità dell'erogazione del servizio per tutte le sedi operative; ✓assegnazione di **responsabilità specifiche centralizzate,** a livello di CS e a diretto riporto del responsabile del CS, in merito alla gestione della sicurezza informatica e della continuità operativa; ✓assegnazione di **responsabilità specifiche distribuite**, a livello di sede operativa, in merito alla sicurezza fisica e alla gestione ambientale ed energetica. Di seguito le principali responsabilità.

Figura	Principali responsabilità
Responsabile del Centro Servizi	✓Gestisce l'erogazione complessiva dei servizi verso le PA ✓Rende disponibili alle strutture operative le risorse umane, tecnologiche ed economiche per l'erogazione dei servizi in funzione delle necessità manifestate dalle PA ✓Governa complessivamente gli aspetti di conformità normativa, gestione dei rischi e tutti gli adempimenti necessari al funzionamento della macchina operativa ✓Costituisce l'interfaccia verso le nostre aziende in RTI
Responsabile di sicurezza informatica e continuità operativa	✓Analizza i rischi relativi ai servizi da erogare e ai dati/informazioni gestite ✓Definisce e manutiene il Piano per la sicurezza delle informazioni e il Piano di continuità operativa ✓Sviluppa e implementa gli strumenti di controllo di efficacia delle soluzioni implementate ✓Pianifica ed esegue test di verifica di efficacia delle stesse soluzioni ✓Rendiconta ai Vertici del RTI in merito allo stato della sicurezza informatica e della continuità operativa ✓Gestisce le certificazioni di sicurezza del CS
Responsabile di sede operativa (include la gestione della sicurezza fisica e ambientale ed energetica)	✓Gestisce le infrastrutture e i servizi logistici pertinenti il sito di riferimento ✓Supervisiona l'operatività delle risorse presenti nel sito ✓Interagisce con i responsabili dei servizi che vengono erogati nel sito ✓Implementa e gestisce gli apprestamenti di sicurezza fisica ✓Implementa e gestisce le necessità in ambito energy management ✓Effettua le valutazioni dei rischi sulle strutture e risorse del sito ✓Rendiconta i vertici del RTI su eventuali criticità pertinenti il sito di riferimento

4.3 Modello di funzionamento

Il modello di funzionamento è stato disegnato in accordo alle migliori pratiche internazionali in ambito IT Service Management ed è basato su processi operativi unici da applicare a tutte le sedi operative e ai singoli servizi garantendone **l'interoperabilità completa**. Il modello si articola su 3 livelli:



- **Layer 1 – Governo del CS**. Include i processi unici comuni a tutte le sedi operative, necessari a garantire la corretta implementazione ed erogazione dei servizi tra i quali si evidenziano: ✓**Demand management** dedicato alla gestione delle richieste delle singole PA che vengono raccolte tramite portale e indirizzate sui singoli servizi in modo automatizzato per le richieste standard e a seguito di analisi specialistica per eventuali richieste a maggiore complessità; ✓**Quality assurance** finalizzato a monitorare nel continuo il rispetto dei più elevati standard di erogazione dei servizi nel tempo e ad indirizzare eventuali azioni di rafforzamento che si dovessero rendere necessarie; ✓**Service level management** finalizzato alla gestione dei livelli di servizio al fine di garantirne un monitoraggio e una rendicontazione continuativa, nonché ad abilitare l'esecuzione di eventuali azioni di miglioramento che si rendessero necessarie; ✓**Information security management**, gestito dal responsabile della sicurezza informatica, per garantire la corretta implementazione dello Information Security Management System (ISMS).
- **Layer 2 – Erogazione dei servizi**. Include i processi necessari a garantire l'erogazione sicura e continuativa dei servizi in modalità univoca e sinergica tra tutte le sedi operative tra i quali si evidenziano: ✓**Access management** per poter garantire l'accesso ai servizi informativi agli utenti delle PA in modalità sicura; ✓**Availability management** finalizzato a garantire la continuità dell'erogazione dei servizi secondo gli standard contrattualizzati; ✓**Incident management** finalizzato alla gestione degli incidenti che possono impattare le dimensioni di riservatezza, integrità dei dati e di disponibilità dei servizi; ✓**Problem management** per l'analisi di eventuali problematiche che si dovessero riscontrare nell'erogazione e l'identificazione delle relative iniziative di adeguamento. In tale ambito sono incluse anche le attività di knowledge transfer verso le PA necessarie a garantirne l'autonomia operative.
- **Layer 3 – Tecnologia e infrastruttura**. Include tutte le componenti fisiche di natura **informatica e infrastrutturale** necessarie all'erogazione dei servizi. Per i Data Center include le dotazioni delle sale adibite a ospitare i sistemi operativi, di connettività e di storage; per i Delivery Center include tutti gli asset per

l'accesso delle risorse nonché gli apprestamenti di sicurezza fisica e per la sicurezza sul lavoro del personale. È gestito dal responsabile di sito tramite presidi locali necessari a garantire un costante adeguamento e manutenzione degli stessi.

4.4 I requisiti di sicurezza delle informazioni

Il CS è dotato di misure di sicurezza delle informazioni atte alla protezione di dati, informazioni e servizi erogati alle PA e, in particolare, a garantire: ✓la **riservatezza** dei dati e delle informazioni gestite permettendo l'accesso solo a chi è autorizzato; ✓l'**Integrità** dei dati e delle informazioni gestite impedendo modifiche non autorizzate o manomissioni; ✓la **Disponibilità** dei servizi erogati grazie a soluzioni di protezione e ridondanza dei dati e delle infrastrutture. La soluzione proposta prevede l'implementazione, per le sedi operative, di contromisure di sicurezza logica secondo il principio di "difesa in profondità" e "zero trust" strutturato secondo livelli che comprendono più strati di protezione, in conformità dello **standard ISO 27001**. Viene quindi definito il **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** ovvero lo strumento che permette di controllare in modo sistematico e continuativo i processi che riguardano la sicurezza di tutto il patrimonio informativo coinvolto nell'erogazione dei servizi.

Tra le misure di sicurezza implementate in accordo a tale standard si evidenziano: ✓controllo degli accessi per utenti finali, utenti interni e personale con privilegi amministrativi (cd access control) ✓crittografia per la gestione dei segreti aziendali e delle chiavi di cifratura ✓protezione delle postazioni di lavoro tramite antivirus, EDR, Data Loss Prevention, e-mail security ✓protezione dei server tramite antivirus, EDR, FIM ✓protezione delle basi dati tramite soluzioni di mascheramento e di controllo delle operazioni ✓protezione da minacce cyber tramite security monitoring e della threat intelligence ✓protezione delle applicazioni tramite controllo del codice sorgente e la protezione delle applicazioni esposte su internet ✓protezione della rete tramite sistemi perimetrali, di monitoraggio del traffico e di segregazione / segmentazione ✓processi continuativi di vulnerability management, di patching e l'applicazione di standard di hardening.

Il CS è dotato di un proprio **Piano per la sicurezza delle informazioni** redatto secondo i principi del Client Data Protection Program, sviluppato e adottato da Accenture per garantire la tutela delle informazioni dei Clienti e certificato ISO27001. Il Piano è soggetto a revisione continua e ad approvazione da parte del RTI.

4.5 I requisiti di sicurezza fisica

Tutte le sedi operative sono dotate di soluzioni volte alla protezione nei confronti di danni dovuti ad eventi esterni (incendi, inondazioni, esplosioni, disastri naturali) o causati dall'uomo tramite accessi non autorizzati mirati a danneggiare sistemi e dati (manomissione e furto delle informazioni e degli apparati IT, impedimento allo svolgimento dei servizi e dei processi IT, manomissioni e interruzioni delle attività). Per ogni sede operativa è previsto un **piano per la sicurezza fisica** e ambientale e l'assegnazione della responsabilità della sicurezza fisica al responsabile di sede.

Le contromisure di sicurezza fisica sono strutturate secondo **livelli di protezione progressivi** e includono: ✓Sistemi di protezione fisica perimetrale tramite barriere fisiche arricchite da sensori di rilevamento presenze e sensori anti-intrusione; ✓Sistemi di controllo accessi tramite barriere di protezione (bussole o tornelli) e sistemi di autenticazione a due fattori (inclusi elementi di biometria); ✓Sistemi di videosorveglianza arricchiti da soluzioni che si basano sull'AI per identificare anomalie in corrispondenza degli accessi critici; ✓Sala di monitoraggio operativa 24x7 in grado di gestire eventi allarmi e di allertare servizi di ronda/vigilanza a chiamata; ✓Presidio fisico tramite personale di presidio 24x7 per gli accessi alle aree ad alta criticità; ✓Collegamento con le forze dell'ordine per gestire interventi di emergenza; ✓Integrazione con il servizio Security Operation Center in grado di collegare anomalie sui sistemi di accesso fisico e logico.

Con particolare riferimento agli stabili adibiti a **Data Center** sono previste misure di sicurezza specifiche, stante la criticità dei dati e dei servizi gestiti. Queste sedi sono dotate, tra le altre misure, di impianti e sistemi di sicurezza controllati e monitorati 24x7 da personale Fastweb specializzato e certificato e sono gestiti dal sistema di supervisione GEMSS (GEneral Manager for Security Systems). Sono installati sistemi di videosorveglianza ad alta definizione e ad alte prestazioni con funzionalità di Motion Detection e, in particolare in sala dati, sono presenti telecamere dedicate ad ogni fila di rack (43 Telecamere, in media 1 cam ogni 10mq). Sono installate sbarre o cancelli di protezione azionati dalla postazione di guardiania per regolamentare l'accesso dei veicoli, laddove ritenuto necessario.

Tutte le aree del Data Center, sala dati e locali esterni, sono protette da un sistema di rilevazione fumi e, per un maggior grado di sicurezza, è presente anche un sistema di rivelazione fumi a campionamento d'aria HSSD nella sala dati e nei locali UPS e batterie. Tutte le aree del DC sono protette con un sistema di spegnimento automatico a gas tipo IG-01 (Argon), oltre che da sensori di rilevamento del calore, sensori di fumo, sistema di estinzione incendi, estintori portatili. La protezione dal fuoco è effettuata tramite compartimentazione e isolamento dei locali impianti. La resistenza è garantita fino a 120 minuti (REI 120 / F 120) tramite utilizzo di materiali da costruzione ignifughi e autoestinguenti.

Il processo di accesso al Data Center prevede l'adozione di procedure di autenticazione via web, riconoscimento puntuale, abilitazione e consegna di un badge e successivamente l'accesso tramite una bussola classificata "antirapina".

È presente un sistema ridondato di rilevamento dello spandimento dei liquidi a protezione della sala dati e dei locali con trasformatori, UPS e batterie, e centrali idrauliche. Gli allarmi di perdite provocano la chiusura delle valvole di linea e InRow del tratto interessato.

4.6 Continuità Operativa

Il CS è disegnato in modo tale da poter erogare i servizi con requisiti di continuità operativa definiti in accordo alle indicazioni definite dallo standard ISO 22031. Tali requisiti sono implementati per garantire la continuità: ✓**dei servizi informatici** secondo l'architettura dei Data Center di Fastweb descritta in precedenza che prevede 2 siti di erogazione (Caracciolo e Bernina) e 1 sito di Disaster Recovery (Polo Tiburtino) e ✓**dei servizi erogati dai centri di delivery** di Accenture e di Fastweb tramite la ridondanza di tutti i servizi di connettività e di alimentazione e la possibilità di spostare l'operatività presso altri centri di delivery. Questo consente la **copertura completa degli scenari di rischio** definiti dalle più stringenti normative applicabili in Italia, tra cui: ✓Indisponibilità dei sistemi e dei servizi informatici (erogati dai Data Center); ✓Indisponibilità della sede operativa di riferimento per l'erogazione di un servizio; ✓Indisponibilità del personale; ✓Indisponibilità dei servizi; ✓infrastrutturali (tlc ed energia); ✓Indisponibilità di dati e della documentazione essenziale; ✓Indisponibilità delle terze parti coinvolte.

Le soluzioni previste garantiscono requisiti di ripristino elevati che prevedono un **RTO e un RPO prossimi allo 0** per eventi che coinvolgono i Data Center e/o i Delivery Center (es. incendio/allagamento/terremoto). Solo nel caso in cui si rendesse necessario il ricorso al sito di Disaster Recovery e alla relativa terza copia di dati (indisponibilità contemporanea di entrambi i Data Center di Milano) è previsto un RTO di 4 ore e un RPO prossimo allo 0.

Con riferimento **ai servizi informatici**, nell'ambito dell'architettura sopra presentata, i Data Center sono serviti da 2 reti pubbliche di distribuzione e sottostazioni

separate ciascuna delle quali può tenere il pieno carico del sito. Sono presenti 2 gruppi di 2 x 800 KVA UPS con autonomia a pieno carico di 15 minuti (ogni gruppo ha 2 linee di alimentazione separate (A e B) e un sistema aggiuntivo di Inertial Water Storage da 26 m^3 e generatori di standby costituiti da 2 Gruppi Elettrogeni per una potenza complessiva di 4,2 MW e 2 serbatoi addizionali e separati da 16.000l.

La soluzione è abilitata da specifiche dotazioni e configurazioni che includono: ✓Link di interconnessione tra i datacenter in fibra ottica di tipo L2 e percorsi geografici affatto diversificati che rendono possibili allineamenti sincroni delle SAN ✓Adeguato dimensionamento della banda di rete tra i datacenter e basse latenze ✓Opportune apparecchiature di rete e relative configurazioni di WAN geografiche ✓Tecniche di stretch clustering che consentono di estendere il concetto di cluster di risorse su scala geografica ✓Due nodi SAN storage con replica sincrona per la disponibilità continua dei dati su entrambi i siti di erogazione in BC ✓Suite di virtualizzazione VMWare in grado di garantire ambienti speculari sui due siti e potenza elaborativa resa disponibile in modo immediato e automatico.

In **aggiunta** evidenziamo l'applicazione di soluzioni per **isolare le seconde e terze copie** dei dati da eventuali compromissioni delle copie primarie a seguito di attacco informatico (es. ransomware). La disponibilità di un back-up basato su versioning continuativo consente di ripristinare i dati immediatamente, rendendo disponibili le ultime versioni prima dell'attacco identificato.

In riferimento **ai servizi erogati dai centri di delivery**, sono previste soluzioni atte a garantire l'erogazione dei servizi tramite: ✓Formazione di risorse di back up e disponibilità di unità operative gemelle presso altre sedi operative ✓Possibilità di erogare i servizi in modalità "smart working" in situazione di emergenza in conformità alla normativa vigente ✓Ridondanza delle infrastrutture di connettività dei siti di Delivery relativamente alle telecomunicazioni (doppie connessioni alla connettività esterna) e all'approvvigionamento energetico (doppie cabine di connessione al provider di energia) ✓Virtualizzazione della documentazione e sua gestione secondo le configurazioni di continuità dei Data Center ✓Clausole contrattuali di salvaguardia e sulle terze parti e ricorso altri fornitori pre-identificati.

Tutte le soluzioni sono formalizzate all'interno del **Piano di Continuità Operativa** del CS, sono soggette a revisione costante e ad attività di test periodico con cadenza almeno annuale. A garanzia della responsabilizzazione su tale tematica è prevista la nomina formale di un Responsabile della Continuità Operativa cui sono assegnate risorse economiche adeguate ad adempiere ai propri compiti.

4.7 Impatto ambientale ed energetico

Tutte le sedi operative (Data Center e Delivery Center) sono dotate di soluzioni tecnologiche che consentono una **drastica riduzione dell'impatto ambientale** attraverso l'abbattimento delle emissioni di CO_2 e la minimizzazione dei consumi energetici, secondo un percorso iniziato da tempo verso la Green Company da tutti i componenti del RTI, sia nella erogazione dei servizi ai clienti che nella gestione di procedure interne atte a migliorare gli impatti sull'ambiente (uso carta "ecolabel", uso di energia proveniente da fonti rinnovabili, ecc.).

In particolare, il **Data Center Caracciolo** è stato progettato adottando criteri orientati alla sostenibilità ambientale ("green building"), come dimostrato dalla certificazione **LEED Platinum** dell'edificio. La sede è provvista di un impianto fotovoltaico per l'auto generazione di energia elettrica e di un sistema di climatizzazione di ultima generazione, permettendo in questo modo di ridurre i consumi energetici. Fastweb ha ottenuto nel 2013 la certificazione ISO 14001, rinnovata nel 2016 con la **certificazione ISO 14001:2015**, confermando il suo impegno nel mantenere attivo un sistema di gestione ambientale secondo i requisiti della norma per garantire il controllo, la riduzione e la prevenzione degli impatti ambientali, reali e potenziali, connessi alla propria attività. Tra le soluzioni tecnologiche adottate per la **riduzione delle emissioni di CO_2 e la minimizzazione dei consumi energetici** si evidenziano: ✓Impianti di illuminazione progettati e realizzati con tecnologie e materiali a basso consumo energetico e con dissipazione di calore prossima allo zero ✓Dispositivi di monitoraggio e attuatori che consentono il controllo e lo spegnimento automatico dei dispositivi non necessari all'operatività ✓PDU (Power Distribution Unit) intelligenti ad alta efficienza che minimizzano gli overload e quindi la dissipazione di calore ✓Alimentatori degli apparati IT a singola fase e dotati di regolatori di tensione a bassa dispersione ✓Sistemi di raffreddamento dei rack a elevato rendimento ✓Sistemi UPS ad alto rendimento con fattori di potenza estremamente elevati e che minimizzano le perdite di potenza attiva ✓Server a elevata densità ad alte prestazioni per ridurre il numero di macchine fisiche necessarie a parità di capacità computazionale ✓Meccanismi di CPU Scaling per gestire la potenza elaborativa in funzione del carico applicativo e permettere la modulazione del consumo energetico delle CPU ✓Sistema DCIM (Data Center Infrastructure Management) che autoregola i valori di potenza e raffreddamento in tempo reale ✓Sistema per ottimizzare il funzionamento dei gruppi frigo.

Le soluzioni definite consentono di attestare i Data Center su un **valore di PUE (Power Usage Effectiveness) medio pari 1,55** inferiore al valore di 1,6 previsto come obiettivo dalle "Linee Guida per il Consolidamento dei Datacenter della Pubblica Amministrazione" di AgID. In particolare, il Data Center Caracciolo rappresenta l'**eccellenza nello scenario nazionale** con un valore di PUE pari 1,25.

4.8 Descrizione del servizio di Help Desk

Il servizio di Help Desk erogato dal CS ha l'obiettivo di fornire un unico punto di contatto per le PA tramite l'adozione di sistemi multicanale che abilitano l'accesso degli utenti secondo le più moderne **logiche di multicanalità integrata**. In tal senso, vengono resi disponibili una grande varietà di canali di accesso che operano in modalità integrata, rendendo possibile per gli operatori passare da uno strumento ad un altro per garantire la migliore esperienza utente. La soluzione proposta si basa su un'istanza **ServiceNow** installata all'interno del CS. Metteremo a disposizione **SPARK** (ServiceNow Powered by Accenture Resources & Knowledge), toolkit definito da Accenture che abilita su ServiceNow un'implementazione rapida dei processi ITIL4 con numerosi modelli e acceleratori pre-compilati.

L'Help Desk, erogato secondo gli orari ed i livelli di servizio previsti nella documentazione di gara, garantisce quindi accessibilità e fruibilità con molteplici modalità quali: ✓utilizzo del **numero verde unico**, appoggiato su di una infrastruttura VOIP ad alta affidabilità; ✓**interfaccia web** e **mobile** che operano in modalità integrata al portale disponibile alle PA; ✓**Chat / SMS / Social** che abilitano forme di contatto alternative alle tradizionali in base alle differenti esigenze delle PA; ✓**e-mail** per la gestione delle comunicazioni scritte con le PA. A titolo esemplificativo, l'ingaggio da parte della PA può essere iniziato tramite contatto telefonico, proseguire con un una chat ed essere rendicontato tramite interfaccia web o mobile. L'Help Desk costituisce, inoltre, il principale punto di ingaggio del Security Operation Center in modalità 24x7 per tutte le problematiche relative alla gestione di eventi / incidenti di sicurezza.

Tra i principali elementi innovativi introdotti si evidenziano: ✓Applicazione di tecnologie basate sull'**AI** per poter indirizzare al meglio i ticket e proporre all'operatore soluzioni alle necessità della PA. ✓Adozione di **soluzioni automatizzate (BOT)** per la risoluzione di casi standard e a bassa complessità. ✓Costante **misura del livello di soddisfazione** della PA così da indirizzare al meglio eventuali criticità e problematiche. ✓**Accesso facilitato** e comune ai quesiti provenienti da tutti i canali disponibili alle PA (web e mobile).

Di particolare importanza è inoltre la **piattaforma di Knowledge Management integrata in ServiceNow c**he consente di gestire e rendere fruibile la base di conoscenza condivisa con il Portale (cfr. §16) e che consente di accedere ai dettagli operativi dei servizi erogati e delle tecnologie di supporto tramite la costituzione di un patrimonio informativo specifico. La piattaforma consente di accedere alla Knowledge Base per cercare le informazioni, filtrando i contenuti per tipologia e ordinando per aggiornamento più recente, per numero di visualizzazioni o per il livello di valutazione definito dagli utenti. L'applicazione consente agli utenti di iscriversi a specifici Knowledge articles e di ricevere notifiche su nuovi articoli e revisioni o commenti. Gli utenti possono commentare i Knowledge articles in vari modi: ✓segnalare un articolo come errato o inappropriato; ✓fornire una valutazione sull'articolo; ✓indicare l'articolo come utile o non utile; ✓visualizzare i commenti, aggiungere un nuovo commento o rispondere ai commenti esistenti.

Il servizio di Help Desk è governato da un **Help Desk Manager** che ha la responsabilità complessiva dell'erogazione del servizio e si occupa del monitoraggio continuativo del livello di servizio, ne esegue la rendicontazione e definisce e implementa le eventuali azioni di miglioramento che si dovessero rendere necessarie. Dal punto di vista operativo, il servizio viene erogato tramite: ✓**una struttura di 1° livello** costituita da team composti da analisti e coordinati da supervisori esperti. Questo livello gestisce le richieste standard secondo playbook predefiniti (stimate intorno allo 80% dei casi totali); ✓**una struttura di 2° livello** costituta da specialisti dei singoli servizi, distinti per tipologia di PA servita, che si occupano di gestire i casi a maggiore complessità o comunque che esulano dalle richieste standard (stimati intorno al 20% dei casi totali). È inoltre prevista la figura del **Customer Assistant** ovvero di risorse dedicate a seguire PA che hanno attivato molteplici servizi. Il Personal Assistant è una risorsa dotata di elevata esperienza che consente di facilitare la presa in carico e l'evasione delle richieste di tali PA.

I processi operativi del servizio sono supportati da uno strumento di **case management** avanzato che sarà opportunamente implementato per gestire le casistiche di eventi legate a tutti i servizi oggetto di erogazione.

Il servizio prevede un'organizzazione basata su turnistica frutto di un **processo continuo di analisi e pianificazione**, che tiene conto delle **statistiche** acquisite quotidianamente sulle chiamate ricevute per tipologia e durata. Il **dimensionamento è quindi flessibile e adattativo**, in conseguenza dei volumi di traffico e del numero di ticket stimato e sarà progettato sulla base di pregresse esperienze consolidate e utilizzando strumenti di analisi in base a tutte le variabili di servizio a disposizione (volumi, tempi di risposta/intervento, incremento di attività su base oraria, SLA, etc.) si calcola con precisione il numero di risorse necessarie.

Elemento fondamentale del servizio sono le risorse umane allocate sulle attività che sono oggetto di **interventi di formazione continuativi** finalizzati a: ✓Garantire la conoscenza dei servizi erogati, tramite affiancamento alle risorse che si occupano dell'erogazione dei servizi affinché possano avere esperienza diretta del contenuto degli stessi e delle problematiche che si possono riscontrare, ✓Gestire la relazione con le PA. Si procederà quindi ad interventi di formazione specifici per poter interloquire in modalità efficace con le PA e poter dare un riscontro corretto e tempestivo alle relative esigenze; ✓Indirizzare problemi complessi in funzione della relativa esperienza lavorativa. Sono previsti **meccanismi di crescita professionale** che consentono di assumere progressivamente un ruolo di riferimento per la gestione delle problematiche a maggiore complessità.

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

5.1 Soluzione proposta

Il modello **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di 'Security Operations Center (SOC) nel dominio: ✓"Threat Monitoring" e "Threat Hunting", riconducibili alla Funzione NIST "Detect" ✓"Threat Response" e "Active Defence", riconducibili alla Funzione NIST "Respond & Recover".

La ventennale esperienza di Accenture, unitamente a quella di Fastweb nell'ambito della PA, ha permesso di consolidare e far evolvere un modello di servizio ponendo a fattor comune esperienze analoghe nella realizzazione ed erogazione di servizi di Security Operation Center per istituzioni governative nazionali ed internazionali. Si è giunti alla definizione ed ingegnerizzazione di un modello di "**Next Generation Security Operation Center (NG-SOC)**" basato sulla piattaforma tecnologica di Accenture denominata "**Advanced Security Monitoring & Detection (ASMD)**", la quale sfrutta un'architettura modulare flessibile e multi-cliente, che permette di scalare a seconda del numero e livello di integrazione delle amministrazioni in ambito di gara. La soluzione ASMD di Accenture abilita ad un servizio di Managed Detection & Response (MDR), per offrire alle Amministrazioni aderenti servizi gestiti SIEM **segregati e integrati** con la piattaforma centralizzata SOAR, nel seguito descritte. La soluzione opera in modalità 24x7x365 e viene erogata dai *SOC* di Napoli e Milano, operanti all'interno dei Centri Servizi in ambito di gara (cfr. §4). Accenture ha selezionato e integrato nella piattaforma *ASMD* la tecnologia **Splunk** per la parte di *"Security Information & Event Management (SIEM)"* e **PaloAlto Cortex XSOAR** per la parte di "*Security Orchestration, Automation & Response (SOAR)"*, entrambi leader di mercato secondo fonti affermate di analisti di settore quali Gartner e Forrester e partner decennali a livello globale delle Aziende del RTI.

La natura del *Security Operations Center* proposto (SOC) fa sì che **assuma un ruolo centrale** nella proposta del RTI per **tutti i servizi, inclusa la gestione delle funzionalità di sicurezza afferenti alla rete, ai sistemi, ai dati e alle applicazioni, *On-Site* e non**, delle PA. Questo include la possibilità di estendere il monitoraggio ad eventi e specifici casi d'uso provenienti da sorgenti non squisitamente IT (si pensi ad esempio alla possibilità di importare i log prodotti dai dispositivi IoT/OT connessi nelle Smart-City per individuare minacce in grado di minare la sicurezza fisica dei cittadini). Attraverso un continuo **scambio informativo bidirezionale**, in particolare con i Servizi da L1.S2 a L1.S7 e L1.S10, **il SOC aumenta la propria efficacia e accuratezza** tramite un processo automatico di **arricchimento** degli eventi di sicurezza ingegnerizzato dal RTI e basato su un processo di *datamining, ML e deep learning;* sfruttando le funzionalità offerte dalle soluzioni tecnologiche in uso presso il SOC per lo sviluppo di modelli di identificazione delle anomalie e clustering dinamico per gli use case di detection, incrementa la produttività della gestione degli incidenti mediante ✓attribuzione automatica della ownership ✓sviluppo assistito di playbook di risposta ✓inferenza di azioni di risposta applicabili. Il servizio proposto di SOC ha l'obiettivo di **individuare nel minor tempo possibile** gli attacchi ai danni dell'Integrità, Confidenzialità e/o Disponibilità del patrimonio informativo delle Amministrazioni siano esse Locali o Centrali. A fronte della rilevazione e della convalida dell'incidente, **viene innescato il processo di Incident Management supportato dalle informazioni di dettaglio fornite dal Servizio SOC, contestualizzate e arricchite** da ulteriori ambiti oggetto della presente proposta quali ad esempio il 'Servizio di Gestione continua delle Vulnerabilità di Sicurezza' - per assegnare in fase di Triage la corretta priorità all'incidente - e il 'Servizio di Threat Intelligence & Vulnerability Data Feed' - per correlare informazioni sugli Indicatori di Compromissione (IOC) e Tactics Techniques and Procedure (TTP) del MITRE ATT&CK relative al potenziale Threat Actor. Questo permette di offrire alla Amministrazioni servizi avanzati di **Monitoraggio di Sicurezza in "real-time"** per identificare le minacce in modalità proattiva e automatizzata, comprimere i tempi di analisi e presa in carico degli incidenti, incrementare la capacità di

individuazione e rimozione dei falsi positivi, e **attivare in maniera tempestiva il processo di 'Risposta agli attacchi e agli incidenti'** supportato dalle informazioni di dettaglio necessarie all'efficace contenimento ed eradicazione dell'incidente stesso, rendendo la risposta agli eventi di sicurezza molto più veloce rispetto ai servizi SOC tradizionali, con un incremento di efficienza misurato di circa il 60%. L'efficacia e la qualità del servizio sono frutto dell'esperienza maturata dai nostri pluricertificati CyberSecurity Analyst in due decadi di servizio nel settore pubblico e privato, nella costante gestione operativa end-2-end della piattaforma ASMD ivi inclusi gli ambienti del SIEM segregati e integrati con la soluzione di orchestrazione e automazione centralizzata (SOAR), e su un insieme di oltre cinquanta procedure consolidate che sono evolute nel tempo raggiungendo oggi un **livello di maturità riconosciuto** non solo dai clienti ma anche dagli analisti di mercato come nei report *"Forrester Wave European Managed Security Services Providers 2020"* e "*IDC Marketscape Worldwide Managed Security Services 2020*".

BEST PRACTICE - ASMD - La piattaforma ASMD attualmente in Italia è in uso presso oltre 20 clienti, portando **standardizzazione** nella gestione degli incidenti di Sicurezza tramite i propri playbook e **riducendo** la manualità delle operazioni ripetitive, con conseguente maggiore spazio operativo per attività a maggiore valore aggiunto (più approfondita analisi delle cause e miglioramento nella caccia delle minacce). L'analisi dei KPI interni ha evidenziato un **notevole abbassamento nei tempi di risposta degli incidenti di sicurezza.**

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: circa 30, tra cui Roma Capitale e SACE

Private: Intesa Sanpaolo, NEXI, A2A, ISAB, Poste Italiane e Poste Mobile, primario operatore finanziario

Descrizione di un caso di successo - Intesa Sanpaolo →Esigenza - Team di presidio in ambito cybersecurity che eroghi servizi di SOC insieme al team di cybersecurity del cliente **→Soluzione** - Accenture ha erogato servizi SOC 24 x7, tramite un team MSS presso il cliente e ricorrendo al Cyber Fusion Center per servizi extra orario di lavoro. Gestione degli incidenti, malware, analisi di phishing e spam, valutazione delle vulnerabilità ed esecuzione di test di penetrazione, early warning, caccia alle minacce e supporto di Digital Forensics **→Benefici** - Efficace gestione della cybersecurity e contenimento del rischio a livelli richiesti dal cliente.

5.1.1 Funzioni Offerte

Il servizio prevede: un livello di **Interfaccia** utile all'interazione con il servizio, un livello di **Erogazione** in cui sono espletate le funzioni principali del servizio, un livello di **Automazione** (intelligent layer) che aggiunge funzioni avanzate, un livello **Interazioni** per le relazioni con gli altri servizi. I livelli comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative**, descritte di seguito:

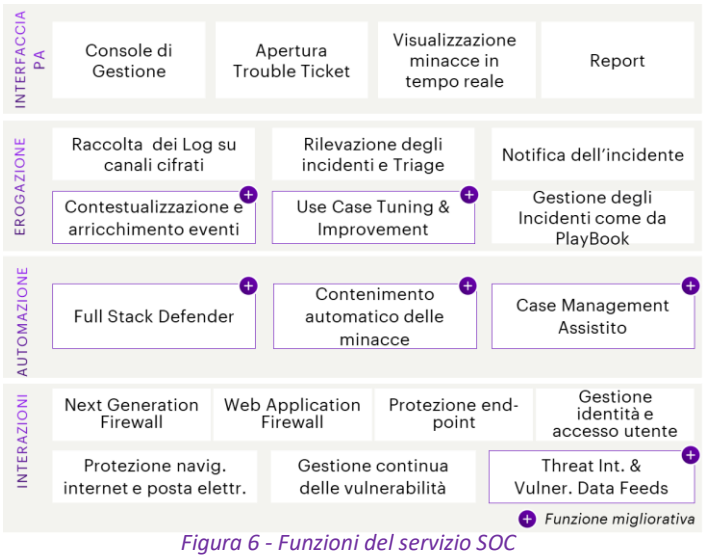


Figura 6 - Funzioni del servizio SOC

- **Contestualizzazione e arricchimento eventi:** Tutti gli eventi di sicurezza raccolti dal servizio SOC sono correlati e arricchiti con le informazioni fornite dagli altri servizi integrati attivi sulla singola PA, in modo da calare i dati raccolti e gli alert identificati sullo specifico contesto e velocizzare le attività degli analisti.
- **Use case Tuning & Improvement:** L'esperienza maturata sui casi/incidenti gestiti sulle singole PA viene utilizzata per migliorare continuamente la libreria di use case sviluppati dal servizio SOC, minimizzando il numero di falsi positivi, migliorando l'efficienza dei team di analisti ed eventualmente inferendo soglie di alert o use case aggiuntivi rilevanti tramite ML/deep learning.
- **Full Stack Defender:** Il nostro modello NG-SOC permette di superare i limiti di efficacia nella detection delle moderne soluzioni SIEM e SOAR, offrendo un controllo real-time dello stato di sicurezza delle amministrazioni, e correlando le informazioni di monitoraggio con interrogazioni dirette ai dati delle altre soluzioni tecnologiche in ambito di gara per sfruttare il pieno potenziale di visibilità sugli asset su cui sono installati. Mette inoltre a disposizione playbook sviluppati per agevolare le interrogazioni degli analisti sui tool e dedicare il tempo di analisi sulle attività di valore.
- **Contenimento automatico delle minacce:** Il servizio SOAR implementato dal SOC è integrato con le soluzioni di sicurezza in ambito di gara in modo da offrire una risposta automatica efficace di primo intervento sulle piattaforme tecnologiche relative ai servizi attivi sulle singole PA, permettendo di ridurre sensibilmente i tempi di intervento.
- **Case Management Assistito:** Il servizio SOC utilizza le più moderne tecnologie SOAR per supportare gli analisti nella gestione degli incidenti e analisi degli eventi di sicurezza rilevanti, tramite l'implementazione di playbook di automazione che permettono di arricchire automaticamente le informazioni collezionate con le fonti di Intelligence oppure assegnare la priorità ai case aperti.
- **Threat Intelligence & Vulnerability Data feed:** Le soluzioni di Threat Intelligence e Vulnerability Data feed sono utilizzate internamente dal SOC come fonte di arricchimento degli eventi di sicurezza raccolti in relazione al contesto del panorama delle minacce globale di interesse per le PA.

5.1.2 Architettura tecnologica

La piattaforma ASMD proposta prevede l'integrazione di una componente SIEM - segregata per la specifica PA e basata su tecnologia Splunk - con la piattaforma SOAR centralizzata del RTI basata su tecnologia PaloAlto Cortex XSOAR.

La soluzione **Splunk** ci ha permesso di superare i limiti delle soluzioni SIEM convenzionali, tramite un **deploy scalabile** che rende

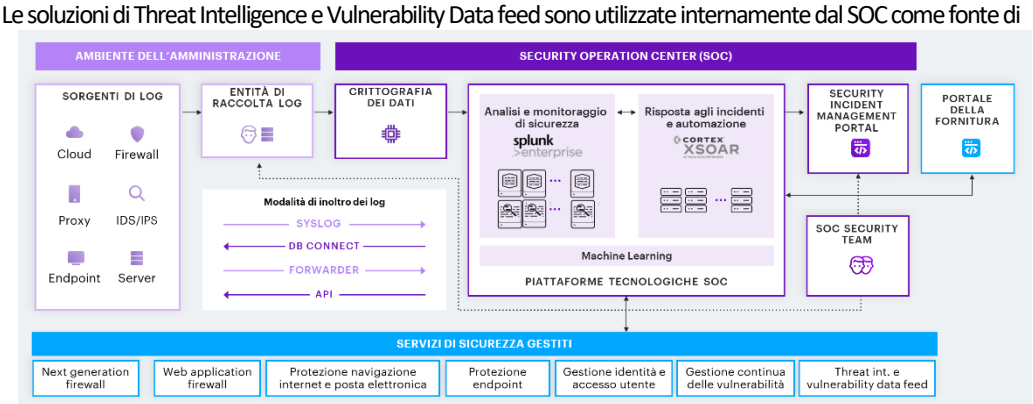


Figura 7 - Architettura tecnologica SOC

possibile l'integrazione con ogni tipo di sorgente di dati senza alcuna limitazione di schema. La piattaforma garantisce **piena visibilità sugli eventi di sicurezza**, riducendo sensibilmente il tempo di identificazione delle minacce, e offrendo non solo funzionalità di ricerca, correlazione dei dati e creazione di cruscotti, ma anche strumenti avanzati di analytics, ML e analisi comportamentale. L'utilizzo di un **approccio basato sul rischio** e il supporto nativo alle tecnologie in ambito di gara, permette inoltre di prioritizzare gli interventi e minimizzare i tempi di investigazione in caso di incidente.

Come soluzione SOAR è stato identificato **PaloAlto Cortex XSOAR:** l'utilizzo in ASDM ha permesso un **abbattimento del tempo di risposta agli incidenti**, riducendo sensibilmente il volume degli allarmi generati dagli strumenti di sicurezza. Cortex XSOAR ci ha permesso di integrare nel servizio funzionalità avanzate di deep learning per fornire raccomandazioni, accelerare lo sviluppo di playbook e migliorare i modelli di risposta sulla base di incidenti e azioni precedenti.

La soluzione tecnologica proposta mira a ridurre sensibilmente il tempo speso dagli analisti su task operativi ricorrenti, in modo da soffermarsi su **attività a maggior valore** quali approfondimento delle analisi, ricerca proattiva e miglioramento continuo. Il disegno proposto permette inoltre di segregare i contesti delle singole PA, e di creare viste personalizzate per ognuna di esse, in modo da avere sempre chiaro il livello di sicurezza dei singoli asset integrati in relazioni a tutti i servizi di sicurezza attivi. L'integrazione con i servizi attivi sulle PA permette inoltre di correlare e arricchire le informazioni raccolte dal SIEM, permettendo di offrire una *detection* olistica dell'ecosistema delle singole PA.

Nel corso della fornitura per l'erogazione dei servizi, al fine di indirizzare le diverse esigenze di cluster di PA diverse, in ottica multivendor, potremo utilizzare piattaforme tecnologiche diverse da quella descritta o anche una combinazione di più prodotti di mercato. Questa considerazione vale per tutti i servizi di fornitura.

5.1.3 Next Generation SOC (NG-SOC): caratteristiche tecnologiche e prestazionali migliorative e innovative

Il servizio NG-SOC nasce con l'obiettivo di rilevare e interrompere il processo di attacco il prima possibile, in modo da minimizzare gli impatti sulle singole PA. Con il suo approccio innovativo, basato sulla forte coesione tra strumenti di monitoraggio avanzati e meccanismi di automazione delle analisi, nonché su un modello pienamente gestito (Managed Security Services) che libera le PA dagli oneri di gestione delle infrastrutture a supporto. Il servizio di *NG-SOC* basato sulla piattaforma *Advanced Security Monitoring & Detection (ASMD)* è stato ingegnerizzato da Accenture avendo come obiettivo principale l'abbattimento del lasso di tempo che intercorre tra l'ingestione da parte del *SIEM* dei *log* contenenti i dati grezzi dell'attacco, e l'identificazione dell'incidente da parte del team preposto. **Si raggiunge quindi la minimizzazione degli impatti sulle singole Amministrazioni** attraverso un processo accelerato e consapevole di risposta all'incidente. Per conseguire tale obiettivo è stata posta particolare attenzione all'integrazione nativa tra soluzione SIEM Splunk e SOAR PaloAlto con fonti di Threat Intelligence e i servizi di sicurezza in ambito delle PA. L'arricchimento automatico ottenuto tramite la standardizzazione da parte del RTI di feed normalizzati fornisce alle PA piena visibilità sullo stato di sicurezza dei sistemi monitorati, sia dal punto di vista degli attaccanti sia per quanto concerne l'impatto sull'organizzazione stessa. Il modello si fonda inoltre su un paradigma di miglioramento continuo che, a partire dalle evidenze raccolte dalla funzione di controllo qualità (cfr. § 5.3.2), identifica e implementa le azioni migliorative applicabili al servizio per fornire sempre un **livello di sicurezza competitivo e rilevante** rispetto al contesto delle minacce cyber a livello globale.

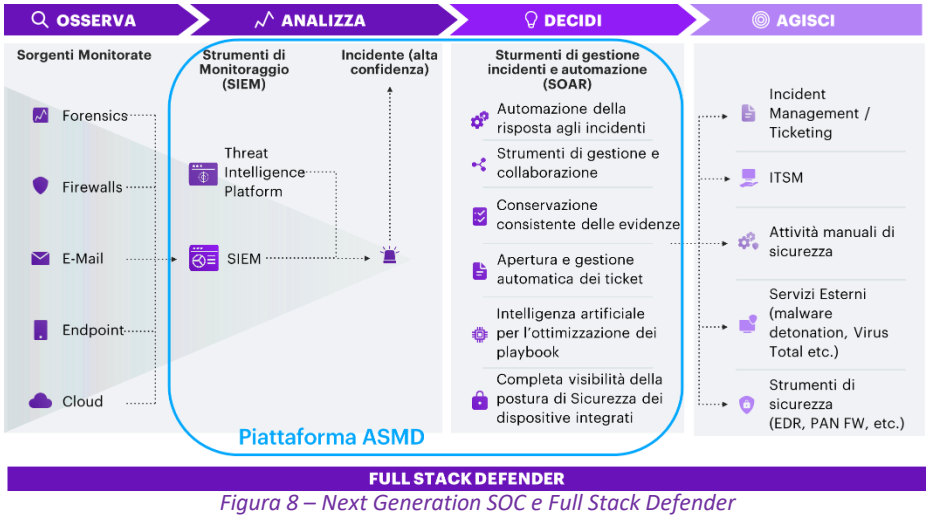


Figura 8 – Next Generation SOC e Full Stack Defender

Il modello NG-SOC proposto utilizza un approccio innovativo denominato "**Full Stack Defender**", il quale permette di superare i limiti di efficacia nella detection delle moderne soluzioni SIEM e SOAR. Tramite integrazione con le soluzioni tecnologiche proposte dai servizi di gara, questo modello offre un pannello centralizzato per il controllo real-time della postura di sicurezza delle amministrazioni, correlando e arricchendo le informazioni del SIEM con interrogazioni dirette ai dati delle altre soluzioni, sfruttandone così il pieno potenziale di visibilità sugli asset su cui sono installati. Permette inoltre di semplificare la complessità di ricerca e analisi delle cause sui sistemi, mettendo a disposizione degli analisti del SOC playbook di sicurezza sviluppati per agevolare le interrogazioni, delegando ad ASDM la complessità legata all'ottenimento dei dati, e abilitando gli analisti a focalizzarsi solo su temi significativi e compromissioni non note.

5.1.4 SIEM: Caratteristiche tecniche della soluzione

Un elemento cardine della piattaforma ASMD è il SIEM basato sulla soluzione ***Splunk***, le cui caratteristiche sono elencate nel §5.1.2. Il RTI ha maturato una lunga esperienza nell'integrazione e onboarding di log custom da un'ampia varietà di Clienti e tecnologie, che ha permesso la strutturazione di un **processo efficiente, flessibile e facilmente adattabile** ad ogni tipo di esigenza. La soluzione Splunk è stata selezionata proprio per la capacità del sistema di poter eseguire l'ingestione del *log* con diverse modalità, che includono, ad esempio, sia l'utilizzo del protocollo ***Syslog***, sia componenti per l'integrazione diretta come il ***DB-Connect*** oppure Agent quali ***Universal/Heavy Forwarder*** per collezionare, comprimere, pre-elaborare e inoltrare i dati in maniera sicura tramite canali cifrati. Inoltre, sono disponibili anche le ***API*** per l'implementazione delle chiamate alle interfacce offerte dai dispositivi da integrare al fine di raccogliere e correlare gli eventi di sicurezza prodotti. Il modello proposto sfrutta la normalizzazione e mapping dei logs tramite lo **Splunk Common Information Model** per garantire una rapida e uniforme fruizione attraverso gli use-case. La soluzione proposta permette di segregare i contesti delle singole PA, e di creare viste personalizzate per ognuna di esse, in modo da avere sempre chiaro il livello di sicurezza dei singoli asset integrati in relazione a tutti i servizi di sicurezza attivi.

Abbiamo inoltre sviluppato negli anni un'ampia libreria di *use-case*, basata sulle tipologie di attacchi osservati nei diversi settori e sulle tecniche identificate dal framework MITRE ATT&CK. Gli use-case vengono ottimizzati e integrati regolarmente attraverso un processo consolidato e un modello di sviluppo agile, a fronte dell'evoluzione delle minacce e sulla base dei feedback da parte degli analisti SOC e dei team coinvolti nella gestione degli incidenti. In aggiunta alle regole fornite dalla libreria, il servizio può sviluppare **regole personalizzate** sulle necessità e fonti dati specifiche dei clienti, attraverso un processo di identificazione e analisi dei requisiti, progettazione, sviluppo, test, messa in produzione e tuning degli *Use Case*.

5.1.5 Automazione e case management: caratteristiche tecniche della soluzione

Accenture ha progettato la piattaforma *ASMD* attorno al *SOAR* prendendo in input le esperienze maturate su altri progetti analoghi su svariate istituzioni governative in particolare italiane, inglesi, americane e dei paesi del nord Europa che hanno indirizzato gli investimenti dell'azienda dedicati allo sviluppo. Si è quindi giunti alla definizione di una libreria proprietaria di oltre 50 playbook capaci di introdurre un livello di **automazione** che partendo dalla *Knowledge Base* condivisa dai SOC di Accenture, porta alla riduzione dei tempi di identificazione, classificazione, notifica e risposta degli incidenti. Si ottiene così l'abbattimento dei falsi positivi e degli eventi duplicati consentendo agli specialisti *SOC* di concentrarsi su indagini di dettaglio e sul miglioramento continuo della qualità del servizio, con un incremento di efficienza misurato di circa il 60%. Quest'ultimo beneficia inoltre di processi strutturati, documentati e tracciabili che garantiscono consistenza nei risultati e relativa misurazione di efficacia rispetto ai KPI. Le **integrazioni** e i **playbook** implementati da Accenture e messi a disposizione della piattaforma ASDM proposto, mettono a disposizione una serie di valori aggiunti in termini di **efficacia di monitoraggio e risposta** alle Amministrazioni, tra cui:

- ***Case Management assistito*:** raccolta degli incidenti sulla base di filtri rilevanti, gestione assistita degli incidenti, arricchimento automatico di incidenti con informazioni di interesse, correlazione tra incidenti diversi e coordinamento delle azioni di risposta tra team distribuiti.
- **Gestione accessi:** blocco degli *account*, *reset password*, attivazione automatica di meccanismi di autenticazione a più fattori.
- **Arricchimento e *Threat Intelligence*:** ricerca automatica di indicatori di compromissione, ricerca e analisi dei risultati di scansioni precedenti, arricchimento delle informazioni raccolte, definizione di uno score complessivo, eventuale *whitelisting/blacklisting* dell'indicatore su base score.
- ***E-mail Gateway*:** download della mail e relativi allegati, blocco/rilascio automatico di mittenti e *URL*, codifica/decodifica degli *URL* nei messaggi, eventuale rilascio di un messaggio in quarantena.
- ***Forensics* e *Malware Analysis***: detonazione automatica di *URL*/allegati, ricerca di esiti per analisi passate, raccolta automatica del traffico di rete e di snapshot delle componenti potenzialmente malevole.
- ***Endpoint Protection e contenimento minacce*:** contenimento automatico di file e servizi, isolamento e contenimento automatico degli endpoint, raccolta di eventi rilevanti per uno specifico *host*, propagazione degli indicatori di compromissione sulle soluzioni di sicurezza installate, verifica della presenza di indicatori di compromissione su altri *host* diversi da quello compromesso.
- ***Firewall, IDPS, Web Gateway*:** raccolta automatica dei flussi di rete, raccolta dei log di rete e correlazione con quelli relativi agli strumenti di sicurezza degli endpoint, creazione/gestione/rimozione di regole e *policy*, aggiornamento delle firme degli strumenti di sicurezza, *blacklist* indirizzi IP/ FQDN.
- ***Vulnerability Management*:** raccolta di informazioni sulle vulnerabilità e correlazione automatica con le informazioni degli altri servizi attivi; è quindi possibile gestire un *triage* dinamico dell'incidente.

Inoltre, l'esperienza pluriennale delle aziende componenti il **RTI** nella ***SOC Automation,*** unita alla relazione di partnership strategica a livello globale con i principali player del settore tra cui *Palo Alto Networks* e *Splunk,* fornisce alle PA contraenti il beneficio del **continuo sviluppo di integrazioni, *use case* e *playbook*** che permettono di indirizzare le minacce emergenti. Accenture rappresenta un partner strategico per Splunk e, insieme a Fastweb, di PaloAlto Networks, con cui condivide l'esperienza accumulata sui Clienti e investe capitali significativi nello sviluppo di capability, asset e metodologie di delivery dal 2016; con oltre 3500 persone certificate su scala globale sulle tecnologie di entrambi i vendor, Accenture è stata riconosciuta da Splunk come *"Solution Partner of the Year"* nel 2019, *"Global Solution Partner of the Year"* nel 2020 e *"Global Sales Partner of the Year"* nel 2021, nonché da PaloAlto Neworks come *"Partner of the Year"* per il 2017, 2018 e 2019. Anche Fastweb vanta una forte collaborazione con Palo Alto Networks, certificata dal livello massimo di partnership "Diamond", ed è stata riconosciuta "Enterprise Service Provider of the Year 2021 – Italia". Un esempio di questo è rappresentato dal ***playbook* di *Threat Hunting*** per effettuare la ricerca proattiva di Indicatori di Compromissione (*IoC*) su larga scala per garantire una rapida identificazione e risposta delle minacce emergenti. Ogni qualvolta le fonti di *Threat Intelligence* identificano nuovi *IoC* rilevanti, quali indirizzi IP, *URL* o *hash* di codici malevoli, il *Playbook* ne esegue in parallelo la ricerca su tutte le istanze delle PA integrate con il servizio SOC nell'arco degli ultimi 90 giorni. Questo permette di industrializzare il processo di ricerca delle minacce, rendendolo continuo e immediato, riducendo la finestra di esposizione al rischio delle Amministrazioni.

5.2 Organizzazione

5.2.1 Strutture coinvolte

Il servizio *SOC* è erogato da un unico gruppo di lavoro *(SOC Team)* con base nel *Centro Servizi*, che risponde a un **Responsabile del Servizio SOC** (RSOC, vale a dire il Service Manager) il quale rappresenta il punto di contatto con il Referente tecnico dell'Amministrazione; il SOC Team è supportato da uno o più *SME* (*Subject Matter Expert*), esperti verticali nelle varie aree di *Cyber Security*. Al suo interno, il SOC Team presenta **tre gruppi di analisti** incaricati dell'analisi e gestione degli incidenti a complessità crescente: L1, L2 e L3. Il servizio si interfaccia inoltre con lo Smart HUB, per supporto nelle attivazioni del servizio, e con i Centri di Competenza/Partnership per competenze specialistiche utili all'erogazione del servizio.

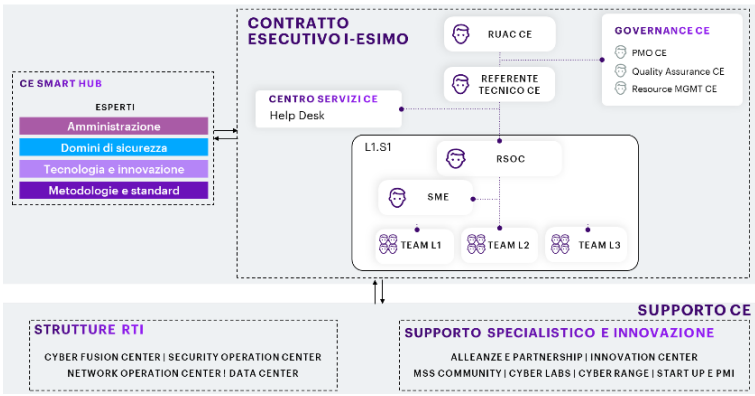


Figura 9 – Strutture coinvolte nel servizio

5.2.2 Team di servizio

Il 'SOC Team' che eroga il servizio è composto da esperti di Sicurezza certificati che operano all'interno di gruppi di lavoro ben definiti con chiara responsabilità e interagiscono tra loro e con l'Amministrazione attraverso canali di comunicazione con **massimi livelli di confidenzialità** in base alla natura delle informazioni scambiate. Di seguito si riporta una vista sintetica delle figure che compongono il 'SOC Team':

FUNZIONE-TEAM	RUOLO / PROFILO	COMPITI E RESPONSABILITÀ
Responsabile del	RSOC / SP	Punto di contatto tra l'Amministrazione e il SOC team con le responsabilità elencate nel §5.2.2 (Security

servizio		Operations Governance). Possiede certificazioni quali: ISO 27001, CISSP, ITIL, CISM.
Supporto di sicurezza Livello 1	Team L1 / Jr-ISC	Effettua il monitoraggio 24x7 degli allarmi di sicurezza, prioritizza gli allarmi, effettua l'analisi degli eventi e la verifica, verificare la raccolta dei log dalle sorgenti attive, fornisce report predefiniti, propone la riduzione dei falsi positivi, notifica gli eventi alle Amministrazioni. Possiede certificazioni quali: SSCP, CEH.
Supporto di sicurezza Livello 2	Team L2 / Sr-ISC	Fornisce report SIEM predefiniti, revisiona e analizza i report, effettua l'analisi degli allarmi e la verifica dei falsi positivi, fornisce supporto per la prima investigazione di breve periodo, effettua la qualifica di un evento in incidente di sicurezza, crea e traccia gli incidenti, monitora le Performance, identifica le azioni di contenimento di breve periodo. Possiede certificazioni quali: GCIH, GPEN, GCFE.
Supporto di sicurezza Livello 3	Team L3 / Sr-ISC	Investiga eventuali problemi relativi alle funzionalità del SIEM, supporta la risoluzione in caso di interruzione della raccolta dei log, supporta il tuning delle regole esistenti e delle risorse associate, si interfaccia con la PA, raccoglie e trasmette evidenze, valutazione post incidente per miglioramento continuo, fornisce supporto tecnico per escalation in caso di incidenti complessi. Possiede certificazioni quali: OSCP, GREM, GCFA
Specialisti di Cyber Security	SME / SSA	Esperti verticali nelle tematiche Cyber Defense per supporto nell'erogazione del servizio SOC, miglioramenti e risoluzione problemi sulle tecnologie e investigazione complessa in caso di incidente. Possiede certificazioni quali: CCSA, GCTI, certificazioni avanzate di prodotto (Splunk, Cortex XSOAR).
Legenda: SP Security Principal, Sr-ISC Senior Information Sec. Consultant, Jr-ISC Junior Information Sec. Consultant, SSA Sec. Solution Architect		

5.2.3 Security Operation Governance

Data la sua criticità, il servizio utilizza un *framework* di comunicazione che prevede allineamenti a differenti livelli, da quello operativo fino a quello Direzionale/Leadership. Il framework è già attivo su diversi contesti ed è in grado di scalare e indirizzare le esigenze di **PA di diversa dimensione**. La profondità e la frequenza delle interazioni, è dettata dal livello di **complessità e maturità** della PA coinvolta. Il RSOC rappresenta il punto di contatto tra il Referente Tecnico della PA e il SOC Team; ha la responsabilità di: ✓stilare e condividere il **Questionario di Pre-Installazione** (*QPI*) contenente le informazioni necessarie al processo di *onboarding*, i contatti dei referenti operativi della PA e i processi di escalation, ✓valutare e convalidare eventuali fornitori/terze parti/feed che forniranno dati alla **piattaforma di correlazione** (*SIEM*), ✓condividere e confermare le **aspettative** della PA ed evidenziare/indirizzare qualsiasi potenziale disallineamento, ✓creare i **collegamenti** tra i vari referenti dei team coinvolti, ✓rendere **disponibili e accessibili** alla PA le informazioni operative legate al servizio SOC, ✓lavorare a contatto con i referenti della PA per recepire i riscontri operativi e tradurli in attività di **miglioramento continuo**, ✓aiutare a costruire una **Knowledge Base** con informazioni sull'ambiente della PA e sui processi e le procedure del servizio, ✓mantenere contatti regolari con eventuali altri team, esterni all'ambito sicurezza, per condividere informazioni rilevanti che possano aiutare/migliorare l'integrazione e la collaborazione, ✓garantire che il RTI sia informato, come parte del processo di *Change Management*, su tutto ciò che è rilevante per il team di sicurezza o su incidenti operativi ed emergenze, ✓identificare i processi di automazione che facilitino la condivisione delle informazioni e la risposta alle minacce per guidare una **reazione più rapida e accurata**, soprattutto quando sono coinvolti più team.

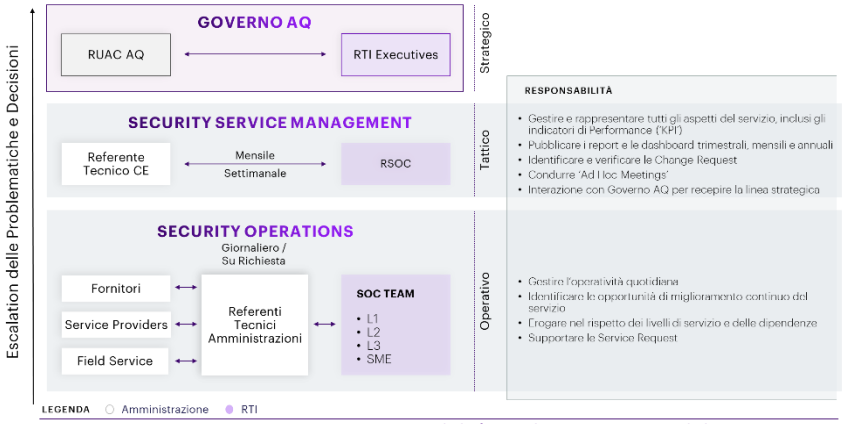


Figura 10 – Interazioni e responsabilità per la Governance del SOC

5.3 Modello Operativo

Il modello operativo del NG-SOC si basa su una stretta collaborazione tra i macro-processi di **Analisi e Monitoraggio della Sicurezza** e **Risposta agli attacchi e incidenti**, come rappresentato in figura.

Nello specifico, il macro-processo di **Analisi e Monitoraggio della Sicurezza** riportato in figura si articola nei sottoprocessi seguenti:

- **Raccolta delle sorgenti dati:** attraverso un processo standard che si avvale di checklist frutto dell'esperienza ventennale di Accenture e di Fastweb nel supporto delle PA, si offre un repository consolidato e scalabile di dati di sicurezza, inclusi eventi, *asset*, flussi e informazioni di contesto. I sistemi di memorizzazione sono gestiti secondo i più moderni standard di sicurezza quali ad esempio FIPS 140-2.
- **Attivazione di *use case* e regole di correlazione:** include la definizione, consolidamento e attivazione di un insieme di regole di correlazione di interesse per lo specifico contesto delle Amministrazioni contraenti.
- **Monitoraggio del SIEM e *alerting*:** il processo garantisce il monitoraggio continuo delle informazioni prodotte dal SOC. Questo include l'utilizzo di dashboard e canali necessari al monitoraggio continuo e completo dei sistemi, che permettano ad analisti, *team lead* e *stakeholder* in generale di avere visibilità sulla postura di sicurezza dell'Amministrazione.
- **Correlazione, identificazione e classificazione degli incidenti**: L'utilizzo di meccanismi di AI, *Analytics* e automazione, in aggiunta alle fonti esterne integrate, permette all'analista di incrementare significativamente la rilevanza e contestualizzazione delle segnalazioni in termini di completezza e accuratezza incrementando così il livello di efficacia del servizio.

Il macro-processo di **Risposta agli attacchi e incidenti** ha la responsabilità di gestire e, in caso, rispondere e notificare eventi di sicurezza nei confronti della PA contraente. Nello specifico, si articola nei seguenti sottoprocessi:

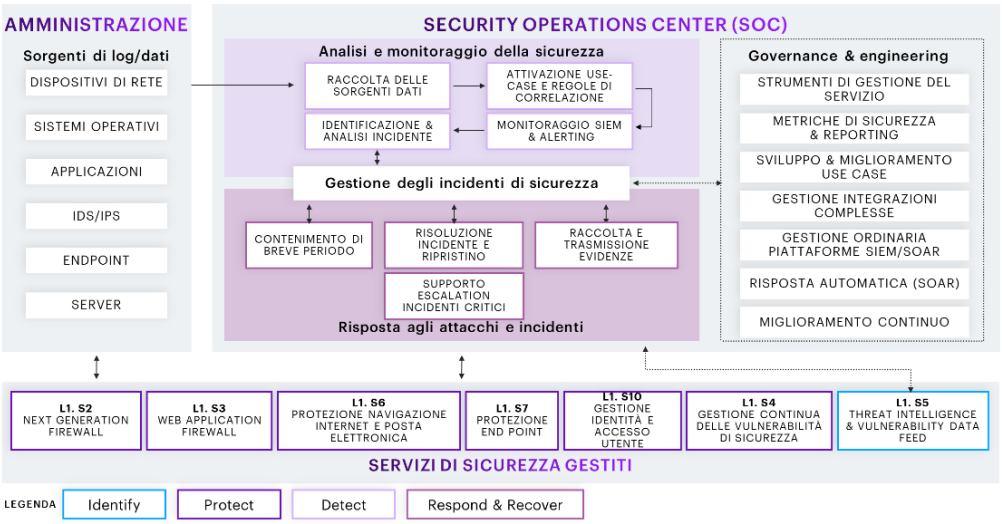


Figura 11 – Modello Operativo del SOC

- **Contenimento di breve periodo:** Identificazione e comunicazione verso la PA delle possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione.
- **Raccolta e trasmissione delle evidenze:** Acquisizione di eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente. Le evidenze digitali raccolte sono poi trasmesse al referente tecnico della PA e archiviate.
- **Risoluzione dell'incidente e ripristino:** Azioni necessarie per rispondere all'incidente in maniera pervasiva. La risoluzione dell'incidente include inoltre una valutazione a posteriori, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza e aumentare l'efficacia del SOC.
- **Supporto escalation incidenti critici:** In caso di incidenti di sicurezza critici sugli ambienti delle Amministrazioni, la cui gestione non rientri nella normale operatività prevista per il SOC, è previsto un processo di escalation verso gli SME del RTI al fine di investigare in maniera estesa sulla natura della compromissione e l'eventuale apertura di un tavolo tecnico con i vendor della tecnologia specifica per assicurare un confronto tempestivo, sfruttando gli accordi di partnership che garantiscono il massimo supporto nell'esecuzione delle attività. Data la natura altamente eterogenea degli scenari possibili, legati necessariamente alla specificità della compromissione, si assume che attività di questo tipo rientrino nel contesto di un ingaggio dedicato dei servizi professionali.

ATTIVITÀ	RTI	AMMINISTRAZIONE
Identificazione	R/A	
Classificazione	R/A	
Notifica	R/A	I
Contenimento	R/A	C
Risoluzione	C	R/A
Ripristino	I	R/A
Lesson Learned	R/A	C
*LEGENDA: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed*		

Figura 12 – RACI per le fasi di gestione degli incidenti

In figura si riporta la RACI relativa al modello operativo del servizio SOC in relazione alle fasi di gestione degli incidenti di sicurezza. L'assegnazione della priorità di gestione verrà effettuata in maniera coerente con i livelli specificati in ambito di gara.

5.3.1 Modalità di erogazione

Al netto della fase di setup iniziale delle soluzioni tecnologiche in uso dal SOC, l'attivazione del servizio per le singole PA passa per un approccio a fasi, con l'obiettivo di identificare e predisporre la raccolta dei log di interesse e attivare le regole di correlazione per lo specifico contesto. Si riporta nel seguito una descrizione delle singole fasi.

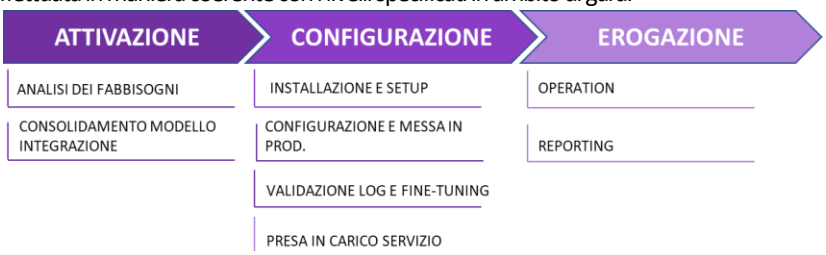


Figura 13 - Modalità di erogazione

ATTIVAZIONE	
Analisi dei Fabbisogni, Piano Operativo e Contratto Esecutivo	**Deliverable**: Piano Operativo e Contratto Esecutivo **Descrizione**: Il Team supporta l'Amministrazione nella stesura del Piano dei Fabbisogni in termini di esigenze di sicurezza, per definire, in particolare: ✓quantità e tipologie dei servizi da richiedere ✓modalità di erogazione e consuntivazione degli stessi ✓tutte le ulteriori caratteristiche utili ottenute dall'analisi del contesto tecnologico e applicativo. Kick off meeting volto ad avviare le attività propedeutiche all'erogazione del servizio riportate nella fase "Configurazione". Il Fornitore procede, quindi, con l'identificazione e contestualizzazione dei servizi, l'eventuale declinazione delle figure professionali e degli strumenti a supporto per finalizzare il Piano Operativo. Espletamenti economici e amministrativi in relazione al Contratto Esecutivo
Consolidamento modello di attivazione SOC	**Deliverable**: "Questionario di Pre-Installazione" (QPI) contenente tutti gli aspetti tecnici e organizzativi dell'ambito di monitoraggio **Descrizione**: Eventuale aggiornamento del Piano di Presa in carico (incorporato nel Piano Operativo). Attività conseguenti di: ✓consolidamento delle soluzioni tecnologiche in ambito ✓identificazione di eventuali prerequisiti di integrazione e raccolta delle sorgenti ✓consegna della documentazione necessaria all'attivazione del servizio ✓identificazione dei responsabili

CONFIGURAZIONE	
Installazione e setup	**Deliverable**: N/A **Descrizione**: Comprende: ✓predisposizione delle componenti di raccolta e inoltro dei log ✓installazione delle componenti nelle specifiche amministrazioni ✓attivazione dei flussi di rete e dati in ingresso e uscita necessari all'attivazione
Configurazione e messa in produzione	**Deliverable**: N/A **Descrizione**: Comprende: ✓configurazione dei dispositivi e sistemi in ambito ✓configurazione delle componenti di back-end delle soluzioni SIEM e SOAR ✓configurazione delle componenti di raccolta e inoltro
Validazione dei log e fine-tuning	**Deliverable**: N/A **Descrizione**: Comprende: ✓controllo della qualità dei log e rimozione dei falsi positivi ✓configurazione sicura delle componenti installate (hardening) ✓convalida degli eventi e attivazione dei casi d'uso
Presa in carico	**Deliverable**: "Checklist di Presa in Carico" (CPIC) **Descrizione**: Presa in carico delle piattaforme e avvio del monitoraggio attivo per la

CONFIGURAZIONE	
	specifica Amministrazione.

EROGAZIONE	
Operation	**Deliverable**: Report attività manutenzione **Descrizione:** Erogazione continuativa del servizio SOC come da modello operativo descritto al §5.3.
Reporting	**Deliverable**: Report di servizio **Descrizione**: Generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF

5.3.2 Controllo di Qualità e miglioramento continuo

Il processo di miglioramento continuo proposto è parte integrante del CDOM e, nello specifico, del servizio SOC; prevede un monitoraggio costante su base trimestrale degli indicatori di performance e qualità sopra definiti da parte del RSOC. I gap identificati rispetto ai livelli attesi vengono analizzati e catalogati secondo la combinazione di impatto sulla qualità e complessità di implementazione. Il RSOC disegna, discute e condivide con la PA una roadmap suddivisa tra azioni di tipo quick-win a breve e medio termine e prevede una serie di aree di intervento che riportiamo a titolo esemplificativo e non esaustivo, suddivise per ambiti tematici:

- **Tecnologica** (es. rivisitazione delle regole dei dispositivi, tuning dei log inviati, ampliamento e integrazione delle sorgenti, valutazione di ulteriori prodotti di sicurezza, affinamento della use-case library e/o dei playbook per la corretta prioritizzazione e l'analisi dei trend, tuning delle regole della piattaforma ASDM)
- **Processi** (es. revisione delle procedure di escalation, rivisitazione della matrice RACI, affinamento del processo di OnBoarding, eventuale ri-allineamento con il contesto di business e i nuovi scenari di minaccia)
- **Persone** (es. riassegnazione del team a supporto, training mirato ai referenti tecnici dell'Amministrazione, del SOC Team e delle terze parti).

In caso di **specifiche esigenze** emerse durante le regolari **service review** condivise con la PA, vengono organizzati workshop tematici dedicati, ove possibile, svolti in ambienti immersivi come i centri di innovazione citati al §17, sfruttando approcci come il **Design Thinking,** agevolato da simulazioni di miglioramento dei processi su **SPARK** (cfr. §4.8). Strumento di ausilio alle service review è **LimeSurvey** (cfr. §16.1.1) per raccogliere livello di gradimento e suggerimenti. Gli argomenti di cybersecurity trattati possono essere svariati, ad esempio: Strategia di CyberSecurity, Security Operations, Strategie di Platform e Content Development, Application Security, Insider Threat, Adversary Simulation. I risultati possono portare a una rivisitazione dell'Operating Model di Sicurezza dell'Amministrazione, una Roadmap evolutiva, un'analisi del Modello di Maturità, oppure uno specifico e dettagliato "piano di azione".

Inoltre, il capitale umano e professionale del pool di risorse impiegato che vanta un numero considerevole di certificazioni di settore, non solo opera all'interno del Servizio SOC mantenendo i più alti standard qualitativi, ma **partecipa attivamente alla CyberSecurity Room** come descritto al §17'. In questo modo vengono recepite le esigenze del Servizio SOC che, tradotte ove possibile in stream innovativi, concorrono al miglioramento costante dell'efficacia del servizio.

Per raggiungere tale scopo risulta fondamentale una corretta ed efficace definizione degli indicatori di prestazione (KPI), i quali sono stati definiti a partire dai seguenti principi: ✓i '*KPI*' possono differire o essere aggregati in base all'audience di destinazione ✓la valutazione deve essere fatta non solo sui numeri relativi, ma anche per i valori assoluti ✓i valori isolati non sono sufficienti, anche il trend e la progressione sono rilevanti ✓un singolo '*KPI*' può essere suddiviso in più valori, raggruppati per unità di business, geograficamente, ecc. ✓i picchi o i cambiamenti significativi devono essere analizzati e spiegati. Sulla base della valutazione dei '*KPI*' vengono definite e implementate le azioni di miglioramento, concordate con adeguati livelli di gestione.

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, in aggiunta agli indicati richiesti dal bando di gara si illustrano gli ulteriori indicatori di qualità previsti per il servizio in oggetto:

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "SOC"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_PICM	Presa in carico di un incidente da parte dei sistemi di monitoraggio - Tempo trascorso dall'accadimento dell'incidente alla registrazione sul sistema di TT da parte dei sistemi di monitoraggio	[#incidenti presi carico nei tempi previsti / #totale incidenti aperti] x 100 Tempo previsto di registrazione < 10'	Trimestre	95%
PCI_TIIS	Tempo di prima investigazione per incidenti di sicurezza	Come TIIS ma con frequenza maggiore e soglia più sfidante	Mensile	PCI_TIIS = 0 con tempi massimi di consegna della "prima investigazione" dimezzati rispetto a TIIS
KPI_ISU	Incidenti segnalati dagli utenti	Num. incidenti di cybersecurity segnalati dagli utenti e non dai sistemi di monitoraggio	Trimestre	Atteso un non incremento rispetto alla rilevazione precedente

5.3.3 Report aggiuntivi per l'Amministrazione

Il RTI ritiene il reporting e miglioramento continuo attività chiave per la completa ed efficace gestione dei servizi in ambito, in quanto componenti fondamentali nel monitoraggio e misurazione dell'efficacia e della maturità dei servizi erogati attraverso: ✓report forniti all'Amministrazione ✓analisi delle risorse e delle attività in base ai KPI definiti ✓supporto alla gestione tramite l'analisi dei risultati ottenuti ✓elaborazione di raccomandazioni e punti di miglioramento. In aggiunta ai report richiesti dal capitolato che verranno prodotti durante la normale operatività del servizio SOC, offriamo i seguenti report aggiuntivi:

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sulle tecnologie SOC solo qualora fossero previsti possibili impatti di servizio.

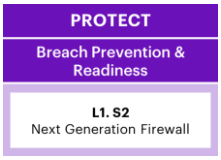
5.4 Interazioni

5.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
Next Generation Firewall	Log di audit ed eventi verso il SIEM	Input/ Output	I sistemi inviano log al SIEM affinché gli eventi generati dai NGFW possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza. Attivazione di eventuali azioni di risposta automatica.
Web Application Firewall	IoC	Input/ Output	Gli IoC provenienti dalla piattaforma di Threat Intelligence sono raccolti in input dai Next Generation Firewalls per limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash). Attivazione di eventuali azioni di risposta automatica.
Gestione continua delle vulnerabilità	Vulnerability Report	Input	Le vulnerabilità identificate dal processo di Vulnerability management possono essere correlate agli eventi di sicurezza per ridurre i falsi positivi e innalzare la criticità di eventi identificati sui target.
Threat Intelligence & Vulnerability Data feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence possono essere correlati agli eventi di sicurezza per identificare più rapidamente le nuove minacce in modo proattivo o per identificare minacce già presenti nel perimetro non precedentemente identificabili.
Protezione navigazione internet e posta elettronica	Log di eventi verso il SIEM	Input	I sistemi inviano log al SIEM affinché gli eventi generati dai sistemi di Navigazione Internet e di Posta Elettronica possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza
Protezione end point	Log di eventi verso il SIEM	Input / Output	I sistemi inviano log al SIEM affinché gli eventi generati dai sistemi di Protezione End Point possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza. Attivazione di eventuali azioni di risposta automatica.
Gestione identità e accesso utente	Log di audit ed eventi verso il SIEM	Input / Output	I sistemi inviano log al SIEM affinché gli eventi generati dai sistemi di Gestione identità ed accesso utente possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e arricchire la ricostruzione della timeline di incidenti di sicurezza. Attivazione di eventuali azioni di risposta automatica.
Innovazione	CyberSecurity Room	Input / Output	Recepire le esigenze del Servizio SOC e tradurle ove possibile in stream innovativi, in modo da concorrere al miglioramento costante dell'efficacia del servizio.

6 PROPOSTA PROGETTUALE PER IL SERVIZIO "NEXT GENERATION FIREWALL"

6.1 Soluzione Proposta



Il **modello CDOM** (cfr. §§1 e 3.3) colloca questo servizio nel dominio di sicurezza "**Breach Prevention & Readiness**" allineata alla Funzione NIST "**Protect**".

Il servizio di **Next-Generation Firewall** (NGFW) rappresenta uno degli asset fondamentali del Centro servizi, in quanto consente di implementare i controlli di sicurezza essenziali alla protezione di rete, applicando restrizioni alle comunicazioni esterne o interne alla singola PA, limitando gli accessi delle singole risorse ai soli flussi di traffico definiti come leciti. Ciò è possibile utilizzando policy basate non solo sui **meccanismi classici di segregazione di rete L3 (network) e L4 (trasporto)**, ma anche su **capacità di analisi del layer applicativo**, ispezionando il contenuto dei messaggi scambiati con protocolli quali HTTP, FTP, SIP, ecc. che consentono di implementare **filtri molto più dettagliati** rispetto alle funzionalità base dei firewall standard. Ulteriori **elementi di valore** sono rappresentati dalla possibilità di definire regole basate sull'identità dell'utente, abilitando l'infrastruttura ad ammettere flussi di traffico in base al **principio least-privilege** e di procedere all'**ispezione di traffico TLS/SSL** necessaria per controllare efficacemente il traffico cifrato che costituisce gran parte del traffico interno ed esterno alle PA.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: più di 50, tra cui Ministero delle Infrastrutture e dei Trasporti, Regione Lombardia, AgID, RAI

Private: NEXI, A2A, ENI, primario operatore finanziario

Descrizione di un caso di successo - **Ministero delle Infrastrutture e dei Trasporti - Provveditorato Interregionale alle Opere Pubbliche per il Veneto, Trentino Alto Adige e Friuli Venezia Giulia** →**Esigenza** - Realizzazione dell'infrastruttura di sicurezza di rete del sistema "MO.Se" di Venezia, atta a contrastare eventuali attacchi e minacce apportate all'infrastruttura di rete ed ai servizi ospitati in Data Center →**Soluzione** – Fastweb ha realizzato un'architettura caratterizzata da un elevato grado di flessibilità, prestazioni e resilienza. Sono state condotte campagne di Network penTesting di tipo blackbox/greybox che hanno mostrato l'efficacia dei presidi di sicurezza Fortigate nel resistere agli attacchi simulati →**Benefici** - Il beneficio più evidente è stato una riduzione del rischio complessivo dell'intera architettura di rete: ✓forte resilienza dei bastioni Fortigate di resistere alle minacce garantendo una riduzione della superficie d'attacco e un miglioramento della postura di sicurezza del Network e dei sistemi, come confermato dai dati del servizio SIEM che hanno mostrato il trend di riduzione delle minacce intercettando un numero di IoC molto minore rispetto alla soluzione di sicurezza precedente ✓capacità di integrarsi con la soluzione Active Directory DS permettendo di implementare logiche di policy basate sull'identità dell'utente

6.1.1 Funzioni offerte

Il servizio prevede: un livello di **Interfaccia PA** utile all'interazione con il servizio, un livello di **Erogazione** in cui sono espletate le funzioni principali del servizio, un livello di **Automazione** (intelligent layer) che aggiunge funzioni avanzate, un livello **Interazioni** per le relazioni con gli altri servizi. I livelli comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative**, descritte di seguito.

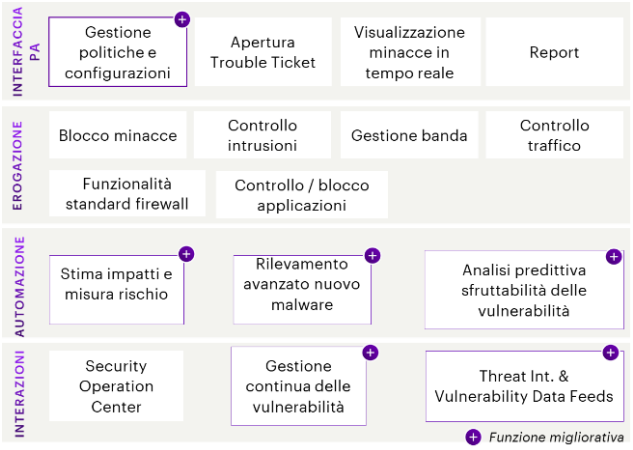


Figura 14 - Funzioni del servizio

- **Gestione politiche e configurazioni**: funzioni di "Geo-IP filtering e Geo-Blocking" per consentire la creazione di regole di policy da applicare a specifici paesi e/o regioni geografiche;
- **Stima degli impatti e misura del rischio**: la funzione esegue le stime di impatti e rischio sulle configurazioni implementate o che si prevede di implementare fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura. Tali valutazioni sono effettuate tenendo in considerazione: ✓la classificazione delle informazioni trattate, ✓la criticità del servizio abilitato per la PA, ✓le dipendenze e interazioni con altri servizi, funzioni e sistemi;
- **Rilevamento avanzato del malware**: la funzione prevede metodi avanzati di 'malware detection' fortemente potenziate dall'integrazione con il servizio di Threat Intelligence, nonché con il SOC e prevedono azioni automatizzate per isolare comportamenti di rete anomali che possono segnalare la presenza di malware noto o di possibili varianti;
- **Analisi predittiva della sfruttabilità delle vulnerabilità**: la funzione combina dati e informazioni sulle minacce da più fonti analizzando con un algoritmo di apprendimento automatico basato su ML, per anticipare la probabilità che una vulnerabilità venga sfruttata, anche grazie all'**Interazione con i servizi** di SOC, **ma anche di Gestione continua delle vulnerabilità e Threat Intelligence e Vulnerability Data Feeds** (cfr. §6.4.1).

6.1.2 Architettura tecnologica

La soluzione tecnologica NGFW offerta dal Centro Servizi è basata su tecnologia **Fortinet**, riconosciuta come **leader sul mercato** come attestato da Gartner in entrambi i report Magic Quadrant 2020 per Network Firewall e WAN Edge Infrastructure. Accenture, Fastweb e Fortinet vantano una pluriennale partnership che ha consentito di integrare tali tecnologie in sistemi informativi complessi ma, soprattutto, di definire una metodologia standard per poterla portare rapidamente e con strumenti di configurazione standard presso altri Clienti. In particolare Fastweb è il principale partner di Fortinet nell'ambito della PA. Il NGFW Fortinet, denotato dalla classe di prodotti **Fortigate**, fornisce una **ampia e consolidata copertura dei requisiti** di tecnico-funzionali espressi nel capitolato e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi.

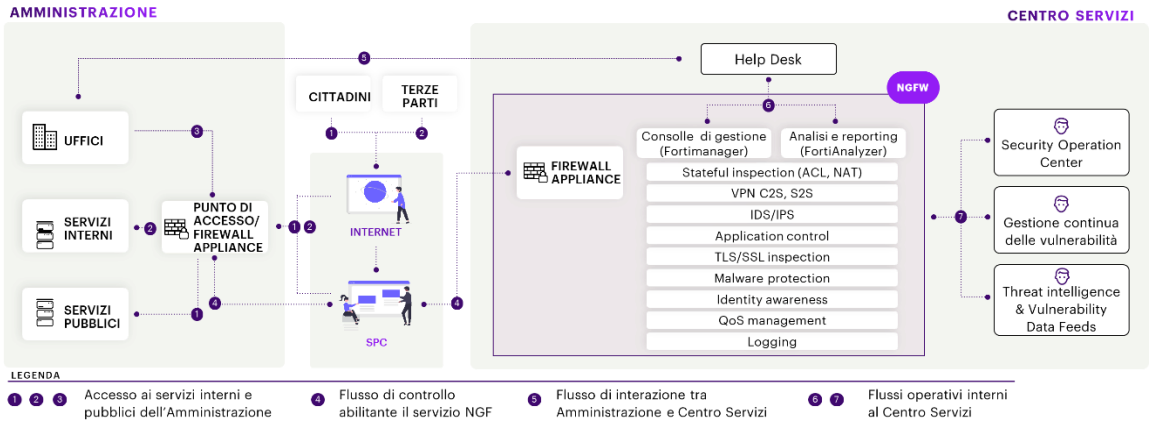


Figura 15 - Architettura tecnologica NGFW

L'architettura prevista per la fornitura di servizio prevede l'integrazione del NGFW (o gateway), nella sua forma fisica o virtuale, localmente presso la singola PA oppure remotamente presso il Centro Servizi (scelta subordinata agli accordi con la PA contraente), predisponendo una console di gestione centralizzata in esercizio presso lo stesso Centro Servizi. La scelta architetturale inerente all'installazione on-premise degli appliance presso la PA oppure remotamente presso il Centro Servizi sarà eseguita durante la fase di attivazione del servizio, subordinata alle caratteristiche dell'infrastruttura di rete della singola sede piuttosto che alla lista di servizi di sicurezza NGFW da attivare. La console di gestione centrale, denominata **FortiManage**r, consente di avere una visibilità generale sullo stato dei singoli gateway, permettendo la configurazione della soluzione e il relativo monitoraggio anche grazie all'integrazione con la soluzione SIEM, gli Active Directory o altri user repository. La possibilità di avere in unico punto la gestione di molteplici PA è garantita dal concetto di **Dominio Amministrativo** (ADOM – Administrative Domain), che consente la definizione di ambienti completamente indipendenti. Al fine di garantire funzionalità avanzate di analisi e reporting, sarà implementato un ulteriore elemento centrale di analisi, logging e reporting, denominato **FortiAnalyzer**, deputato alla raccolta e correlazione dei messaggi provenienti da tutti gli apparati attivi, con la possibilità di produrre report a diversi livelli di sintesi.

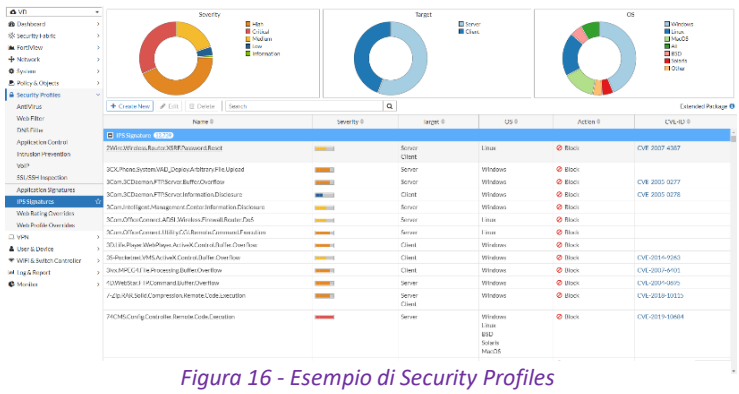


Figura 16 - Esempio di Security Profiles

6.1.3 Caratteristiche tecnologiche e prestazionali, comprese quelle migliorative

Gli appliance firewall saranno disponibili in versione chassis fisico o macchina virtuale al fine di garantire la **massima adattabilità** al contesto di rete e vincoli tecno logico/operativi. L'utilizzo di una forma piuttosto che di un'altra sarà concordata e selezionata dalla specifica PA.

Le caratteristiche degli **appliance FortiGate** vanno oltre quelle standard di stateful firewall, in quanto dotati di capacità di **ispezione dei contenuti avanzate fino**

al livello 7 del modello ISO/OSI. Questo garantisce capacità di ispezione sul layer applicativo con funzionalità di Intrusion Prevention**,** Antivirus, Cloud Sandbox, Application Control e Web Filtering, disponibili come security profile. In figura si fornisce un esempio della dashboard di analisi per erogare "IDS e IPS".

In particolare, questo tipo di appliance consente di attivare in maniera granulare tali funzionalità, associando uno o più security profile alle specifiche policy di accesso (ACL). In accordo con le **best practice di settore**, per ciascuna tipologia di traffico sarà predefinito un set di profili di sicurezza da abilitare su ciascuna categoria di traffico. Tuttavia, sarà possibile richiedere ed evadere richieste di apertura e controllo del traffico su cui abilitare o meno, determinati servizi in accordo con gli standard della specifica PA. In generale, saranno definite linee guida di sicurezza infrastrutturale che permetteranno di identificare flussi di comunicazione pre-approvati per i quali non è necessaria un'approvazione esplicita. In accordo con la PA sarà possibile definire un flusso di approvazione esplicito del provisioning delle regole in caso di deroga allo standard pre-approvato piuttosto che sempre necessario per ogni singola richiesta.

Service	Action	NAT	Security Profiles	Log
SSH UDP-22	ACCEPT	Disabled	SSL no-inspection	UTM
ALL	ACCEPT	Dyna_2...	SSL no-inspection	UTM
ALL	ACCEPT	NAT IN...	WEB web_monitor APP application_monitor SSL certificate-inspection	All
HTTP HTTPS	ACCEPT	pool_2...	WEB web_basic_security APP application_monitor SSL certificate-inspection	All

Figura 17 - Applicazione granulare security profiles per singola ACL

Inoltre, un aspetto **migliorativo** rispetto al modello di cybersecurity Zero Trust, è la possibilità di poter impostare **regole di accesso basate sull'identità dell'utente, indipendentemente dalla network location sorgente**. È importante quindi specificare che mediante un'integrazione con l'infrastruttura di autenticazione, quale ad esempio Active Directory, è possibile implementare policy di accesso specifiche per singoli utenti o gruppi di utenti, in base al principio del least-privilege. Considerando il contesto distribuito di accesso alle risorse, con un numero sempre maggiore di utenti in smart working, questa feature diventa indispensabile per garantire una **user-experience soddisfacente**. Inoltre, come elemento **distintivo e migliorativo** occorre considerare l'**integrazione dei gateway con la piattaforma di Threat Intelligence** (TIS) proprietaria di Accenture (cfr. §10.1.3), con la quale sarà **immediata** la distribuzione di IOC associati a URL, IP, domini e file malevoli per bloccare l'interazione degli asset della PA con risorse malevoli. Questa funzionalità è particolarmente utile nel caso sia necessario attuare una risposta immediata ad eventi di cybersecurity.

I NGFW Fortinet soddisfano appieno le **esigenze di prestazioni delle architetture IT ibride e hyperscale**, permettendo alle PA un'esperienza utente ottimale e gestire al meglio i rischi di cyber security. In linea con questo requisito e con le indicazioni formulate in capitolato, saranno forniti gateway con throughput diverso a seconda delle necessità delle singole PA.. I singoli componenti saranno aggiornati in base alle roadmap evolutive del vendor e le date pubblicate di End of Life e End of Support, al fine di garantire la **disponibilità in esercizio di appliance continuamente aggiornate e supportate**.

Ulteriore elemento **migliorativo** rispetto ai requisiti da capitolato riguarda i **livelli prestazionali** degli apparati che sono assicurati da una **elaborazione del traffico realizzata prevalentemente a livello hardware, anziché software, mediante l'utilizzo di circuiti integrati denominati Secure Processing Units (SPU)**. In particolare, le SPU hanno il compito di eseguire funzioni di sicurezza ad alto impatto computazionale come la decrittazione TLS/SSL (incluso TLS1.3), IPS e antivirus, in modo che la CPU centrale possa svolgere altre attività di elaborazione del traffico, **evitando impatti sulla fruizione dei servizi protetti dal gateway e impatti sulla esperienza utente**.

6.2 Organizzazione

6.2.1 Strutture coinvolte

Il servizio NGFW è erogato da un team specializzato su servizi di sicurezza infrastrutturale, che risponde a un **Responsabile del servizio;** il team è supportato da uno **SME** (Subject Matter Expert) esperto su tecnologie NGFW. Come per tutti i servizi, è previsto il supporto delle seguenti strutture:

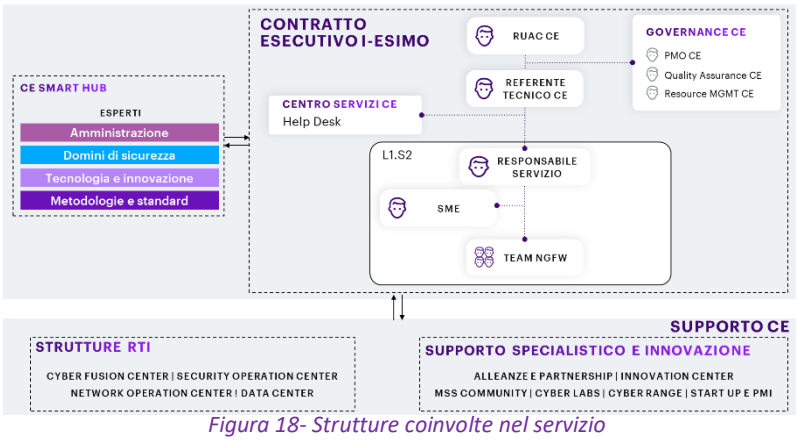


Figura 18- Strutture coinvolte nel servizio

- **CE SMART HUB**: team di esperti con lo scopo di fornire un contributo fondamentale in fase di Attivazione del servizio poiché, grazie alle loro specializzazioni su diversi Clienti, tecnologie e metodologie/standard, supportano il design del servizio in modo che possa erogare con il più alto livello di qualità le richieste della PA contraente. L'HUB sarà poi disponibile in corso di Erogazione in tutti i casi in cui il team del servizio abbia necessità di contributi specialistici nei domini sopra citati (es. è possibile richiederne l'intervento per supportare la PA nell'integrazione del gateway e l'abilitazione dei profili di sicurezza).
- **Centri di Competenza/Partnership** che forniscono competenze specialistiche utili all'erogazione del servizio. In particolare, il team di lavoro avrà la possibilità di avvalersi del supporto fornito dai CdC Infrastrutture (cfr. §3.x) e dai vendor.

6.2.2 Team del servizio

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
Governo del Servizio	Responsabile del servizio / Sr-ISC	Supporta la PA per la redazione del Piano dei Fabbisogni, redige il Piano Operativo. Coordina le attività del servizio per garantire che i risultati siano ottenuti nei tempi e con le modalità previsti. Rappresenta il punto di contatto con la PA; è incaricato della comunicazione con gli altri servizi e della condivisione delle informazioni.
SME NGFW	Supporto al team NGFW / SSA	Offre consulenza nella risoluzione di attività critiche (Incident, Change), problemi infrastrutturali o progetti specifici. È coinvolto nell'ottimizzazione del Servizio e supporta la PA nell'evoluzione dell'infrastruttura.
NGFW team	L2 Security Engineer / Sr-ISC	Supporta e integra le attività del L1 Security Engineer e si attiva per incident di priorità elevata e change complesse. Attiva il supporto dei Vendor e gestisce l'andamento della richiesta sino alla chiusura.

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
NGFW team	L1 Security Engineer / Jr-ISC	Registra il ticket e ne assegna la priorità, eseguendo l'analisi e la diagnosi iniziale. Esegue procedure per la risoluzione dei ticket o l'applicazione di workaround, attivando eventualmente procedure di escalation.

Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect

6.3 Modello operativo

6.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

Figura 19 - Modello operativo

6.3.2 Modalità di erogazione

Di seguito la descrizione delle attività.

ATTIVAZIONE	
Analisi dei Fabbisogni, Piano Operativo e Contratto Esecutivo	**Deliverable**: Piano Operativo e Contratto Esecutivo **Descrizione**: Il Team supporta la PA nella stesura del Piano dei Fabbisogni in termini di **esigenze di sicurezza**, per definire, in particolare: ✓quantità e tipologie dei servizi da richiedere ✓modalità di erogazione e consuntivazione degli stessi ✓tutte le ulteriori caratteristiche utili ottenute dall'analisi del contesto tecnologico e applicativo. Il Fornitore procede, quindi, con l'identificazione e contestualizzazione dei servizi, l'eventuale declinazione delle figure professionali e degli strumenti a supporto per finalizzare il Piano Operativo. Espletamenti economici e amministrativi in relazione al Contratto Esecutivo.
Presa in carico	**Deliverable**: Piano di Presa in carico aggiornato, Verbale di completamento del passaggio di consegne, verbali di SAL **Descrizione**: Eventuale aggiornamento del Piano di Presa in carico (incorporato nel Piano Operativo). Attività conseguenti di: ✓allocazione delle risorse ✓predisposizione strumenti ✓configurazione del Portale della Fornitura ✓condivisione ed eventuale adattamento del processo di gestione degli incidenti ✓predisposizione della documentazione sulle modalità di misurazione degli Indicatori di Qualità. Ove richiesti, ✓acquisizione di know how relativo al contesto organizzativo, tecnologico e funzionale ✓acquisizione di standard, modalità operative, linee guida e metodologie in uso presso la PA. Governo e Monitoraggio delle attività. Kick off meeting volto ad avviare le attività propedeutiche all'erogazione del servizio riportate nella fase "Configurazione"

CONFIGURAZIONE	
Installazione e setup	**Deliverable**: N.A. **Descrizione**: All'interno di questo processo rientrano: ✓Consegna dell'apparato presso la PA (consegna fisica o OVA) ✓Setup iniziale HW (rack & stack) o vHW (deployment virtual appliance) ✓Setup configurazione (major and minor version, patches, interfaccia management) ✓Integrazione nella rete della PA ✓Integrazione con le piattaforme centralizzate
Configurazione e messa in produzione	**Deliverable**: N.A. **Descrizione**: All'interno di questo processo rientrano: ✓Configurazione delle policy standard ✓Configurazioni specifiche rispetto al CE, eventuale porting di configurazioni da appliance esistenti ✓Test della configurazione ✓Passaggio in produzione ed eventuale swap da sistemi pre-esistenti ✓Tuning delle funzionalità attivate ✓Supporto post passaggio in produzione

EROGAZIONE	
Gestione ciclo di vita policy	**Deliverable**: N.A. Descrizione: ✓Creazione e modifica di policy di sicurezza ✓Estrazione informazioni quali esportazione di log, accessi, policy attive o procedure in essere
Operation	**Deliverable**: Report attività manutenzione **Descrizione**: Gestione di incidenti o problemi mediante: ✓l'applicazione di soluzioni permanenti utili a risolvere l'incidente ✓l'applicazione di workaround e analisi successiva della root cause per l'eliminazione definitiva di incidenti e problemi. Applicazione di aggiornamenti software, hotfix, operazioni di riavvio di specifici processi applicativi. Verifica funzionalità di base per alta affidabilità, backup e monitoraggio infrastrutturale
Reporting	**Deliverable**: Report di servizio **Descrizione**: Generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF

CHIUSURA	
Passaggio di consegne	**Deliverable**: Piano di Trasferimento di fine fornitura, Verbali di SAL, Reporting finale delle attività svolte **Descrizione**: ✓Sessioni di lavoro per il passaggio della conoscenza e sua verifica. ✓Governo e monitoraggio e supporto alle attività.
Consegna dei dati dell'Amm.ne	**Deliverable**: Dati **Descrizione**: Sono riconsegnati i dati riguardanti la PA che sono stati utilizzati durante il periodo di erogazione
Consegna della documentazione	**Deliverable**: Documentazione tecnica **Descrizione**: Verifica e Consegna della documentazione tecnica completa e aggiornata che è stata prodotta durante il periodo di erogazione

6.3.3 Livelli di assistenza

Il Modello Operativo per l'erogazione di **tutti i servizi** si basa su **tre livelli di lavorazione**, più un quarto livello per l'interazione con i Vendor tecnologici: ✓Il **Primo Livello (L1)** corrisponde all'Help Desk del Centro Servizi che effettua triage e ingaggia, laddove non riesca a risolvere autonomamente il ticket aperto dall'Amministrazione, il Secondo Livello ✓Il **Secondo Livello (L2)** corrisponde al team di specialisti dello specifico servizio che operano all'interno del Cento Servizi ✓Il **Terzo Livello (L3)** corrisponde ad esperti tecnologici (resi disponibili dal RTI), che intervengono laddove necessario per la risoluzione di incident critici e/o per interventi particolarmente complessi. Inoltre, si occupa dell'eventuale coinvolgimento dei Vendor Tecnologici **(L4)**. Tutte le interazioni tra i livelli sono registrate sulla

piattaforma di ticketing, che permette il tracciamento delle richieste e, in caso di mancata risoluzione da parte dei team di supporto coinvolti, l'attivazione delle procedure di escalation e il reporting relativo su SLA e KPI.

Il Modello permette al Fornitore di **massimizzare l'efficienza** e alla PA di **accedere a tutti gli skill necessari** a seconda delle esigenze che emergeranno durante il ciclo di vita del servizio. Tutte le procedure operative sono definite con la PA durante la Presa in Carico.

6.3.4 Controllo di Qualità

Già nella presente offerta il RTI propone degli indicatori per ciascun servizio. A seguire, essi potranno essere rivisti per meglio rappresentare la qualità dei servizi. Gli Indicatori da monitorare rientrano nelle seguenti categorie: ✓**Indicatori di Qualità** (IQ) previsti negli atti di gara, eventualmente ampliati con **Indicatori di Qualità Aggiuntivi** (IQA) proposti nella presente offerta ✓**Parametri di Controllo Interno** (PCI) - collegati agli IQ/IQA per l'identificazione anticipata di potenziali rischi, non hanno impatto contrattuale ✓**Indicatori Chiave di Performance** (KPI) - valutano il contributo dei servizi al raggiungimento di obiettivi di business definiti con la PA in avvio di Fornitura in base ai Fattori Critici di Successo (CSF), non hanno impatto contrattuale ma sono funzionali ad identificare segnalazioni da presentare al Cliente.

Di seguito gli indicatori previsti per il servizio in oggetto (data la natura estremamente tecnica di questo servizio non sono applicabili KPI).

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "NEXT GENERATION FIREWALL"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSA	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta	*Data_Notifj* = Data Ora di inoltro al SOC della segnalazione *Data_Incj* = Data Ora dell'incidente TNSA = $\sum_{J=1}^{n} Data\_notifj - Data\_Incj$	Trimestre	<1 ora per il 90% degli incidenti
PCI_TNSA	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta	Come IQA_TNSA	Mensile	<1 ora per il 95% degli incidenti

6.4 Interazioni

6.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
SOC	Log di audit ed eventi	Output	I sistemi inviano log al SIEM affinché gli eventi generati dai NGFW possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo ai fine della cybersecurity e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza
Gestione continua delle vulnerabilità	Vulnerabilità in essere e potenziali	Input/ Output	Gli apparati scambiano con il servizio informazioni relative alle vulnerabilità identificate sui sistemi e relative configurazioni e ricevono informazioni in merito alla relativa criticità e prioritizzazione
Threat Int. & Vulnerability Data Feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence sono raccolti in input dai gateway FortiGate per limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash)

6.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui NGFW solo qualora fossero previsti possibili impatti di servizio.

6.5 Capacità di fornire visibilità e controllo degli utenti per creare policy, generare report ed eseguire indagini forensi

L'architettura e la tecnologia del servizio NGFW sono ideati per garantire la possibilità di avere un **controllo puntuale delle operazioni ammesse** agli utenti (in linea con il modello Zero Trust) e la possibilità di **analizzare i flussi di traffico sia a scopi di reportistica sia per esecuzione di indagini forensi** a seguito di incidenti di cybersecurity. L'implementazione di queste due macro-funzionalità è possibile mediante le tecnologie:

- **Fortinet Single Sign-On (FSSO)**, funzionalità disponibile sui gateway tramite la quale è possibile recuperare le informazioni di autenticazione degli utenti, con un approccio Agent-Based o Agentless, in modo da applicare in maniera trasparente policy user-based;

  FortiAnalyzer, elemento centrale dell'architettura che consente di analizzare e riassumere molteplici aspetti degli eventi registrati sui gateway, quali policy applicate, tentativi di accesso, performance dei dispositivi, sia a scopi reportistici che per condurre attività forensi e di risposta agli incidenti.

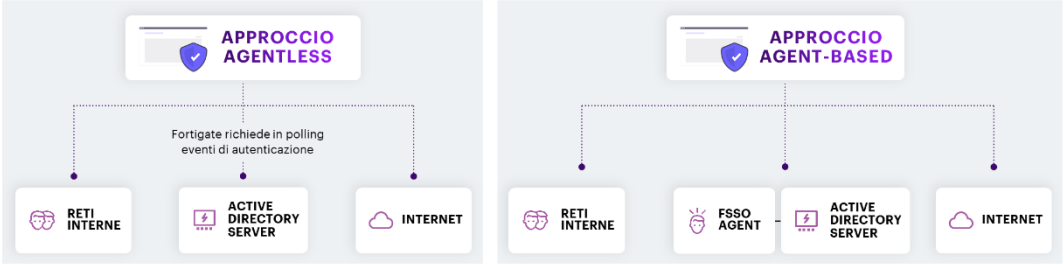


Figura 20 - Metodologie principali per implementazioni di policy basate sull'identità dell'utente

La funzionalità FSSO potrà essere implementata in diversi modi, a seconda del contesto della singola PA e dei requisiti raccolti durante la fase iniziale di ingaggio. Le modalità principali di implementazione sono le seguenti e hanno l'obiettivo di associare un IP ad una identità, al fine di applicare policy su base utente: ✓**Agentless** – il gateway è configurato in modalità polling al fine di recuperare gli eventi di autenticazione dall'identity provider o dall'identity store ✓**Agent-based** – un

FSSO agent è installato sui domain controller dell'Active Directory e inoltra gli eventi di autenticazione al Fortigate.

Esistono altre tecniche di implementazione che possono essere anche non trasparenti all'utente, come ad esempio l'autenticazione esplicita su un portale dell'appliance NGFW. Le modalità saranno ad ogni modo valutate e concordate durante la fase di attivazione del singolo CE. Si riporta in figura un esempio di applicazione di policy basata su utenti.

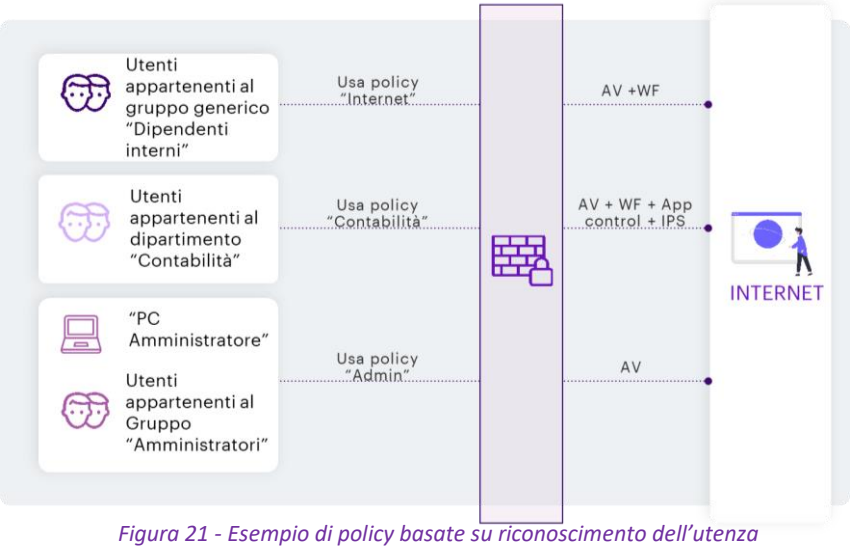


Figura 21 - Esempio di policy basate su riconoscimento dell'utenza

Le funzionalità di analisi sono assicurate centralmente mediante la piattaforma FortiAnalyzer che consente di creare ✓**Dashboard** per un monitoraggio degli eventi sia in tempo reale che storicizzati, ✓**Report** ad hoc a seconda delle esigenze. Di seguito si riportano alcuni esempi di Dashboard utili agli scopi descritti: stato degli eventi e delle minacce di sicurezza applicabili per PA, dettaglio delle regole implementate per la sicurezza di rete, elenco delle change applicate nel periodo di riferimento. Considerando il processo di Continuous Improvement, le dashboard e i report saranno personalizzabili e raffinabili, ove applicabile, secondo le esigenze delle singole PA.

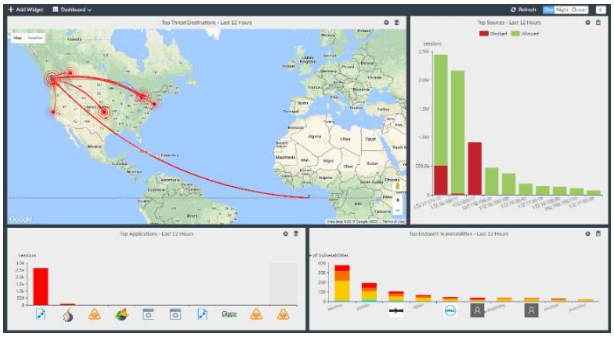
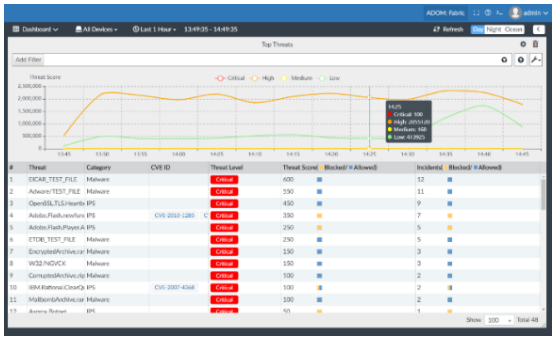
Security Monitor Dashboard	Top Threat Dashboard
	

Figura 22 - Esempi di Dashboard

7 PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL"

7.1 Soluzione Proposta

Il modello CDOM proposto (cfr. §§1 e 3.3) colloca il servizio di **Web Application Firewall** (WAF) nel dominio di sicurezza "Breach Prevention & Readiness" allineata alla Funzione NIST "Protect", riducendo così la superfice di attacco per le applicazioni web delle PA.

Il servizio **WAF** rappresenta uno dei principali asset di sicurezza del Centro Servizi, finalizzato alla protezione delle PA da attacchi veicolati ai dati delle applicazioni web, agendo da **filtro del traffico di rete** dello strato applicativo.

Le vulnerabilità delle Applicazioni Web possono portare a violazioni dei dati o al blocco di sistemi mission-critical per la PA, motivo per cui il servizio WAF proposto vuole superare i limiti dei normali Intrusion Detection System e dei tradizionali sistemi WAF che si affidano all'apprendimento delle applicazioni (manuale o automatico) per il rilevamento di anomalie e minacce. La nostra proposta adotta, invece, un approccio evoluto e completamente diverso al rilevamento delle minacce, grazie all'utilizzo un **motore di apprendimento automatico** (ML) che permette di costruire e aggiornare autonomamente un **modello di comportamento dell'utente** (Behavioral Analytics) ed utilizzare tale modello per discriminare il traffico lecito da quello malevolo, permettendo di bloccare in modo molto più efficace anche le minacce sconosciute (**exploit zero-day**). Questo nuovo approccio sfrutta, inoltre, **due livelli di apprendimento automatico**, uno basato sull'**AI** ed uno **sulle probabilità statistiche** per rilevare anomalie e minacce separatamente. Il primo livello costruisce il modello matematico per ogni parametro appreso e quindi attiva le anomalie per le richieste difformi. Il secondo verifica se l'anomalia è una minaccia reale o se si tratta di una varianza benigna (falso positivo).

Per assicurare che tutto il traffico venga correttamente protetto garantendo l'efficacia dei meccanismi di sicurezza attuati dal servizio WAF, sono previste **funzionalità di full SSL inspection (Deep Inspection)** al fine di garantire che anche il contenuto crittografato venga ispezionato dal presente servizio. Tramite le capacità di full SSL inspection è possibile proteggere le PA da tutte le tipologie di minacce, **anche se in traffico criptato** (es: https), prima di trasmettere il traffico al mittente.

Il corretto funzionamento del servizio WAF dipende, inoltre, da una coerente **interazione con tutti gli altri elementi dell'infrastruttura** e con un **modello operativo integrato**. Questo include la comprensione e la risposta agli errori e ai messaggi di allarme originati dal WAF, nonché da altri aspetti come la gestione delle modifiche alle politiche di sicurezza in concomitanza con le modifiche delle applicazioni WEB protette, garantendo così la corretta e piena disponibilità delle stesse. Si procede quindi ad integrare in modo agile il servizio WAF nel processo standard di gestione delle richieste di change per fare in modo che la distribuzione ed il test delle politiche di sicurezza avvenga prima negli ambienti non produttivi e solo successivamente in quelli di produzione. La distribuzione di specifiche firme o politiche direttamente in modalità di blocco può essere effettuata in caso di criticità o di attacco in corso, in accordo con le indicazioni di remediation ricevute dal servizio di monitoraggio di sicurezza SOC o dalle strutture di sicurezza delle PA finali. Questo assicura che l'**impatto è sempre valutato e ridotto al minimo**.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: Roma Capitale e Comune di Milano

Private: NEXI e Primario operatore finanziario

Descrizione di un caso di successo - **Roma Capitale** →**Esigenza** - Infrastruttura di sicurezza applicativa atta a proteggere il portale istituzionale di Roma Capitale →**Soluzione** – Fastweb ha realizzato un'architettura basta su FortiWeb →**Benefici** ✓facilità di migrazione di tutte le configurazioni e policy di sicurezza ✓servizi evoluti di sicurezza multi-minaccia in un'unica piattaforma di sicurezza che consente di contrastare efficacemente attacchi e minacce all'infrastruttura di rete.

7.1.1 Funzioni offerte

Il servizio prevede: un livello di **Interfaccia PA** utile all'interazione con il servizio, un livello di **Erogazione** in cui sono espletate le funzioni principali del servizio, un livello di **Automazione** (intelligent layer) che aggiunge funzioni avanzate, un livello **Interazioni** per le relazioni con gli altri servizi (cfr. §6.1.1). I livelli comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative**, descritte di seguito.

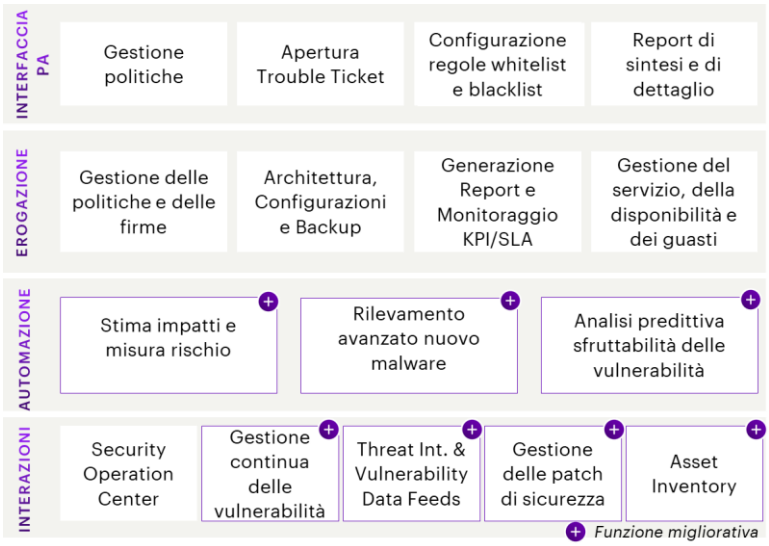


Figura 23 - Funzioni del servizio WAF

- **Stima degli impatti e misura del rischio**: la funzione esegue le stime di impatti e rischio sulle configurazioni implementate o che prevede di implementare, fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura. Tali valutazioni sono effettuate tenendo in considerazione: ✓la classificazione delle informazioni trattate, ✓la criticità del servizio abilitato per la PA, ✓le dipendenze ed interazioni con altri servizi, funzioni e sistemi.
- **Rilevamento avanzato del malware**: la funzione prevede metodi avanzati di "malware detection" fortemente potenziate dall'integrazione con il servizio di Threat Intelligence, nonché con il SOC e prevedono azioni automatizzate per isolare comportamenti di rete anomali che possono segnalare la presenza di malware noti o di possibili varianti; presenza di funzioni di "Protezione dagli attacchi DDOS - Distributed Denial of Service".
- **Analisi predittiva della sfruttabilità delle vulnerabilità**: la funzione combina dati e informazioni sulle minacce da più fonti analizzando con un algoritmo di apprendimento automatico basato su ML, per anticipare la probabilità che una vulnerabilità venga sfruttata, anche grazie all'interazione con i servizi di Gestione continua delle vulnerabilità e Threat Intelligence e Vulnerability Data Feeds.
- **Interazioni** con i servizi Threat Intelligence & Vulnerability Data Feed, Gestione continua vulnerabilità di sicurezza, Gestione delle patch di sicurezza, Asset Inventory, descritte al §7.4.1.

7.1.2 Architettura tecnologica

La soluzione tecnologica scelta dal Centro servizi prevede l'utilizzo della soluzione di WAF di Fortinet riconosciuta come leader sul mercato.

L'architettura prevista per la fornitura del servizio prevede l'integrazione del WAF, nella sua forma fisica o virtuale, localmente presso la singola PA oppure remotamente presso il Centro Servizi (scelta subordinata agli accordi con la singola PA), predisponendo una console di gestione integrata e centralizzata in esercizio presso lo stesso Centro Servizi. La scelta architetturale inerente all'installazione degli appliance presso la PA oppure remotamente presso il Centro Servizi sarà eseguita durante la fase di attivazione del servizio, subordinata alle caratteristiche dell'infrastruttura di rete della singola sede o alla lista di servizi di sicurezza WAF da attivare.

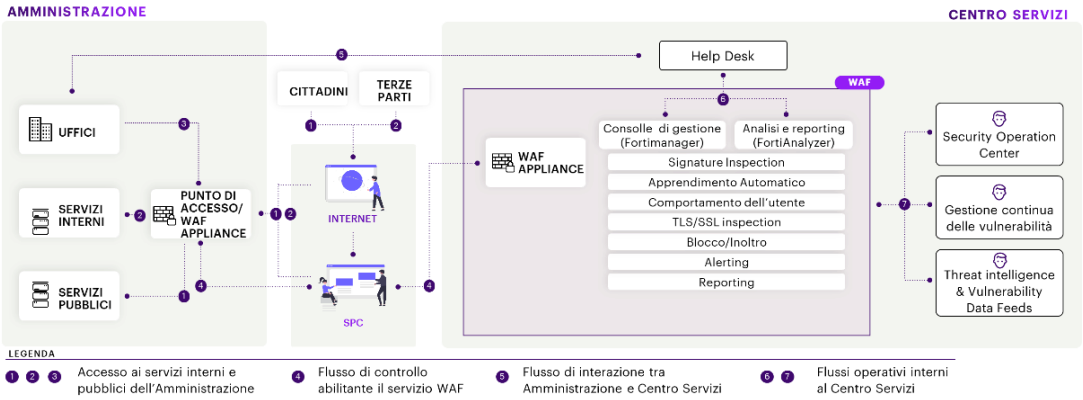


Figura 24 -Architettura tecnologica WAF

La gestione degli apparati WAF, analogamente a quanto già esposto per il servizio NGFW (cfr. §6), avviene mediante la console di gestione centrale **FortiManager** e l'ulteriore elemento centrale di analisi, logging e reporting, denominato **FortiAnalyzer**.

7.1.3 Caratteristiche tecnologiche e prestazionali migliorative

Gli apparati adottati dal servizio WAF saranno disponibili in versione chassis fisico o macchina virtuale (VM), al fine di garantire la massima flessibilità e adattabilità al contesto di rete, infrastrutturale e vincoli tecnologico/operativi. L'utilizzo di una forma piuttosto che di un'altra sarà concordata e selezionata dalla specifica PA.

La tecnologia Fortinet prescelta oltrepassa le capacità di protezione previste dal capitolato tecnico in quanto è in grado di fornire alle PA funzionalità evolute quali: ✓Approccio evoluto al **rilevamento delle minacce** che, oltre ai metodi "standard" basati su firma, sfrutta la probabilità per identificare le minacce piuttosto che eseguire corrispondenze precise con le attività osservate. ✓**ML**, che raccoglie dati su ciascun elemento dell'applicazione mentre gli utenti effettuano le normali interazioni con l'applicazione, utilizzando un modello statistico per determinare se una richiesta HTTP varia in modo significativo dalle richieste osservate in precedenza consentendo di definire delle azioni da applicare. ✓Un **ulteriore livello di apprendimento automatico** che, una volta identificata un'anomalia, determina se si tratta di una minaccia o semplicemente di una variazione benigna, come un errore di battitura, un nuovo carattere che non era stato visto in precedenza o anche un cambiamento legittimo all'applicazione stessa.

In questa proposta e in accordo con le best practice di settore, per ciascuna tipologia di applicazione e layer dello stack tecnologico sarà predefinito un set di regole di sicurezza da abilitare su ciascuna categoria di traffico. Tuttavia, sarà possibile richiedere ed evadere richieste di apertura e controllo del traffico su cui abilitare o meno determinati servizi, in accordo con gli standard della specifica PA. Inoltre, particolare importanza sarà fornita all' ottimizzazione dei processi operativi per il passaggio delle regole e delle policy tra i landscape di sviluppo e produzione per la modalità di apprendimento del traffico, tuning e blocco del traffico in modo da limitare la ricezione di alert per garantire che venga bloccato esclusivamente il traffico indesiderato (rimozione falsi positivi).

7.2 Organizzazione

7.2.1 Strutture coinvolte

Il servizio WAF è erogato da un team specializzato su servizi di sicurezza infrastrutturale ed applicativa che risponde a un **Responsabile del servizio**; il team è supportato da un **architetto** esperto su tecnologie WAF e da un **esperto** in ambito infrastrutturale.

Si propone, dunque, un servizio WAF gestito per competenze: la componente di «Platform Management» che si fa carico della gestione della parte System (versione & patch, utenze di sistema, capacity planning) e la componente di «Application Management» che si basa su un approccio application-oriented per ogni PA: supporto analisi applicative, politiche WAF, gestione delle firme, analisi dei falsi positivi e dei log.

Analogamente al servizio NGFW (cfr. §6.2.1) è previsto il supporto delle strutture CE SMART HUB e i Centri di Competenza/Partnership.

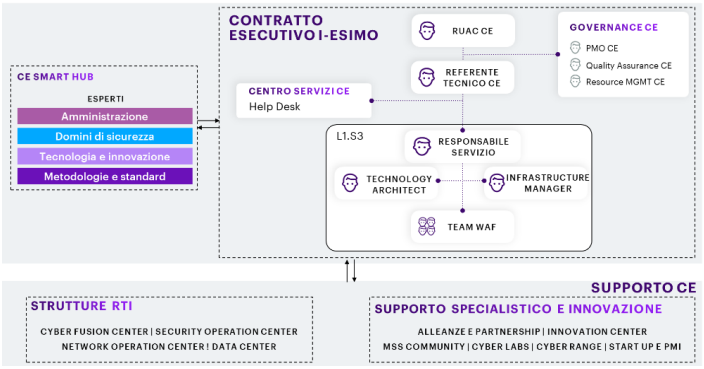


Figura 25- Strutture coinvolte nel servizio

7.2.2 Team del servizio

Di seguito sono dettagliati i ruoli organizzativi e i profili professionali che andranno a comporre il team di servizio WAF (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
Infrastructure Manager	Supporto al team WAF / Sr-ISC	Offre consulenza per le attività tecniche e di design riguardante la parte puramente infrastrutturale.
Technology Architect	Supporto al team WAF / SSA	Offre consulenza in ambito architetturale alla PA, ha una conoscenza approfondita del contesto e partecipa alla fase di analisi e di pianificazione delle attività.
WAF team	L2 Security Engineer / Sr-ISC	Supporta e integra le attività del L1 Security Engineer e definisce il design della soluzione supportato dal Supporto al team WAF e configura la soluzione.
WAF team	L1 Security Engineer / Jr-ISC	Registra il ticket e ne assegna la priorità, eseguendo l'analisi e la diagnosi iniziale. Esegue procedure per la risoluzione dei ticket o l'applicazione di workaround, attivando eventualmente procedure di escalation.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

7.3 Modello operativo

7.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

Figura 26 - Modello operativo servizio WAF

7.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di **Configurazione** ed **Erogazione** specifiche per il servizio in oggetto. Per le fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

CONFIGURAZIONE	
Installazione e setup	**Deliverable**: N/A **Descrizione**: All'interno di questo processo rientrano: ✓Consegna dell'apparato presso la PA (consegna fisica o OVA) ✓Setup iniziale HW (rack & stack) o vHW (deployment virtual appliance) ✓Setup configurazione (major and minor version, patches, interfaccia management) ✓Integrazione nella rete della PA ✓Integrazione con le piattaforme centralizzate
Configurazione e messa in produzione	**Deliverable**: N/A **Descrizione**: All'interno di questo processo rientrano: ✓Configurazione delle policy standard e dei profili d'ispezione ✓Configurazioni specifiche rispetto al CE, eventuale porting di configurazioni da appliance esistenti ✓Test della configurazione ✓Passaggio in produzione ed eventuale swap da sistemi pre-esistenti ✓Tuning delle funzionalità attivate ✓Supporto post passaggio in produzione

EROGAZIONE	
Gestione ciclo di vita policy	**Deliverable**: N/A **Descrizione**: ✓Creazione e modifica di policy di sicurezza ✓Estrazione informazioni quali esportazione di log, accessi, policy attive o procedure in essere
Operation	**Deliverable**: Report attività manutenzione **Descrizione**: Gestione di incidenti o problemi mediante: ✓l'applicazione di soluzioni permanenti utili a risolvere l'incidente ✓l'applicazione di workaround e analisi successiva della root cause per l'eliminazione definitiva di incidenti e problemi ✓Applicazione di aggiornamenti software, hotfix, operazioni di riavvio di specifici processi applicativi ✓Verifica funzionalità di base per alta affidabilità, backup e monitoraggio infrastrutturale

EROGAZIONE	
Reporting	Generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF

7.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano di seguito gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO WEB APPLICATION FIREWALL				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSW	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta per il servizio WAF	*Data_Notifj* = Data Ora di inoltro al SOC della segnalazione *Data_Incj* = Data Ora dell'incidente TNSA = $\sum_{J=1}^{n} Data\_notifj - Data\_Incj$	Trimestre	<1 ora per il 90% degli incidenti
PCI_TNSW	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta per il servizio WAF	Come IQA_TNSW	Mensile	<1 ora per il 95% degli incidenti
KPI_NABB	Numero di accessi da IP in blacklist bloccati	Numero di attacchi bloccati (include sia accessi da IP in blacklist che mancato rispetto di regole logiche)	Trimestre	Incremento < 50% rispetto alla rilevazione precedente

7.4 Interazioni

7.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione / Finalità
SOC	Eventi analizzati dal WAF	Output	Integrazione funzionale e tecnica delle piattaforme WAF e SIEM volta a consentire l'invio dei log al SIEM affinché gli alert di sicurezza generati dai WAF possano essere analizzati e correlati in real-time con gli eventi degli altri sistemi delle singole PA al fine di rilevare situazioni di rilievo ai fine della cybersecurity e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza.
Threat Int. & Vulnerability Data Feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence potranno essere raccolti in input dai WAF Fortinet al fine di limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash) in modalità preventiva e non solamente reattiva a seguito di un attacco.
Gestione cont. vulnerabilità di sicurezza	Vulnerabilità in essere e potenziali	Input/ Output	Gli apparati scambiano con il servizio informazioni relative alle vulnerabilità identificate sui sistemi e relative configurazioni e ricevono informazioni in merito alla relativa criticità e prioritizzazione
Gestione delle patch di sicurezza	Da Patch Management a WAF	Input	Per quelle applicazioni, laddove non è presente una patch ad una specifica vulnerabilità di sicurezza, si potrà effettuare l'enforcement tramite il servizio WAF per mitigare il rischio di impatto della vulnerabilità (virtual patching).
Asset Inventory	Da CMDB a WAF	Input	Ove presente una soluzione di Asset Inventory presso le PA, l'integrazione abilita la gestione centralizzata dell'asset, la compliance e i processi di patch management. L'integrazione sarà sia funzionale che tecnica delle piattaforme, volta a consentire l'acquisizione delle informazioni.

7.4.2 Reporting per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui WAF solo qualora fossero previsti possibili impatti di servizio e analisi della protezione applicata alle applicazioni. Esempi di report disponibili: PCI Reports, Attack Activity, Traffic Activity e Event activity.

7.5 Protezione da exploit zero-day, infezioni da malware e vulnerabilità

In aggiunta agli aspetti sopra indicati, il servizio WAF introduce anche le seguenti funzionalità, fondamentali per la protezione da exploit zero-day: ML, Rilevamento bot e Sandbox.

7.5.1 Machine learning

Il servizio WAF, tramite la tecnologia individuata, offre una funzione di apprendimento automatico che consente di rilevare il **traffico Web dannoso e i bot** (FortiWeb). Oltre a rilevare attacchi noti, la funzione è in grado di rilevare potenziali attacchi zero-day sconosciuti per fornire protezione in tempo reale per i server Web. Il modello di rilevamento delle anomalie della funzionalità di apprendimento automatico osserva gli URL, i parametri e il metodo HTTP delle sessioni HTTP e/o HTTPS che passano ai server web e costruisce modelli matematici per rilevare il traffico anomalo. FortiWeb utilizza due livelli di apprendimento automatico per rilevare attacchi dannosi. Il primo livello utilizza l'Hidden Markov Model (HMM) e monitora l'accesso all'applicazione e raccoglie dati per costruire un modello matematico dietro ogni parametro e metodo HTTP. Una volta completata, verifica ogni richiesta rispetto al modello per determinare se si tratta di un'anomalia o meno. Una volta che il primo livello di apprendimento automatico rileva una richiesta come anomala, viene attivato il secondo livello di apprendimento automatico per verificare se si tratta di un attacco reale o solo di un'anomalia benigna che dovrebbe essere ignorata. Per fare ciò, FortiWeb include modelli di minacce

addestrati (reti neurali) predefiniti. Ciascuno rappresenta una determinata categoria di attacco, come SQL Injection, Cross-site Scripting e così via. Ogni modello di minaccia è già addestrato sulla base dell'analisi di migliaia di campioni di attacco. I modelli di minaccia vengono continuamente aggiornati utilizzando il servizio di sicurezza FortiWeb. Quando vengono rilasciati nuovi tipi di attacco, il team FortiGuard analizza le nuove minacce e riqualifica il modello di minaccia pertinente. Il nuovo modello di minaccia viene quindi inviato a tutte le installazioni dei clienti in modo simile a come vengono aggiornate le firme.

7.5.2 Rilevamento bot

Il modello di rilevamento dei bot di apprendimento automatico basato sull'AI integra le regole esistenti basate su firme e soglie. Rileva bot sofisticati che a volte possono passare inosservati. Il modello di rilevamento dei bot osserva i comportamenti degli utenti da tredici dimensioni, ad es. quante volte le richieste HTTP vengono avviate dall'utente, se la richiesta utilizza versioni HTTP illegali, se recupera risorse JSON/XML.

Rispetto ai meccanismi tradizionali per rilevare i bot, il modello di rilevamento dei bot semplifica il tuning della soglia appropriata per rilevare comportamenti anomali degli utenti. In particolare, per sapere quante volte le richieste HTTP avviate da un utente devono essere considerate anomale, con il meccanismo tradizionale, potrebbe essere necessario sperimentare diversi valori di soglia e controllare continuamente il registro degli attacchi fino a quando non vengono riportati registri degli attacchi correlati per il traffico normale. Pertanto, FortiWeb utilizza un algoritmo basato SVM (Support Vector Machine) per creare il modello di rilevamento dei bot che autoapprende i profili di traffico dei client regolari. Quando arriva il traffico di un nuovo client, viene confrontato con quello dei client normali. Se non corrispondono, il modello consente di classificare il nuovo client come un'anomalia. Quando i profili di traffico dei client regolari variano notevolmente, FortiWeb aggiorna automaticamente il modello per adattarsi ai cambiamenti.

7.5.3 Sandbox

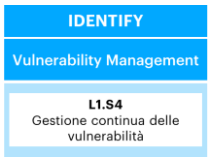
Il servizio FortiSandbox è una soluzione software sandbox che consente un accesso completo alla configurazione della stessa e invii illimitati per l'ispezione di oggetti sospetti o classificati come tali. Lla soluzione presenta i seguenti benefici: ✓**Riduzione dei rischi**. Con una sandbox dedicata basata sull'AI, si hanno a disposizione risultati in pochi minuti e non in ore, il che è fondamentale per ridurre il successo degli attacchi nell'odierno panorama delle minacce in continua evoluzione. ✓**Scalabilità**. Ridimensionamento della capacità di sandbox attraverso l'aggiunta di VM. ✓**Maggiore efficienza**. Integrazione del sandboxing nell'infrastruttura di sicurezza per automatizzare la protezione dalle violazioni senza la necessità di un team di sicurezza IT dedicato per monitorare costantemente le minacce.

8 PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL" – FUNZIONALITÀ AGGIUNTIVE

Con riferimento al servizio di "web application firewall" (di cui al par. 3.1.3 del Capitolato Tecnico speciale), il Raggruppamento conferma la presenza di funzioni di "Protezione dagli attacchi DDOS - Distributed Denial of Service".

9 PROPOSTA PROGETTUALE PER IL SERVIZIO "GESTIONE CONTINUA DELLE VULNERABILITÀ DI SICUREZZA"

9.1 Soluzione proposta



Il **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di Gestione continua delle vulnerabilità di sicurezza nel dominio di sicurezza "Vulnerability Management", riconducibile alla Funzione NIST "Identify". Il servizio in oggetto ha lo scopo di rilevare, monitorare e ridurre la superfice d'attacco esposta dalle PA contraenti. La nostra esperienza su vasta scala ci ha consentito di consolidare ed evolvere un **modello di servizio proprietario** che arricchisce ed estende la gestione dell'intero ciclo di vita delle vulnerabilità attraverso l'adozione di una **piattaforma TVMP (Threat and Vulnerability Management Platform)**, dispiegata c/o il Centro Servizi e integrata con altri sistemi di controllo (SIEM/SOAR, Threat Intelligence, NGFW/WAF, Asset Inventory/CMDB ove presenti), alla quale accede esclusivamente personale altamente qualificato e certificato (SANS, GEVA/GXPN, OSCP, OSCE, CEH, OPST, etc.). La proposta per il servizio si connota per le seguenti **caratteristiche distintive**: ✓Rilevazione delle vulnerabilità presenti in sistemi, apparati di rete, applicazioni (web, mobile, client-server, etc.), dispositivi ad uso professionale e personale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MITRE kill-chain, etc.) capaci di sfruttarle; la fase di ricerca delle vulnerabilità agevola peraltro la ricostruzione (ove non presente) di un 'Asset Inventory' (con CCE e CPE) del patrimonio informativo delle PA ai fini della successiva **misura del livello di esposizione alla minaccia cyber associato ai singoli cespiti IT**; inoltre, l'integrazione con le piattaforme di Cyber Threat Intelligence (es. TIS e iDefense) rende più profonda la ricerca di nuove vulnerabilità sulla base delle **evidenze predittive** prodotte degli analisti (artifact, IoC, IoA, etc.) anche se non note alla community (es. CVE); ✓Categorizzazione, classificazione e misura del potenziale impatto delle vulnerabilità rilevate, sulla base della misura del rischio ponderato con il livello di criticità associato all'asset e derivante dalla **rilevanza dei processi** della PA che l'asset abilita, dalla **sensibilità dei dati trattati** e delle **interdipendenze** (con altre funzioni e/o sistemi), unitamente alle indicazioni sulle modalità tecniche, organizzative e procedurali di risoluzione (o mitigazione) delle problematiche riscontrate; ✓**Pianificazione, su base priorità** (stante la misura del rischio residuo corrente), delle azioni di risoluzione o mitigazione delle problematiche di sicurezza individuate e delle fasi di controllo orientate al rientro dalle non conformità e al miglioramento continuo; ✓**Supporto tecnico-organizzativo** e **tecnico-funzionale,** come nel seguito descritti; ✓Reportistica relativa alle scansioni con un alto grado di personalizzazione di elementi quali: superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: circa 40 tra cui Azienda ULSS4 VENETO, IPZS, ENAC, MIUR, Agenzia delle Entrate, Università studi di Cagliari, Comune di Lecce

Private: Intesa Sanpaolo, ENEL, ENI, Poste Italiane, NEXI, Primario operatore finanziario

Descrizione di un caso di successo - **Azienda ULSS4 VENETO** →**Esigenza** - Indirizzare un ampio numero di misure minime di sicurezza AgID →**Soluzione** -Fastweb ha erogato un servizio avanzato di Asset Discovery & Profiling, Vulnerability Management costruito ad hoc, basato sulla piattaforma Qualys →**Benefici** ✓indirizzamento dei primi 4 AgID Basic Security Controls (ABSC) in contesti con decine di migliaia di host ✓verifica che tutte le conformità, una volta raggiunte, vengano nel tempo mantenute, evidenziando eventuali non conformità ✓processo di "Automated Asset Discovery" che, scansionando costantemente lo spazio di indirizzamento IP, consente di automatizzare il processo di inventario.

9.1.1 Funzioni offerte

Il servizio prevede i 4 livelli, già presentati al §6.1.1, che comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative** utili anche a supportare le Amministrazioni nelle fasi di progressiva riduzione della superficie d'attacco. Le migliorative sono di seguito descritte.

Figura 27 - Funzioni del servizio Gestione cont. vulnerabilità di sicurezza

- **Gestione dei piani e configurazione scansioni**: raccolta ed utilizzo delle informazioni secondo profili di utenza diversi, tramite un'interfaccia grafica e/o API.
- **Conduzione del servizio**: è previsto **supporto tecnico-organizzativo** volto al controllo dello stato d'avanzamento dei piani di rientro (include esecuzione controlli tecnici di '**re-check**' sulla persistenza delle vulnerabilità riscontrate) e **supporto tecnico-funzionale** per la risoluzione o mitigazione delle problematiche di sicurezza individuate (es. hardening, bug fixing, upgrading, fine tuning, replatforming).
- **Rendicontazione direzionale e rapporti tecnici***:* La funzione espone interfacce per consultazione, archiviazione, ricerca e download dei rapporti redatti al termine di ciascuna scansione (on-demand, pianificata, campagna, **re-check**, etc.). È prevista la stesura di un rapporto tecnico con le evidenze oggettive sulle vulnerabilità riscontrate e di una rendicontazione direzionale. La classificazione delle vulnerabilità si avvale di un modello di rischio basato sullo **standard CVSS**, che, tenendo conto di diversi fattori (es. vettore di attacco, complessità dell'attacco, livello dei privilegi richiesti, criticità dell'asset vulnerabile), assegna un punteggio ed un conseguente livello di rischio su 4 livelli (Low, Medium, High, Critical). Il TVM team (cfr. §9.2) su richiesta della PA può monetizzare il rischio residuo attraverso un'analisi quantitativa che si avvale degli output prodotti della funzione '**Stima degli impatti e misura del rischio'.** Nei rapporti sono altresì indicate le **azioni di rientro** volte alla risoluzione o mitigazione delle problematiche riscontrate con una **stima quantitativa degli interventi.**
- **Analisi e correlazione di vulnerabilità**: La funzione consente di ricostruire un contesto nel quale le vulnerabilità sono analizzate sia puntualmente che nel complesso al fine di identificare le potenziali **kill-chain** cui la PA potrebbe essere soggetta.
- **Classificazione dinamica degli asset**: La funzione consente di aggregare gli asset sulla base di una o più caratteristiche (es. sistema operativo, porte esposte e servizi). Le viste generate da questa classificazione consentono di ridurre notevolmente il tempo di gestione delle vulnerabilità in quanto abilitano campagne di patching, bug fixing, hardening, upgrading, fine tuning, replatforming mirate ed efficaci.
- **Stima degli impatti e misura del rischio***:* La funzione esegue le stime di impatto e rischio, informazioni oggetto poi di visualizzazione in tempo reale e/o tramite report periodici grazie ai canali di Interfaccia. Gli asset vulnerabili sono analizzati considerando: ✓la classificazione delle informazioni che trattano ✓la criticità del servizio che abilitano per la PA ✓le dipendenze/interazioni con altri servizi, funzioni e sistemi.
- **Rilevamento avanzato del malware**: La funzione prevede metodi avanzati di 'malware detection' che aumentano l'efficacia dei risultati delle scansioni individuando una serie di evidenze, correlate o correlabili, tali da rappresentare contesti nei quali potrebbero essere potenzialmente presenti tipologie note di malware, di potenziali varianti o di nuovo malware.
- **Analisi predittiva della sfruttabilità delle vulnerabilità**: La funzione combina dati e informazioni sulle minacce da più fonti analizzando con un algoritmo di apprendimento automatico basato su ML, per anticipare la probabilità che una vulnerabilità venga sfruttata.
- **Interazioni** con i servizi Security Operation Center, CMDB/Asset Inventory, Next Generation Firewall e Web Application Firewall, descritte al §9.4.1.

Cruscotti e viste personalizzabili

CRUSCOTTI DINAMICI - La funzione "Cruscotti dinamici personalizzabili" espone **cruscotti dinamici** sullo stato della sicurezza, personalizzabili in base alle esigenze della singola PA e accessibili da una console centralizzata della TVMP. Tali **cruscotti** sono sistematicamente aggiornati **(Real-Time dashboard)** al fine di **monitorare la superficie d'attacco in tempo reale**. Nell'ambito delle personalizzazioni già previste in base all'esperienza del RTI, sono disponibili **template e baseline di riferimento** che possono essere **arricchiti** con ✓indicatori ad hoc e aggregazioni/scomposizioni (es. geografiche e settoriali) ✓rappresentazioni grafiche per il **monitoraggio del patrimonio informativo nelle sue diverse categorizzazioni** (dispositivi, reti, infrastrutture, sistemi, dati, identità, ecc.), differenziate per livelli di utenza. Il cruscotto dinamico, in particolare, offre **di default** la possibilità di: ✓visualizzare graficamente i risultati delle singole scansioni ✓aggregarli per ottenere informazioni statistiche sulle vulnerabilità più frequenti e individuare quelle più rischiose ✓analizzare lo storico per valutare lo stato delle singole vulnerabilità nel tempo sullo specifico sistema informativo ✓disporre di una vista generale sul livello di esposizione delle PA, interagire direttamente con altri servizi (es. SOC per trouble ticketing, patch management, etc.) ✓classificare gli asset per tipologia (es. sistema operativo, database, app) ✓prioritizzare le vulnerabilità includendo 'feed' di threat intelligence, etc.

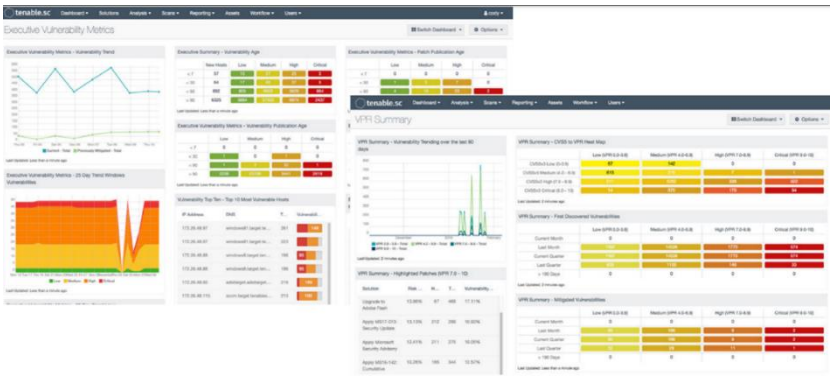


Figura 28 – Esempio Cruscotti dinamici

CRUSCOTTO DI 'ENTERPRISE RISK MONITORING' - AGGIUNTIVO - Si prevede, inoltre, l'apporto del TVM team (cfr. §9.2) per la realizzazione e l'aggiornamento di un **cruscotto aggiuntivo di 'Enterprise Risk Monitoring'** per la singola PA, nel quale la misura del rischio (che può stimarsi sia qualitativamente che quantitativamente) non sia limitata agli asset IT vulnerabili ma **afferisca ai processi e ai servizi** della PA abilitati da tali asset. Questa rappresentazione, mantenuta costantemente aggiornata, diviene fondamentale per supportare adeguatamente il percorso decisionale, nelle diverse PA, sia della dirigenza sia del personale tecnico

preposto alla sicurezza, dal momento che: ✓**favorisce** la corretta interpretazione dei rischi (monetizzati e non livellati) ✓**agevola** una miglior comprensione della superficie d'attacco esposta (processi/servizi e non asset IT) ✓**guida** l'assegnazione della priorità ai piani di rientro (suggerendo e stimando gli interventi necessari). Il TVM si renderà disponibile a personalizzare le viste per le singole PA contraenti.

Per **entrambi i cruscotti**, l'accesso sarà profilato e basato su ruoli/gruppi con diversi livelli e coni di visibilità. Le viste e le infografiche presenti nei cruscotti saranno esportabili su file, coerentemente ai profili d'accesso attivati presso le diverse PA. Le **esigenze di personalizzazione** saranno formalizzate in **requisiti, specifiche e mock-up** presentati alla PA e, una volta approvati, rilasciati in ambiente di produzione a integrazione delle viste sopra descritte.

Figura 29 – Esempio cruscotto di 'Enterprise Risk Monitoring'

CONTEXTUAL KNOWELDGE BASE - AGGIUNTIVA - Il TVM provvederà inoltre a rendere disponibile e aggiornare sistematicamente una **Contextual knowledge base** (CKB) con le casistiche e le migliori pratiche applicate per le diverse classi di vulnerabilità riscontrate e risolte sulle singole PA: in un'ottica di 'information sharing', ciascuna PA avrà la possibilità di pubblicare sul Portale di Fornitura, in toto o in parte, la propria CKB e renderla pertanto visibile alle altre PA, con le quali attivare anche confronti in modalità social (cfr. §16.2).

9.1.2 Architettura tecnologica

L'architettura della piattaforma TVMP riportata in figura 30 (integrata con tecnologia Tenable) che abilita il servizio è composta dalle seguenti componenti principali: ✓Una sonda fisica o virtuale**,** da installare nell'infrastruttura della PA contraente qualora necessaria per raggiungere gli asset target, per l'esecuzione delle scansioni verso gli apparati di rete, gli host, i server, le applicazioni web, i database e tutti i dispositivi dotati di un indirizzo IP presenti nelle reti in perimetro; se necessaria la sonda sarà connessa alla rete della PA e sarà abilitata a comunicare verso tutte le porte TCP e UDP dei i sistemi informativi presenti nelle reti in perimetro per eseguire le scansioni. ✓Una **console di gestione,** installata presso il Centro Servizi, da cui è possibile pianificare le analisi infrastrutturali e applicative, visualizzare i risultati e gestire la reportistica per mantenere una visione complessiva dello stato di esposizione delle singole Amministrazioni; la console di gestione comunica con le sonde tramite una connessione VPN. ✓Una **console per il dashboarding avanzato e l'automazione**, installata presso il Centro Servizi, per la configurazione e la gestione remota delle sonde; la console di gestione comunica con le sonde tramite una connessione VPN. ✓Un **modulo di supporto** con acceleratori e strumenti di diagnostica per l'esecuzione delle scansioni manuali, le analisi delle evidenze e la rappresentazione dei risultati. ✓Un **modulo di monitoraggio del rischio** calcolato sui **processi**. ✓Una **knowledge base contestualizzata** e aperta all'**information sharing**.

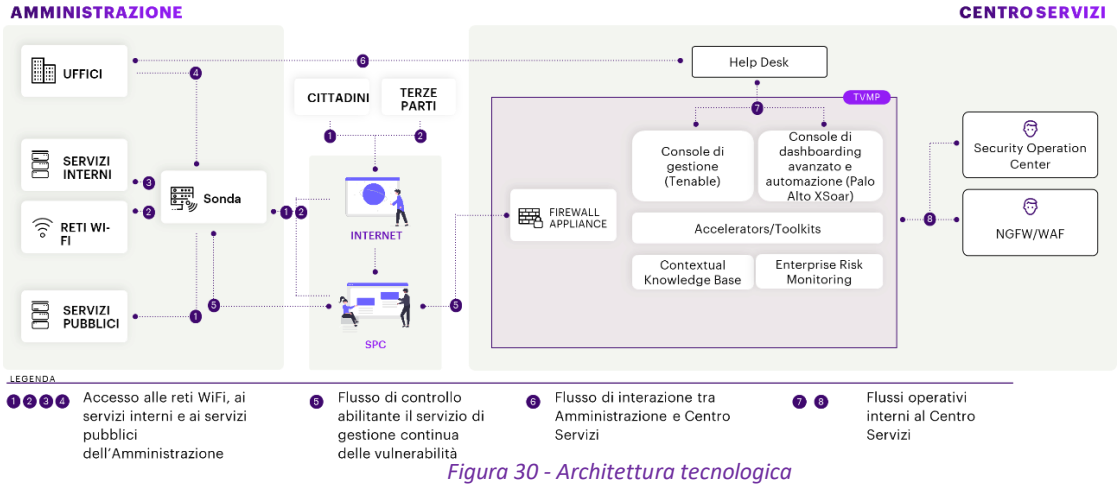


Figura 30 - Architettura tecnologica

9.2 Organizzazione

Nel contesto della struttura-tipo presentata al §6.2.1, il servizio è erogato da un unico gruppo di lavoro denominato **Threat and Vulnerability Management (TVM) Team**, che risponde a un **Responsabile del servizio**, il quale rappresenta il punto di contatto tra il TVM Team e l'Amministrazione ed è supportato da uno **SME** (Subject Matter Expert), esperto nell'ambito della Cyber Security. Il TVM Team viene di seguito descritto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
Automazione e integrazione	Resp. attività di integrazione / SSA	Gestisce le integrazioni del Centro Servizi in base alle esigenze delle singole PA, coordina le attività tra i team per l'aggiornamento e il miglioramento continuo con l'obiettivo di aumentare il livello di automazione del servizio
Gestione delle vulnerabilità	Resp. attività di gestione continua delle vulnerabilità di sicurezza / Sr-ISC	Configura gli strumenti software, gestisce le politiche di scansione e predispone le dashboard/cruscotti dinamici per le PA. Supervisiona le attività del team "Verifiche di sicurezza". Fornisce il supporto tecnico-funzionale per la risoluzione o mitigazione delle problematiche di sicurezza individuate (hardening, bug fixing, upgrading, fine tuning, replatforming, etc.)
Verifiche di sicurezza	Resp. attività di verifica di sicurezza / Jr-ISC	Esegue le attività di scansione, analizza i risultati e predispone i report executive e tecnici per ciascuna attività commissionata dalle Amministrazioni.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

Sempre in analogia con il §6.2.1, il Team del servizio è supportato ✓dal **CE Smart Hub** (es. per identificare in dettaglio le tecnologie critiche in uso presso la PA allo scopo di meglio contestualizzare i feed di Vulnerability) ✓dai **Centri di competenza** della rete di CyberFusion Center altamente specializzati nella ricerca e mitigazione di vulnerabilità ad alta complessità.

9.3 Modello operativo

9.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

Figura 31 - Modello operativo

9.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di **Configurazione** ed **Erogazione** specifiche per il servizio in oggetto. Per la descrizione delle fasi di **Attivazione** e **Chiusura** vale quanto decritto al §6.3.2.

CONFIGURAZIONE	
Deliverable: Pianificazione delle attività e personalizzazione del cruscotto dinamico (Real time Dashboard) / Specifiche di configurazione	
Predisposizione Configurazione	Descrizione: ✓definizione configurazione della sonda ✓Personalizzazione del cruscotto per raccogliere e monitorare i risultati ✓Definizione delle politiche di scansione ✓Selezione del perimetro di intervento ✓Pianificazione dell'attività
Procedura di Configurazione	L'installazione e configurazione della sonda sarà definita durante la presa in carico del servizio e prevede: ✓Un meeting di kick-off ✓L'installazione della sonda, che avverrà di concerto con i tecnici della PA nel caso in cui la sonda debba essere allocata presso un data center della PA ✓La configurazione della sonda sarà effettuata dal RTI
	Personalizzazione del cruscotto: ✓Definizione dell'entità sulla console centralizzata per la gestione della PA ✓Predisposizione delle viste in base alle esigenze della PA ✓Integrazione con il SOC che effettua il monitoraggio continuo delle vulnerabilità
Pianificazione	Pianificazione delle attività che include la redazione del Piano di Scansione

EROGAZIONE	
Deliverable: Report scansioni	
Verifica di sicurezza	Descrizione: L'erogazione rappresenta l'attività operativa durante la quale il servizio verificherà, attraverso le attività di scansione, la presenza di vulnerabilità per gli IP inclusi nel perimetro concordato con la PA. Le evidenze ottenute saranno rendicontate in appositi rapporti (tecnici e direzionali) e pubblicate sul Cruscotto dedicato alla PA contraente per consultazioni in tempo reale.
Esecuzione attività di verifica	Definizione campagna di scansione prevede: ✓Impostazione e configurazione delle policy di scansione sulla console centralizzata ✓Identificazione di reti / sistemi informativi in perimetro ✓Dry-Run tramite una scansione on-demand di prova su un sottoinsieme di sistemi informativi concordati ✓Pianificazione delle campagne di assessment sulla console centralizzata.
	Analisi risultati include: ✓Analisi delle evidenze ed approfondimenti del personale qualificato ✓Eliminazione dei falsi positivi.
	Il reporting include: ✓Executive report ✓Custom report, con associato supporto per eventuali richieste di chiarimento o approfondimento sui risultati della verifica effettuata e per le azioni di rientro volte al trattamento delle vulnerabilità riscontrate.
Integrazione e Cruscotti	Aggiornamento dashboard e integrazione: ✓Aggiornamento della dashboard (cruscotti dinamici) sulla console centralizzata ✓Integrazione con i sistemi del SOC per il monitoraggio continuo delle vulnerabilità.

9.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto:

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO GESTIONE CONTINUA DELLE VULNERABILITÀ DI SICUREZZA				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_PSV	Puntualità nella erogazione delle scansioni di vulnerabilità	Numero scansioni erogate nei tempi previsti / Numero scansioni pianificate da effettuare	Trimestre	85%
PCI_RICD	Num. giorni lavorativi di ritardo nella consegna di documentazione	Come RICD ma con frequenza maggiore e soglia più sfidante	Mensile	RICD = 0
KPI_NVGC	Numero di vulnerabilità rilevate	Numero di vulnerabilità rilevate dal servizio	Trimestre	Incremento<10% risp. rilev. precedente

9.4 Interazioni

9.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
SOC	Vulnerabilità	Output	L'integrazione tra la console di Tenable e il sistema SOAR Palo Alto Cortex XSoar consente a quest'ultimo di importare le vulnerabilità e arricchire Dashboard personalizzate per la gestione e il monitoraggio continuo delle vulnerabilità
Next Gen. e Web Application Firewall	Regole Firewall	Output	Configurazione delle regole firewall necessarie per la raggiungibilità del perimetro da sottoporre a scansione
CMDB/Asset Inventory	Asset	Input	Ove presente una soluzione di Asset Inventory presso le PA, input dei sistemi oggetto di scansione per la valutazione di riservatezza, integrità e disponibilità dei dati trattati dall'asset e la rilevanza del servizio della PA che abilitano

9.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive report da	A ogni	L'Executive report include come **elemento migliorativo** una vista di sintesi dell'esposizione alle minacce, delle analisi

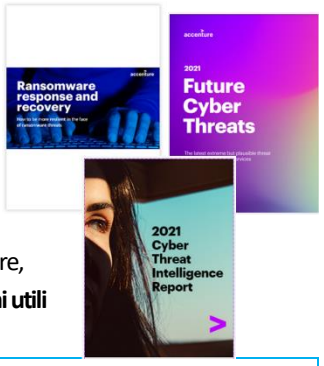
Capitolato	scansione	dei potenziali impatti e del livello di rischio sui processi dell'Amministrazione
Custom report da Capitolato	A ogni scansione	Il Custom report include come **elementi migliorativi**: ✓l'approfondimento tecnico sulle vulnerabilità individuate con ricostruzione delle potenziali kill-chain correlabili ✓le azioni tecnico-organizzative ed il piano di rientro da intraprendere per gestire le vulnerabilità con stima dell'impegno e competenze necessarie
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui NGFW solo qualora fossero previsti possibili impatti di servizio

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

10.1 Soluzione Proposta

Il **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di Threat Intelligence & Vulnerability Data Feed (**TI&VDF**) nel dominio di sicurezza "Threat intelligence" (TI) riconducibile alla **Funzione NIST "Identify"**. Il servizio in oggetto è erogato dal Centro Servizi avvalendosi della piattaforma **piattaforma Threat Intelligence Service (TIS)**, sviluppata e gestita da Accenture che, a sua volta integra il servizio specialistico **iDefense** di Accenture che prevede l'accesso tramite interfaccia Intelgraph e API alle informazioni di intelligence che coprono le vulnerabilità di oltre 1.000 vendor, strumenti e tecniche malware, Indicatori di Compromissione, organizzazioni target, threat actor e loro motivazioni, campagne di phishing e minacce pertinenti l'organizzazione aziendale. Il servizio è reso disponibile tramite **una interfaccia web e accesso API** e si integra con il servizio di SOC di cui costituisce sia un provider informativo utile alla conduzione di indagini di sicurezza. La piattaforma fornisce informative complete e continuative (feed) relative alle minacce e vulnerabilità di sicurezza, specificamente adattate alle PA, grazie alla possibilità di utilizzare un'**ampia quantità di fonti informative OSINT** (Open Source Intelligence ad accesso libero) e **CLOSINT** (Closed Source Intelligence non liberamente disponibili). Il servizio è erogato da **oltre 10 anni** ad una molteplicità di Clienti operanti a **livello nazionale e internazionale** sui principali mercati di riferimento. **Fattore distintivo** del servizio è la possibilità di far leva su competenze e centri di ricerca di Accenture riconosciuti **a livello internazionale** che abilitano l'accesso a fonti informative necessarie per interpretare i fenomeni di sicurezza anche per il mercato italiano, spesso legati a minacce di sicurezza generate da gruppi che operano in paesi terzi. I centri di ricerca di Accenture, in tal senso, sono **riconosciuti a livello internazionale** e, con cadenza periodica, rilasciano **report di interpretazione dei fenomeni utili alla Security Community dei Clienti (Sitrep),** alcuni esempi in figura.

Figura 32 - Interfaccia web iDefense - Intelgraph



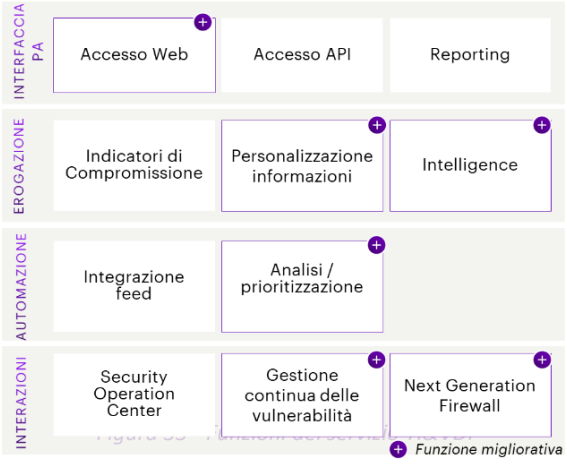
Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Private: Primario operatore delle Telecomunicazioni, Unicredit, ENI, CARIGE

Descrizione di un caso di successo - Primario operatore delle Telecomunicazioni →Esigenza - Supporto per la gestione proattiva delle minacce e delle vulnerabilità di sicurezza al fine di fornire informazioni più approfondite e aggiornate in tempo reale al servizio SOC e migliorare così le attività di threat hunting e il blocco preventivo degli IoC →**Soluzione** - attivazione per la raccolta di feed di Threat Intelligence e Vulnerability per fornire al Cliente le informazioni più aggiornate su campagne di attacco che interessano il settore e l'area geografica di riferimento, vulnerabilità che impattano le tecnologie in uso, IoC per i sistemi di Intrusion Prevention e Intrusion Detection →**Benefici** - Maggiore visibilità sui diversi tipi di minacce che potrebbero impattare il brand, prima ancora che gli eventi di abuso si verifichino, grazie ad una migliorata proattività nel contrasto a tali minacce.

10.1.1 Funzioni offerte

Il servizio **TI&VDF** consente di elaborare ed estrarre le informazioni necessarie attraverso le funzionalità offerte, articolate nei livelli riportati in figura (cfr. §6.1.1). Tali livelli comprendono tutte le funzionalità richieste dal Capitolato e ne aggiungono alcune **migliorative**, di seguito descritte.



- **Accesso web:** la piattaforma integra l'interfaccia Intelgraph che si basa su un modello di rappresentazione dei dati che consente agli analisti di mettere in relazione nodi di informazioni su threat actor, malware, vulnerabilità, campagne, target, domini, e-mail di phishing, ecc. Tale struttura di dati consente un accesso più rapido ai dati rilevanti e la capacità di visualizzare le relazioni tra i diversi dati;
- **Personalizzazione delle informazioni:** la piattaforma consente di personalizzare le informazioni richieste dalla PA in funzione dei sistemi adottati. Tramite l'interfaccia è possibile consultare i bollettini predisposti dal team di Threat Intelligence (**TI**) e generare report personalizzati;
- **Intelligence:** la piattaforma è gestita da un team specialistico di intelligence che ha l'obiettivo di arricchire le informazioni e contestualizzarle rispetto al contesto operativo della PA;
- **Analisi / Prioritizzazione:** la piattaforma dispone di funzionalità atte a filtrare le informazioni in funzione delle necessità della PA secondo meccanismi dinamici e continuativi che consentono di focalizzare l'attenzione sui fenomeni più rilevanti;
- **Interazioni** con i servizi Gestione Continua delle vulnerabilità e Next Generation Firewall, descritte al §10.4.1.

10.1.2 Feed di Threat Intelligence

I feed utilizzati per l'erogazione del servizio TI&VDF provengono ✓direttamente dai vendor dei prodotti, ✓da programmi di Bug Bounty e ✓da analisi effettuate da ricercatori di sicurezza ✓dal newtork Accenture costituito da tutti centri di competenza a livello Globale progressivamente acquisiti negli anni. Contengono **informazioni affidabili, aggiornate e dettagliate** sulle vulnerabilità di sicurezza. Ove possibile, i feed provengono dalle **fonti primarie** dei dati di intelligence in modo da **ridurre la ridondanza** delle informazioni raccolte e **ottimizzarne l'utilizzo**.

Di seguito vengono rappresentate le **caratteristiche**, in termini di descrizione e informazioni fornite, dei **71 feed** utilizzati raggruppati per **Tipologia** provenienti anche dai Centri di Competenza delle società acquisite quali **Symantec e Context-IS**.

TIPOLOGIA - Vulnerability data feed	NUMEROSITÀ - 2 feed
Descrizione	Feed costituiti da informazioni sulle vulnerabilità che impattano i prodotti di interesse, provenienti dal National Vulnerability Database (NVD) e dal database di vulnerabilità CVE Details
Informazioni	Descrizione della vulnerabilità, CPE impattate, score CVSS, classificazione CWE, data pubblicazione e ultimo aggiornamento, link ai bollettini di sicurezza rilasciati dal vendor, sfruttamento della vulnerabilità in campagne di attacco.

TIPOLOGIA - Vulnerability Intelligence Data Feed	NUMEROSITÀ - 6 feed
Descrizione	Feed costituiti da informazioni sulle vulnerabilità provenienti da diverse fonti tra cui la piattaforma proprietaria Accenture iDefense, i database di exploit per lo sfruttamento delle vulnerabilità disponibili in rete e i risultati del programma di Bug Bounty di iDefense
Informazioni	Descrizione della vulnerabilità, CPE impattate, score CVSS, classificazione CWE, data pubblicazione e ultimo aggiornamento, link ai bollettini di sicurezza rilasciati dal vendor, sfruttamento della vulnerabilità in campagne di attacco.

TIPOLOGIA - Threat Advisory Data Feed	NUMEROSITÀ - 2 feed
Descrizione	Bollettini riguardanti le minacce che impattano il contesto italiano e il settore dei Servizi Pubblici, redatti dal team di Cyber Threat Intelligence (CTI) del RTI
Informazioni	Descrizione di minacce, informazioni di contesto approfondite con un focus sulla PA, IoC aggiornati, azioni di mitigazione consigliate.

TIPOLOGIA - Threat Intelligence Data Feed	NUMEROSITÀ - 19 feed
Descrizione	Feed riguardanti il panorama globale delle minacce, inviati automaticamente dai vendor e dai provider di Intelligence.
Informazioni	Informazioni sulle minacce esistenti a livello globale, eventuali informazioni di contesto disponibili, IoC.

TIPOLOGIA - Threat Indicators Data Feed	NUMEROSITÀ - 42 feed
Descrizione	Feed costituiti da Indicatori di Compromissione (IoC) relativi alle minacce che impattano il settore dei Servizi Pubblici in Italia.
Informazioni	IoC aggiornati relativi alle minacce di interesse per la PA contraente relativi a: domini sospetti, URL dannosi, elenchi di hash malware noti, indirizzi IP associati ad attività dannose.

10.1.3 Architettura tecnologica

Tra gli elementi di **valore** della piattaforma Threat Intelligence Service (TIS) si evidenzia l'integrazione con il servizio SOC cui fornisce informazioni in merito alle minacce di sicurezza reali e potenziali, nonché Indicatori di Compromissione (IoC) che alimentano la piattaforma SIEM.

L'architettura del servizio prevede la possibilità per le PA di accedere alla piattaforma TIS tramite **un'interfaccia web** o tramite **API protette**. Il servizio può inoltre essere ingaggiato tramite il servizio di Help Desk che, a sua volta, accede alle interfacce della piattaforma TIS.

La piattaforma raccoglie i feed informativi e procede alla loro **elaborazione in modo automatizzato**. I data feed uniformati tramite la transcodifica nel formato STIX 2.1, un linguaggio strutturato specificamente utilizzato per lo scambio di informazioni di Cyber Threat Intelligence correlati al fine di ottenere informazioni di Intelligence il più possibile approfondite e complete.

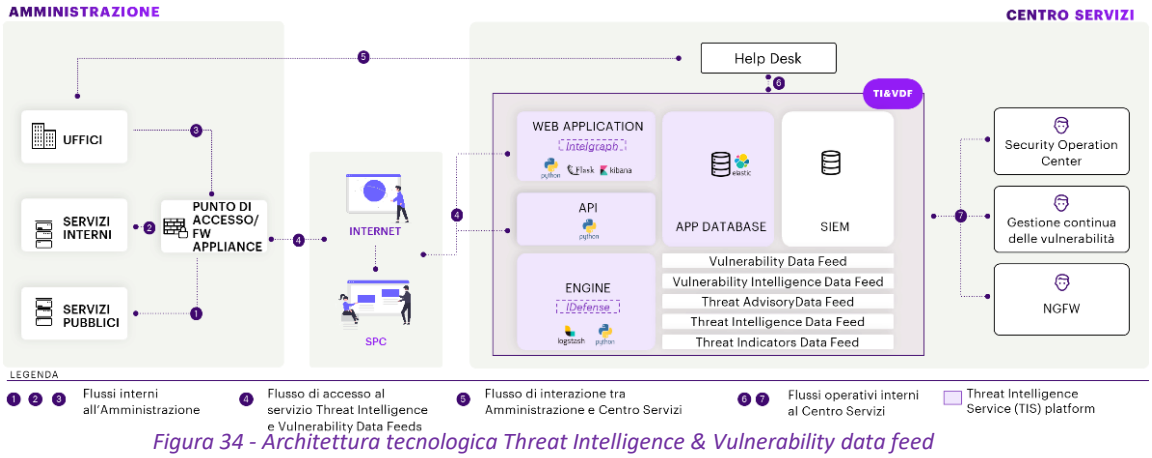


Figura 34 - Architettura tecnologica Threat Intelligence & Vulnerability data feed

La piattaforma si basa su **tecnologie open source** quali: ✓**Stack Elastilk (ELK)** che include (i) Elasticsearch, un search engine utilizzato per la ricerca e l'analisi dei dati, (ii) Logstash, una data processing pipeline che colleziona simultaneamente dati provenienti da molteplici fonti, li trasforma e li invia ad uno "stash" come Elasticsearch, (iii) Kibana, un software di data visualization che consente di visualizzare i dati in Elasticsearch mediante grafici e tabelle; ✓**Python**, un linguaggio di programmazione adattabile e largamente utilizzato per numerosi progetti anche in ambito cyber security; ✓**Flask**, un micro web framework scritto in Python utilizzato per la costruzione di applicazioni web.

10.2 Organizzazione

Nel contesto della struttura-tipo presentata al §6.2.1, il servizio è erogato da un unico gruppo di lavoro – TI Team, che risponde a un Responsabile del servizio, il quale rappresenta il punto di contatto tra il Team e la PA ed è supportato da uno SME (Subject Matter Expert). Il Team sarà così composto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
SME TI	Supporto al team TI / SSA	Offre consulenza per l'interpretazione di specifiche minacce identificate dal servizio di threat intelligence. Analizza le nuove minacce e fornisce indicazioni per l'arricchimento continuo dei vulnerability feed
TI team	L2 Security Engineer / Sr-ISC	Gestisce casi / incidenti che richiedono competenze avanzate. Supporta le attività evolutive della piattaforma TIS tramite l'individuazione delle fonti utilizzabili per la collezione dei feed di Intelligence e Vulnerability e la definizione delle strategie di raccolta dei dati
TI team	L1 Security Engineer / Jr-ISC	Si occupa di implementare sistemi di raccolta e condivisione dei feed provenienti dalle fonti OSINT e CLOSINT individuate, di eseguire la transcodifica dei dati per uniformarne i formati e di procedere alla configurazione e alla manutenzione complessiva della piattaforma TI
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

Sempre in analogia con il §6.2.1, il Team del servizio è supportato ✓dal CE Smart Hub (es. per identificare in dettaglio le tecnologie critiche in uso presso la PA allo scopo di meglio contestualizzare i feed di Vulnerability) ✓dai Centri di competenza della rete dei CyberFusion Center altamente specializzati nella gestione delle attività di threat intelligence.

10.3 Modello operativo

10.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

10.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di **Configurazione** ed **Erogazione** specifiche per il servizio in oggetto. Per le fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

Figura 35 - Modello operativo

CONFIGURAZIONE	
Configurazione Amministrazione	**Deliverable**: "Configurazione del servizio TI&VDF", che riporta le informazioni necessarie per la configurazione del servizio **Descrizione**: il servizio viene configurato con le seguenti informazioni relative alla PA fornite tramite il portale utenti e il servizio di Help Desk: ✓Nome della PA ✓Fascia del servizio richiesta ✓Nominativi, ruoli e informazioni di contatto dei referenti che riceveranno i feed, per la configurazione dei canali di ricezione ✓Canali di ricezione dei feed prescelti dall' PA (es. email, SMS)
Configurazione feed	**Deliverable**: "Configurazione del servizio TI&VDF" - sezione con l'elenco dei feed desiderati, i metodi di raccolta dei feed ed i risultati dei test effettuati allo scopo di verificare che la ricezione di tali feed sulla piattaforma TIS sia ottimale e che i dati siano leggibili e disponibili alla consultazione **Descrizione**: la raccolta, l'invio e la ricezione dei feed vengono configurati mediante le informazioni contenute nell'elenco dei feed previsti per la PA, il cui numero è da stabilirsi sulla base della fascia di servizio scelta
Configurazione della piattaforma	**Deliverable**: "Configurazione del servizio TI&VDF" - sezione sull'esito della configurazione della piattaforma TIS per l'accesso alla PA secondo le modalità previste. Vengono inoltre fornite le credenziali utilizzabili per l'accesso diretto alla piattaforma **Descrizione**: la piattaforma TIS viene configurata per consentire la ricezione dei feed previsti e per garantire l'accesso al Cliente. Viene effettuato il training del personale dell'PA che potrà accedere alla piattaforma per la consultazione diretta dei feed
Configurazione API e integrazione	**Deliverable**: "Configurazione del servizio TI&VDF" - sezione sui i risultati dei test effettuati per verificare che la ricezione dei dati mediante i sistemi in uso della PA sia ottimale e che i dati siano leggibili e disponibili alla consultazione **Descrizione**: vengono configurate le integrazioni necessarie per la consultazione dei feed raccolti dalla piattaforma mediante Interfacce di Integrazione (API). Vengono inoltre fornite le credenziali per utilizzare le API della piattaforma
EROGAZIONE	
Interrogazione feed	**Deliverable**: N/A **Descrizione**: funzionalità di interrogazione dei feed da parte della PA in due modalità: ✓**Lista completa**: la PA ha accesso alla lista completa dei feed e dei dati raccolti, consultabili direttamente sulla piattaforma TIS o tramite API ✓**Lista filtrata**: sulla piattaforma TIS o tramite API, la PA può eseguire ricerche mirate e avanzate mediante appositi filtri che consentono di accorpare i dati di interesse sulla base di diversi parametri (tipologia, data, contesto, associazioni di IoC, ecc.); ✓**Reporting**: la PA può generare report a partire dalle ricerche effettuate, scaricabili dalla piattaforma o ottenibili tramite API
Feeding altri strumenti	**Deliverable**: N/A **Descrizione**: la piattaforma TIS offre una sezione per monitorare lo stato e il numero delle segnalazioni inviate al SIEM del SOC. Tale sezione comprende anche le segnalazioni di IoC, inviate al SIEM automaticamente, e consente la generazione di report
Generazione reportistica	**Deliverable**: N/A **Descrizione**: i report del servizio TI&VDF possono essere generati on demand con due modalità: ✓**Reporting manuale**: mediante l'accesso diretto dalla piattaforma e la consultazione dei feed, è possibile generare manualmente tramite la Dashboard della piattaforma i report contenenti le informazioni di interesse, selezionabili tramite criteri flessibili (es. per campagna d'attacco, famiglia di malware, indicatori) ✓**Reporting automatico**: è possibile generare in modo automatizzato i report contenenti le informazioni di interesse mediante le API fornite

10.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "THREAT INTELLIGENCE & VULNERABILITY DATA FEED"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
PCI_USSS_TIV	Tempo di disponibilità dei servizi oggetto di fornitura e degli strumenti a supporto	Come USSS ma con frequenza maggiore e soglia più sfidante	Mensile	99%
KPI_RIP	Giorni di ritardo nell'installazione delle patch di sicurezza in carico alla PA ma dietro nostra segnalazione di vulnerabilità	Numero installazioni effettuate nei tempi previsti / Numero installazioni pianificate da effettuare (misurati sugli incident chiusi ove applicabile)	Trimestrale	85%

10.4 Interazioni

10.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
SOC	Indicatori di Compromissione	Output	Gli Indicatori di Compromissione e i dati di intelligence raccolti sono trasmissibili al sistema SIEM gestito dal servizio di SOC al fine di migliorare le attività di threat hunting
Gestione continua delle vulnerabilità	Informazioni sulle vulnerabilità in essere e potenziali	Input / output	Scambio di informazioni sulle vulnerabilità che possono essere di pertinenza delle PA al fine di integrarle nel ciclo di gestione e rimedio delle vulnerabilità stesse
Next Gen. Firewall	Indicatori di Compromissione	Output	Distribuzione di Indicatori di Compromissione direttamente sui firewall per prevenire e identificare le minacce di sicurezza

E' previsto l'utilizzo dei formati STIX/TAXII per l'integrazione con il sistema SIEM.

10.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
TI Report - Amministrazione	On Demand	Report generabile tramite API o Dashboard della piattaforma TIS, contenente i dati riguardanti la PA, ottenuti mediante i feed. È possibile generare il report in qualsiasi momento, filtrando dati, indicatori e fonti.
TI Report -Settore pubblico italiano	On Demand	Report generabile tramite API o Dashboard della piattaforma TIS, contenente i dati anonimizzati riguardanti le PA, ottenuti mediante i feed. È possibile generare il report in qualsiasi momento, filtrando dati, indicatori e fonti.
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui NGFW solo qualora fossero previsti possibili impatti di servizio

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

11.1 Soluzione proposta

Il modello **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di Protezione Navigazione Internet e Posta Elettronica nel dominio di sicurezza: "**Breach Prevention & Readiness**", riconducibile alla Funzione NIST "**Protect**". Il servizio ha lo scopo di proteggere gli utenti e i sistemi delle PA da minacce esterne di natura cyber provenienti da web e/o email e di preservare affidabilità, disponibilità, riservatezza e integrità delle comunicazione tra le componenti client e server del patrimonio informativo posto in perimetro. La vasta esperienza su scala internazionale del RTI ha consentito di consolidare ed evolvere un **modello di servizio proprietario** che arricchisce ed estende la protezione dei canali d'interazione web, mail e client-server, attraverso l'adozione della piattaforma **SWMGP (Secure Web and Mail Gateway Platform)**, dispiegata c/o il Centro Servizi e integrata con altri sistemi di controllo attivo e passivo (SIEM/SOAR, TIS, FWM), alla quale accede esclusivamente personale esperto, altamente qualificato e certificato (SANS, OSCP, OSCE, CEH, OPST, etc.). La SWMGP integra **tecnologie leader di settore** (FortiGate SWG, FortiMail) e **strumenti e acceleratori proprietari** del RTI per consentire agli specialisti la massima **efficacia** nella gestione degli allarmi e la massima **efficienza** nei tempi di risposta e risoluzione. Il Centro Servizi del RTI si avvale, peraltro, della rete di CyberFusion Center resa disponibile da Accenture e altamente specializzata sia nella "deep inspection" del codice scaricato da internet (sandboxing basato sia su analisi comportamentale che su firme) che nel rilevamento di accessi ad applicazioni Cloud (SaaS) non conformi alle politiche delle PA contraenti (attraverso liste d'accesso e controlli granulari per la fruizione delle funzionalità), così come della rete di monitoraggio del traffico internet resa disponibile da Fastweb attraverso le proprie infrastrutture di sicurezza tipiche di un provider di servizi internet.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: più di 30 tra cui INPS, ISTAT, Consiglio Nazionale delle Ricerche, Comune di Napoli

Private: NEXI, Intesa Sanpaolo, Primario operatore finanziario

Descrizione di un caso di successo – INPS → Esigenza - Realizzazione e gestione di una infrastruttura di "secure web gateway", per circa 30.000 utenti, che consente di bloccare l'accesso a siti web potenzialmente malevoli in tempo reale, aggiornando la propria base dati in maniera automatica e quindi riconoscere il download di applicazioni potenzialmente dannose →**Soluzione** - È basata sulla tecnologia leader di mercato e caratterizzata da una componente centrale di gestione e dalle componenti gateway (fisiche) dislocate "on premise" presso INPS →**Benefici** - ✓assicura analisi del traffico, rilevazione e blocco dei comportamenti dannosi ✓aggiornamento delle liste dei siti (ogni 24 ore per il database dei contenuti, 5 minuti per il Real Time update e 15 minuti per l'Antivirus).

11.1.1 Funzioni Offerte

Il servizio prevede i **4 livelli**, già presentati al §6.1.1, che comprendono tutte le funzionalità richieste da Capitolato, incluse quelle avanzate di **Application Control**

e **Deep inspection** (dettagliate al §11.5) e ne aggiungono alcune **migliorative** di seguito descritte.

Funzioni migliorative per Protezione della Navigazione Internet

Predictive Machine Learning Sandboxing: il servizio è abilitato da una soluzione di rilevamento di **minacce complesse** che esegue analisi dinamiche volte a identificare sia **malware non ancora noto** sia **malware e ransomware creati appositamente** con proprietà di sandbox evasion. I controlli preventivi volti a disarmare le minacce all'interno della rete vengono attivati dagli output dell'intelligence applicata alle sandbox di investigazione. Contenuti e comportamenti utente vengono, infatti, simulati in ambiente protetto e analizzati da strumenti e personale specializzato nella ricerca di potenziali allegati alle email di natura malevola, utilizzando **algoritmi avanzati di ML** e **AI per filtrare e analizzare** file con peculiarità non note.

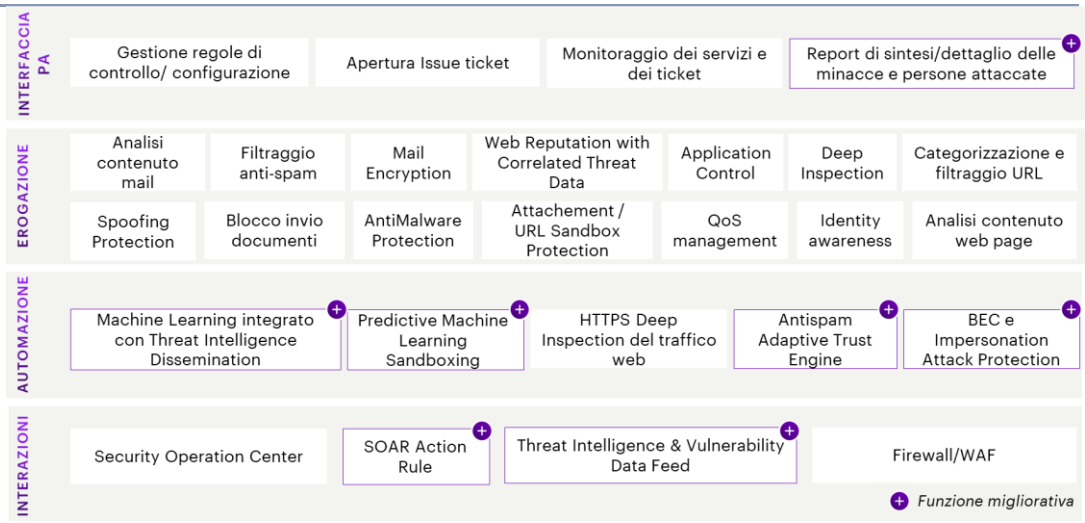


Figura 36 – Funzioni del Servizio

Funzioni migliorative per Protezione della Posta Elettronica

✓**Adaptive Trust Engineering**: Il servizio contempla il tracciamento delle relazioni mittenti-destinatari e il monitoraggio transazioni/interazioni per misurare le reti di fiducia e migliorare il rilevamento delle minacce, unitamente alla protezione delle email in uscita (funzionalità **aggiuntive**: attachment e URL analysis, recipient verification, impostor detection, account compromission detection) ✓**Business Email Compromise e Impersonation Attack Protection**: Il servizio si avvale di algoritmi avanzati volti alla protezione da attacchi di Impostor Detection, Business Email Compromise (Account compromission detection), CEO Fraud e Whaling, Display Name Attacks; prevede, inoltre, l'applicazione di **filtri basati sulla reputazione** dell'indirizzo IP di provenienza e/o URL, oltre che la protezione da email massive e campagne aggressive di marketing.

Funzioni migliorative comuni alla protezione della Navigazione Internet ed alla Posta Elettronica

✓**Reporting**: Il servizio prevede la produzione, periodica o a richiesta, di rendicontazione direzionale (executive summary) e tecnica di dettaglio (technical report) che riporta gli utenti più attaccati e le più rilevanti tipologie di minacce a cui sono sottoposti (es. l'elenco dinamico "Most attacked People" da porre sotto protezione di navigazione link nelle email attraverso sandbox, oppure la lista dei VIP account soggetti ad impersonification attacks), con informazioni utili per pianificare un **percorso di security awareness** mirato e individuale ✓**ML Integrato con Threath Intelligence Dissemination**: Il servizio si avvale di un sofisticato motore di ML che analizza eventi relativi a navigazione internet e comunicazioni di posta, sulla base delle evidenze prodotte dalla threat intelligence e volte a garantire la massima copertura dalle minacce più recenti (Core capabilities: FortiGuard Labs, Fortinet Security Fabric e proprietarie Accenture) ✓**Integrazione con Threat Intelligence & Vulnerability Data Feed**: Il servizio ricostruisce attivamente e sistematicamente una 'situational awareness' di contesto che rende fruibile ai servizi di Cyber Defence Governance (interagendo con threat monitoring and hunting) per aumentare la capacità di rilevamento nel caso di eventuali **scenari di attacco complessi** (es. attraverso threat data enrichment riportante informazioni su esperienze di navigazione o caselle attaccate dallo stesso malware seppur con mail apparentemente diverse) ✓**On demand investigation**: Servizio per analisi 'on demand' richieste dalle PA e relative a esperienze di navigazione o comunicazioni mail con allegati che richiedano approfondimenti o supplemento d'indagine. Interazioni ulteriori sono con i servizi SOC, Next Generation Firewall e Web Application Firewall dettagliatamente descritte al §11.4.1).

11.1.2 Architettura tecnologica

La piattaforma SWMGP è basata su tecnologia **Fortinet** integrata con strumenti e acceleratori proprietari del RTI. L'architettura prevista per la fornitura del servizio di protezione ✓della **navigazione internet** si avvale del modulo FortiGate SWG (Secure Web Gateway) ✓e quella per la protezione della **posta elettronica** del modulo FortiMail. Gli **acceleratori** Accenture della piattaforma SWMGP includono: ✓Standalone sandbox environment ✓Stack inspectors ✓Threat intel extra feed receiver ✓Threat Intelligence Dissemination. Tali strumenti sono resi disponibili agli specialisti del RTI per consentire gli approfondimenti sulle minacce complesse che richiedono attività di '**reverse engineering**'. La soluzione proposta prevede integrazione di appliance fisiche o virtuali presso i CED delle PA oppure implementazione remota presso il Centro Servizi, scelta subordinata a specifiche di contesto (es. caratteristiche

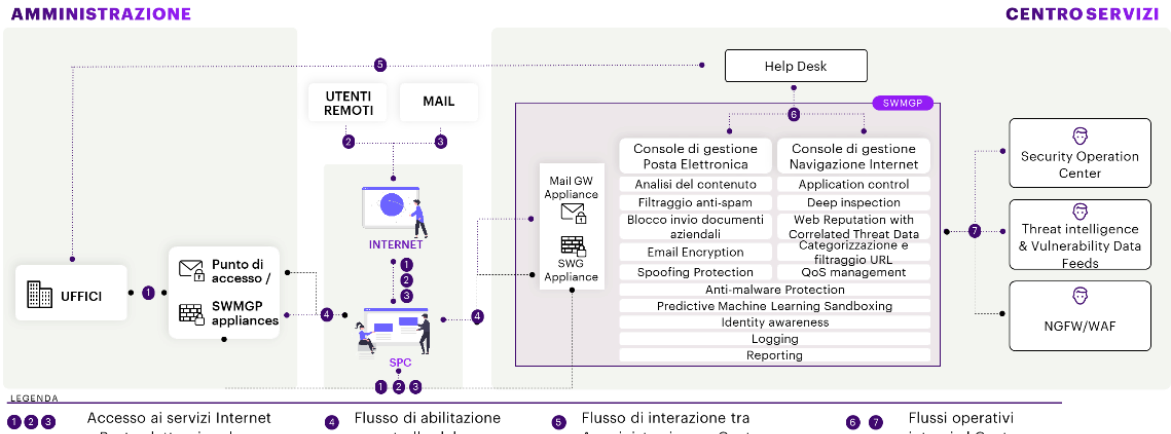


Figura 37 – Architettura tecnologica SWMGP

dell'infrastruttura di rete) e accordi con la singola PA. La scelta sarà effettuata in fase di attivazione del servizio. Il servizio si avvale inoltre dell'integrazione con i moduli **FortiGuard (antivirus)** e **Fortinet Security Fabric**. Il FortiGate SWG (**navigazione internet**) verrà utilizzato in modalità **transparent proxy** ovvero senza necessità di configurazioni lato client. Il servizio di **protezione della posta** verrà erogato in modalità **Gateway** per la protezione del traffico email sia in entrata che in uscita; opererà anche in modalità **out-of-line** per la scansione e il **clawback** (richiamo email) delle minacce direttamente in Microsoft 365 utilizzando l'API Graph.

11.2 Organizzazione

Nel contesto della struttura-tipo presentata al §6.2.1, il servizio è erogato da un unico gruppo di lavoro denominato **Web Navigation and Email Protection (WNEP) Team**, che risponde a un **Responsabile del servizio**, il quale rappresenta il punto di contatto tra il WNEP Team e la PA; il WNEP Team sarà così composto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

SOTTO-TEAM	RUOLO / Profilo	COMPITI E RESPONSABILITÀ
Team Email	Responsabili erogazione servizio Protezione posta elettronica / Sr-ISC + Jr-ISC	Il team presidia lo stato della sicurezza della posta elettronica, esegue analisi su base quotidiana e gestisce richieste SR, ingaggiato dall'Help Desk per erogare i servizi di cui al § successivo.
Team Firewall	Responsabili erogazione servizio Protezione Navigazione Internet / Sr-ISC + Jr-ISC	Il team presidia lo stato della sicurezza della navigazione web, esegue analisi su base quotidiana e gestisce richieste SR, ingaggiato dall'Help Desk per erogare i servizi di cui al § successivo.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant		

Sempre in analogia con il §6.2.1, il Team del servizio è supportato ✓dal CE Smart Hub (es. per identificare in dettaglio le tecnologie critiche in uso presso la PA allo scopo di meglio contestualizzare i controlli su navigazione e posta) ✓dai Centri di competenza della rete di CyberFusion Center altamente specializzati nella ricerca e mitigazione di attacchi ad alta complessità su navigazione web e posta elettronica.

11.3 Modello operativo

11.3.1 Processi

In figura una rappresentazione di sintesi delle fasi del servizio.

Figura 38 – Modello operativo

11.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di Configurazione ed Erogazione specifiche per il servizio in oggetto. Per la descrizione delle fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

CONFIGURAZIONE	
Configurazione sistemi	**Deliverable**: Specifiche di configurazione **Descrizione**: Configurazione degli apparati (tramite policy/regole standard o personalizzate. Integrazione con gli altri servizi interdipendenti
Migrazione dati	**Deliverable**: Piano di migrazione e specifiche ETL **Descrizione**: Migrazione policy/regole standard o personalizzate per configurare gli apparati
EROGAZIONE	
Gestione profili di navigazione	**Deliverable**: Matrice di profilazione **Descrizione**: L'Help Desk indirizza la creazione e/o la modifica dei profili di navigazione Internet, abilitando/disabilitando/limitando l'accesso a diverse categorie di siti web
Personalizzazione categorie e filtri nav.	**Deliverable**: Specifiche di navigazione **Descrizione**: Creazione di categorie 'custom' di siti web per il filtering della navigazione Internet
Gestione soglie anti-spam	**Deliverable**: Specifiche anti-spam **Descrizione**: Gestione delle soglie di spam e high-spam personalizzate per singoli o gruppi di utenti (con filtering ulteriore e dedicato per alcune classi di utenti – VIP)
Gestione allegati di posta	**Deliverable**: Specifiche di controllo allegati **Descrizione**: Gestione dei filtri di blocco degli allegati in base a: tipologia, estensione e profilo di rischio associato ai file
Controllo accessi via white/black-listing	**Deliverable**: Access Control List(s) **Descrizione**: Gestione delle liste di controllo accessi per la protezione della posta elettronica e per la navigazione Internet
Esfiltrazione email malevole	**Deliverable**: Verbale di rendicontazione attività **Descrizione**: Gestione delle richieste di rimozione di email dalla posta elettronica di uno o più utenti (comprese tutte le successive conversazioni correlate)

Non elencate, sono altresì previste le attività di **Aggiornamento e Manutenzione** curate in autonomia dal centro servizi. Tali attività possono riguardare aggiornamenti software, hotfix, operazioni di riavvio di specifici dispositivi, atti a garantire il corretto svolgimento dei servizi di protezione. In particolare, la gestione degli **avanzamenti software e firmware** verrà notificata, programmata ed eseguita fuori orario base e preservando la continuità del servizio.

11.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, illustriamo gli indicatori aggiuntivi per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSA	Cfr. §6.3.4			
PCI_TNSA	Cfr. §6.3.4			
KPI_NAUB	Numero accessi a URL pericolosi bloccati	Conteggio complessivo degli eventi	Trimestre	Riduzione rispetto alla misura del periodo precedente
KPI_NMSB	% messaggi spam bloccati rispetto ai totali	Rapporto tra messaggi bloccati e messaggi ricevuti	Trimestre	Incremento rispetto alla misura del periodo precedente

11.4 Interazioni

11.4.1 Flussi verso altri servizi

ALTRO SERVIZIO	FLUSSO	I/O	DESCRIZIONE/FINALITÀ
SOC	Audit log e log di eventi di sicurezza	Output	La piattaforma SWMGP trasmetterà i log di sicurezza (audit e alarms) al SIEM affinché gli eventi di navigazione internet e inerenti alla posta elettronica possano essere correlati con gli eventi di altri sistemi per ricostruire correttamente gli scenari dei casi d'uso posti sotto monitoraggio.
SOC via SOAR	Filtering rules	Input	Regole puntuali per l'applicazione di filtri di navigazione e/o di controllo di comunicazioni/allegati di posta elettronica attivate da automatismi SOAR (actionable triggers).
Threat Int. & Vulnerability Data Feed	Audit log e log di eventi di sicurezza	Output	La piattaforma SWMGP trasmetterà i log di sicurezza (audit e alarms) al servizio di Threat Monitoring per aumentare la conoscenza del contesto nel caso di incidenti, investigazione o approfondimenti.
Threat Int. & Vulnerability Data Feed	Ind. di Compromissione (IoC) e Indicatori di Attacco (IoA)	Input	Gli IoC/IoA provenienti dalla piattaforma di Threat Intelligence di Accenture sono inviati alla piattaforma SWMGP (moduli FortiGate SWG e FortiMail) e costantemente aggiornati per aumentare il livello di copertura verso minacce recenti.
Next Generation Firewall e Web Application Firewall	Firewall rules ed IDS/IPS signatures	Output	Regole Firewall e firme per IDS/IPS, per filtering e continuous analysis del traffico a livello applicativo (layer 7).

11.4.2 Report aggiuntivi per l'Amministrazione

NOME REPORT	PERIODICITÀ	DESCRIZIONE
Threats/Malware report	settimanale	Tipologie di minacce di cui sono stati oggetto gli utenti, indicando per ciascun caso la presenza di eventuali casi andati a segno.
Most Attacked People	mensile	Riepilogo delle persone più attaccate nel periodo, sia su navigazione internet che su posta elettronica.
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese

11.5 Caratteristiche funzionali avanzate

Le modalità d'impiego delle funzionalità avanzate del servizio rese disponibili alle PA saranno concordate in fase di attivazione e predisposte in fase di configurazione. Un processo di miglioramento continuo attivato in fase di erogazione e governato dal centro servizi fornirà alle PA le proposte di ottimizzazione delle configurazioni al variare del panorama delle minacce e delle specificità di contesto, al fine di mantenere i più alti standard di protezione anche in divenire.

11.5.1 Deep Inspection

Il servizio contempla un meccanismo di protezione avanzata dalle minacce, che esegue una verifica preliminare sulla conformità di browser e plug-in che hanno eseguito la richiesta della URL e una successiva ispezione completa e profonda del contenuto del pacchetto. L'esecuzione della deep inspection è in grado di rilevare qualsiasi malware nascosto all'interno di una risorsa web, sia esso noto (via signature matching) o ignoto (behavioral based), attraverso avanzate funzionalità di prevenzione fondate su AI/ML che si avvalgono di algoritmi predittivi applicati alla sandbox per rilevare varianti complesse di malware recenti e/o attacchi di tipo Zero-Day. Il servizio rileva iFrame nascosti, cross-site scripting, segni di tentativi di phishing e ransomware, furto di cookie e comunicazioni botnet ai server C&C. Tutti i pacchetti sono sottoposti a ispezione in profondità poiché tipicamente le pagine web sono dinamicamente generate con contenuti personalizzati costituiti da centinaia di oggetti ottenuti dalle fonti più varie; ogni oggetto rappresenta pertanto una potenziale minaccia e viene considerato non attendibile indipendentemente dalla fonte (zero-trust). L'analisi del traffico criptato (incluso il protocollo TLS 1.3) viene eseguita ad alte prestazioni (leader di settore), il servizio permette la completa ispezione in real-time del traffico criptato su tutte le porte e i protocolli. La conoscenza del panorama delle minacce combinata con la capacità di rispondere rapidamente agli allarmi è abilitata da ricercatori Accenture iDefense e Fortinet che setacciano quotidianamente su scala globale il web (clear, dark, deep) per scoprire minacce emergenti e sviluppare contromisure efficaci. **Più di 250.000 organizzazioni nel mondo** si avvalgono della tecnologia proposta.

11.5.2 Controllo Accessi ad applicazioni cloud SaaS non conformi

Il servizio contempla un meccanismo di controllo accessi d'avanguardia tale da garantire connessioni veloci e sicure e consentire ai dipendenti di lavorare da qualsiasi luogo utilizzando Internet per accedere alla rete aziendale, ottimizzando peraltro l'uso della larghezza di banda della rete, prioritizzando o bloccando il

traffico in base all'applicazione. Basato sul paradigma zero-trust, il servizio fornisce una sicurezza completa avvalendosi dell'identità digitale emergente dal contesto e dell'applicazione di politiche d'accesso per applicazioni SaaS che si riflettono nei profili di sicurezza assegnati/assegnabili dinamicamente all'utente in base al rischio attinente a identità, dispositivo e localizzazione. Il rischio associato all'utente viene costantemente aggiornato in base alla propria risk-posture e al raggiungimento di soglie predefinite/configurabili, può essere automaticamente assegnato un profilo d'accesso più limitato, sino alla restrizione totale della navigazione in caso di comportamenti sospetti. Il controllo accessi applicativo migliora la sicurezza e soddisfa i requisiti di conformità in virtù dell'applicazione di policy volte a consentire, negare o limitare l'accesso a specifiche applicazioni od a categorie di applicazioni (con attuazione in tempo reale). Il servizio vanta uno dei più rilevanti database di applicazioni (su tecnologia Fortinet, leader di mercato) costantemente aggiornato per proteggere le PA da funzionalità rischiose e consentire piena visibilità e controllo delle sessioni/chiamate in esecuzione. Il servizio è in grado di riconoscere la **totalità di protocolli applicativi** dei maggiori servizi SaaS ad oggi esistenti, classificati per tipologie (es. Cloud Storage, Social Networks, e-commerce, Media and TV Streaming, Team Working, Remote Desktop Tools, Videocall and messaging tools). Risulta peraltro possibile definire profili di accesso differenti che blocchino/permettano l'utilizzo di tutte/alcune categorie o di singoli applicativi non conformi alle politiche aziendali, applicando sistemi di white-listing/black-listing granulari. **L'actionable intelligence** fornita attraverso il servizio di controllo delle applicazioni proviene dal team di sviluppo globale di FortiGuard Labs, leader del settore e attivo nella ricerca sulle vulnerabilità.

12 PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA" - FUNZIONALITÀ AGGIUNTIVE

Con riferimento al servizio di "protezione navigazione internet e posta elettronica" (di cui al par. 3.1.6 del Capitolato Tecnico speciale), il Raggruppamento conferma la presenza di funzioni di protezione della posta anti-phishing e anti-ransomware.

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

13.1 Soluzione Proposta

Partendo dal modello **CDOM** (cfr. §§ 1 e 3.3) definiamo le componenti per le operazioni di sicurezza a copertura del servizio di Protezione degli Endpoint. Il CDOM colloca questo servizio nel dominio di sicurezza "**Breach Prevention & Readiness**" / Funzione NIST "**Protect**".
Il servizio di protezione degli Endpoint (PEP) rappresenta uno degli elementi chiave forniti dal Centro Servizi per garantire la sicurezza delle infrastrutture delle PA, operando direttamente sui dispositivi in uso agli utenti abilitando sia l'identificazione di anomalie di processo che le azioni di contenimento e reazione da implementare in caso di violazione. La soluzione tecnologica di Endpoint Protection proposta è basata su tecnologia **TrendMicro ApexOne**, riconosciuta come leader sul mercato da **Gartner nel Magic Quadrant 2021** di Endpoint Protection Platform. Tale tecnologia fornisce un'ampia e consolidata copertura dei requisiti di tecnico-funzionali espressi nel capitolato e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi. Accenture, Fastweb e Trend Micro collaborano nell'esecuzione di numerose progettualità a livello globale su clienti di diversi settori. Importante sottolineare che Accenture, Fastweb e Trend Micro collaborano congiuntamente nello sviluppo delle soluzioni presso i propri Clienti unendo le competenze di prodotto e di system integration e gestione che, congiuntamente, consentono di adeguare il prodotto alle effettive necessità dei Clienti. All'interno di tale collaborazione si procederà anche a indirizzare uno sviluppo/integrazione di prodotto dedicata alle PA. La soluzione proposta consente di ✓effettuare l'ispezione del traffico generato dalla postazione di lavoro, ✓controllare lo scambio di dati (Data Loss Prevention – DLP) in maniera tale che le informazioni sensibili non possano essere trasferite ad attori non autorizzati ✓controllare lo stato di compliance dei dispositivi rispetto a policy di sicurezza ben definite ✓inviare log al SIEM integrandosi nel Servizio di Security Operation Center e abilitando il monitoraggio 24x7. La soluzione sfrutta tecniche di rilevamento delle anomalie avanzate tramite: ✓metodologie di **ML** prima e durante l'esecuzione dei file ✓tecniche di **cancellazione del rumore di fondo**, come censimento ed elenchi di utenti autorizzati, a ogni livello di rilevamento, per ridurre drasticamente i falsi positivi ✓tecniche specifiche per la protezione contro script, iniezioni, ransomware e attacchi a memoria e browser, grazie a un'innovativa **analisi del comportamento**.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: 2 - Guardia di Finanza, Croce Rossa Italiana

Private: Veritas

Descrizione di un caso di successo - **Guardia di Finanza** →**Esigenza** - Implementazione di una soluzione di end point protection per diverse migliaia di postazioni di lavoro, che sia in grado di effettuare il monitoraggio e la protezione delle postazioni di lavoro da rischi derivanti dalla navigazione web o da altri fattori di rischio →**Soluzione** – Fastweb ha realizzato una soluzione con tecnologia leader di mercato che prevede l'installazione di SW agent sugli endpoint distribuibili in maniera semi-automatica attraverso piattaforme di sw deployment dell'Amministrazione →**Benefici** - ✓protezione dalle minacce informatiche più recenti, incluse le minacce fileless ✓riduzione del rischio di esposizione ai cyberattacchi, grazie all'hardening degli endpoint ✓incremento del livello di sicurezza dei dispositivi utilizzati dai dipendenti attraverso avanzati controlli cloud-enabled ✓protezione dei server e degli endpoint senza comprometterne le performance ✓gestione semplificata della sicurezza delle postazioni di lavoro tramite una console unificata.

13.1.1 Funzioni offerte

Il servizio prevede i **4 livelli**, già presentati al §6.1.1, che comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative** di seguito descritte.

✓**Anti malware avanzato**: la soluzione proposta prevede l'applicazione di algoritmi di ML prima e durante l'esecuzione dei processi, al fine di rilevare più accuratamente attività associabili a malware, ivi incluse forme **fileless e ransomware**; ✓**Host-based Intrusion Prevention System (IPS)**: una funzionalità che consente di mantenere i sistemi protetti contro vulnerabilità note e sconosciute (Zero Day vulnerabilities); tale funzionalità è ulteriormente potenziata dall'integrazione con le informazioni rese disponibili dalla Trend Micro Zero Day Initiative (ZDI) che, tramite la ricerca strutturata di nuove vulnerabilità, consente di identificarle in anticipo (giorni, settimane o mesi prima rispetto alla concorrenza) e abilitare il patching virtuale con cui è possibile anticipare una patch ufficiale da parte del fornitore;

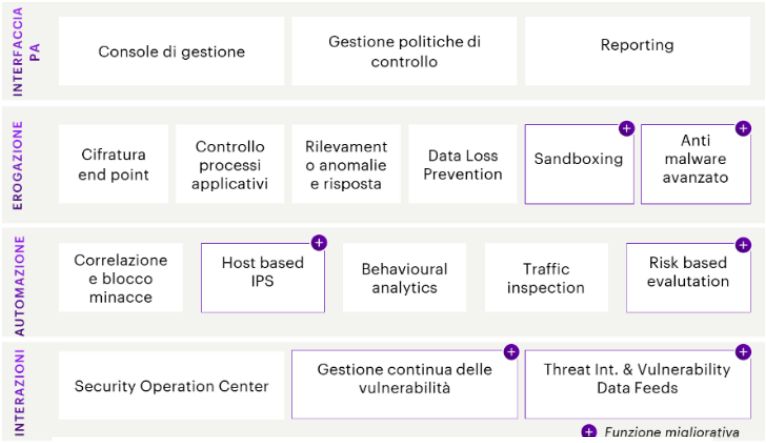


Figura 39 - Funzioni del servizio Protezione Endpoint

✓**Risk based evaluation***:* per ogni change funzionale ed infrastrutturale la soluzione consente di eseguire la stima di impatti e rischio sulle configurazioni implementate o che si prevede di implementare fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura; tali valutazioni sono effettuate tenendo in considerazione: la classificazione del servizio impattato, la criticità del servizio abilitato per la PA e le dipendenze ed interazioni con altri servizi, funzioni e sistemi ✓**Sandboxing** per l'analisi degli elementi sospetti che richiedono di approfondimenti specifici ✓Interazioni con i servizi **Gestione continua delle vulnerabilità di sicurezza** e di **Threat Intelligence & Vulnerability Data Feed**, dettagliatamente descritte al §13.4.1).

13.1.2 Architettura tecnologica

L'architettura tecnologica prevede: ✓**componenti centrali (Apex Central)**, localizzate nel Centro Servizi, che consentono la gestione delle funzionalità di endpoint protection, oltre alle funzionalità di reportistica e analisi degli eventi di sicurezza in caso di segnalazioni; ✓**componenti distribuite (agent)** basate su agent da installare sui dispositivi utenti da proteggere, compatibilmente con le versioni di sistema operativo supportati (scelta subordinata agli accordi con la PA contraente).

Tramite la componente Apex One Server, la piattaforma di controllo centralizzata comunica con gli agenti distribuiti al fine di impostare su ognuno di essi le configurazioni amministrative relativamente alle funzionalità di sicurezza, istruendoli ad eseguire determinati controlli, impostare esclusioni e attivare allarmi. L'agente sul dispositivo utente comunica con l'infrastruttura centrale per la condivisione di dati telemetrici utili agli analisti per le fasi di rilevazione e risposta agli attacchi. La soluzione abilita una comunicazione tra agente e server di gestione centrale indipendente dalla locazione dell'utente tramite la componente **edge relay** consentendo il controllo degli utenti anche quando connessi tramite internet, condizione che si verifica tipicamente con l'adozione di forme di **lavoro agile** (smart working).

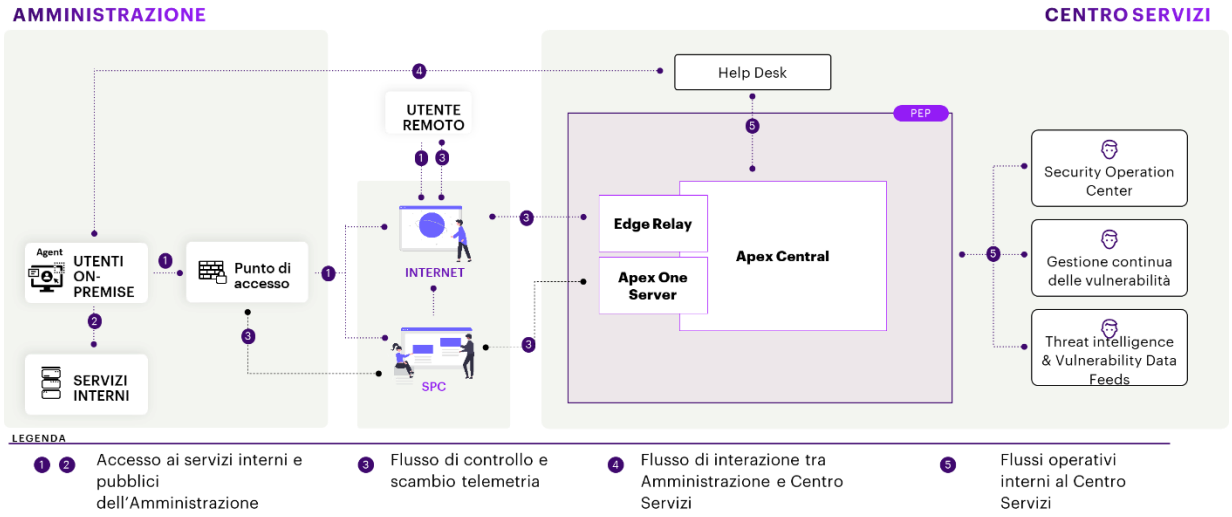
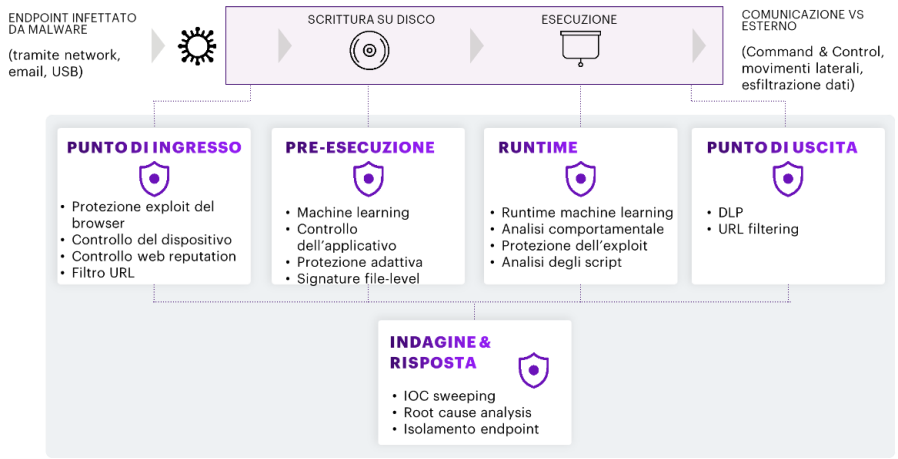


Figura 40 – Architettura Tecnologica Protezione Endpoint



La console centrale consente di avere un unico punto di visibilità e analisi degli eventi, abilitando al contempo la possibilità di gestire in maniera indipendente più domini amministrativi, ossia insieme di agenti che condividono le stesse configurazioni ed eseguono gli stessi compiti. Nel momento in cui viene rilevata una minaccia, l'agente può essere istruito per applicare diverse azioni quali blocco, quarantena o eliminazione dell'oggetto. Inoltre, la soluzione è **integrata con ambienti di sandboxing:** gli oggetti sospetti possono essere inviati alla sandbox (ubicata nei DC del RTI) per un'analisi avanzata. Gli amministratori possono accedere ad una reportistica dettagliata che dimostra ogni singola azione effettuata dall'oggetto analizzato nell'ambiente protetto come comandi powershell lanciati, file o chiavi di registro modificate e chiamate URL verso l'esterno.

13.1.3 Caratteristiche tecnologiche e prestazionali migliorative

La soluzione proposta ha al suo interno diversi fattori distintivi e migliorativi. In particolare introduce i seguenti elementi distintivi: ✓sistema automatizzato avanzato di rilevamento e risposta, a una varietà sempre più ampia di minacce, tra cui fileless e ransomware; ✓approfondimento delle informazioni, capacità investigative ampliate e visibilità centralizzata tramite una forte integrazione SIEM e l'adozione di un set di API aperto; ✓protezione integrata gestita da un singolo agente per rilevamento, risposta e indagine delle minacce, riducendo l'effort di gestione da parte delle singole PA. La soluzione consente inoltre di intervenire sulla catena di attacco in diversi momenti e applicando azioni di contenimento fra loro complementari, come indicato in figura, nelle seguenti fasi del ciclo operativo del malware: infezione dell'endpoint, pre-esecuzione, esecuzione runtime, uscita per esfiltrazione dati o esecuzione di movimenti laterali.

13.2 Organizzazione

13.2.1 Strutture coinvolte

Il servizio Protezione degli Endpoint è erogato da un team specializzato, che risponde a un **Responsabile del servizio**; il team è supportato da uno SME (Subject Matter Expert) esperto su tecnologie Endpoint Protection. Come per gli altri servizi è previsto il supporto delle seguenti strutture: ✓**CE SMART HUB** (cfr. §6.2.1) ✓**Centri di Competenza/Partnership** che forniscono competenze specialistiche. In particolare, il team di lavoro avrà la possibilità di avvalersi del supporto aggiuntivo del Cyber Fusion Center del RTI e il supporto specialistico del vendor. Il team è composto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall) come da tabella seguente.

13.2.2 Team del servizio

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
SME Protezione Endpoint	Supporto al team Protezione Endpoint / SSA	Offre consulenza per l'installazione / configurazione della soluzione in caso di problematiche specifiche e/o nella gestione di eventi / incidenti che non possono essere gestiti con le azioni di analisi e rimedio ordinarie. Viene inoltre coinvolto per l'ottimizzazione della soluzione nel suo complesso.
Team Protezione Endpont	L2 Security Engineer / Sr-ISC	Supporta e integra le attività del L1 e si attiva per incident di priorità elevata e change complesse. Attiva il supporto dei Vendor e gestisce l'andamento della richiesta sino alla chiusura.
Team Protezione Endpont	L1 Security Engineer / Jr-ISC	Esegue procedure per la risoluzione delle richieste relative a installazioni, configurazioni e incidenti, attivando eventualmente procedure di escalation verso L2 in caso di necessità.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

13.3 Modello operativo

13.3.1 Processi

Si riporta a seguire una rappresentazione di sintesi del modello operativo.

Figura 42 - Modello operativo

13.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di configurazione ed erogazione specifiche per il servizio in oggetto. Per le fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

CONFIGURAZIONE	
Setup e supporto alla distribuzione degli agenti	**Deliverable**: "Report distribuzione degli agenti" contenente la definizione delle funzionalità incluse nel pacchetto di installazione e del report finale di distribuzione degli agenti. **Descrizione**: Si procederà a ✓definizione del pacchetto di installazione dell'agente al fine di soddisfare le esigenze di sicurezza definite nell'analisi dei fabbisogni, ✓supporto per la strategia di distribuzione degli agenti (compatibilità con i sistemi, wave pilota, modalità di deployment), ✓verifica della copertura dei sistemi in perimetro.
Configurazione e messa in produzione	**Deliverable**: "Configurazione del servizio Protezione degli EndPoint", contenente il dettaglio delle policy implementate e i test eseguiti per validazione del deployment. **Descrizione**: Si procederà a: ✓ implementazione delle policy di sicurezza per garantire la protezione degli endpoint, ✓esecuzione di test per verificare che le policy implementate siano efficaci dal punto di vista funzionale di sicurezza e che non blocchino l'operatività della PA.

EROGAZIONE	
Gestione ciclo di vita policy	Deliverable: Aggiornamento delle policy di sicurezza
	Si procederà alla manutenzione continua delle policy di sicurezza in funzione delle esigenze espresse dalla PA e/o da evidenze provenienti dal Servizio SOC e/o di Threat Intelligence e Vulnerability Feed
Operation	Deliverable: Report attività manutenzione
	Si procederà alla gestione di anomalie mediante: ✓l'applicazione di soluzioni permanenti, ove già disponibili, utili a risolvere la casistica ✓l'applicazione di workaround e analisi successiva della root cause in assenza di soluzioni disponibili. Nel continuo si procederà alla verifica dello stato della soluzione e dei relativi processi di controllo
Reporting	Deliverable: Report di servizio
	Si procederà alla generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in xls o pdf

13.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "PROTEZIONE DEGLI END POINT"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSA	Cfr. §6.3.4			
PCI_TNSA	Cfr. §6.3.4			
KPI_NVMB	Virus e malware bloccati: Numero medio di eventi per end point	Numero virus e malware bloccati / Numero di end point	Trimestre	Riduzione rispetto alla misura precedente

13.4 Interazioni

13.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
Security Operation Center (SOC)	Log di audit ed eventi verso il SIEM	Output	I sistemi inviano log al SIEM affinché gli eventi generati dagli endpoint e dalle elaborazioni della console centrale possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni d'interesse per la cybersecurity e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza
Gestione continua delle vulnerabilità	Vulnerabilità in essere/potenziali	Input/ Output	La console centrale scambia con il servizio informazioni relative alle vulnerabilità identificate sui sistemi e relative configurazioni e riceve informazioni in merito alla relativa criticità e prioritizzazione
Threat Intelligence & Vulnerability Data Feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence sono raccolti in input dalla console centrale ApexOne per limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash)

13.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando: ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese quali particolari minacce rilevate, eventuali compromissioni e risposte eseguite
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sugli endpoint solo qualora fossero previsti possibili impatti di servizio.

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

La formazione dei dipendenti su tematiche di cyber security è uno degli aspetti fondamentali per sensibilizzare il personale delle PA sulle tematiche inerenti alla sicurezza delle informazioni ed evitare che comportamenti non adeguati dei singoli soggetti possano compromettere la sicurezza dell'intero sistema. Il servizio proposto ha lo scopo di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi. Il CDOM proposto (cfr. §§1 e 3.3) colloca il servizio di Formazione e Security Awareness nel dominio di sicurezza "**Breach Prevention & Readiness**" riconducibile alla Funzione NIST "**Protect**". Al fine di erogare un servizio efficace è necessario fare leva su una serie di fattori innovativi, necessari a garantire il coinvolgimento dell'utente in funzione della percezione che questo ha della sicurezza informatica e dei rischi indotti dalla sua operatività quotidiana, distinti in funzione di ruoli e mansioni ricoperte. Tra i fattori innovativi della proposta evidenziamo, in particolare: ✓**Assessment delle competenze dell'utente** prima dell'esecuzione degli interventi di awareness con l'obiettivo di definire azioni adeguate e motivanti nel percorso di formazione; ✓**Coinvolgimento dell'utente** tramite diversi canali e strumenti, specificamente definiti in funzione delle caratteristiche ricoperte nell'organizzazione delle PA e dei rischi di sicurezza ad esso pertinenti; ✓Utilizzo di **canali e-learning** che facilitano l'accesso continuativo ai servizi e coinvolgono l'utente in percorsi di formazione progressivi nel tempo, con contenuti che possono essere usufruiti secondo le disponibilità operative; ✓Sviluppo di contenuti formativi tramite le **agenzie di Accenture dedicate** al mondo della comunicazione e dell'interattività così da fornire format e qualità di contenuti video e grafici adeguati ad ottenere un forte livello di engagement sulla tematica; ✓Supporto della Fastweb Digital Academy che ha l'obiettivo di portare un contributo alla crescita di innovazione e cultura digitale nella società italiana tramite la definizione di corsi di formazione in Cybersecurity; ✓Adozione di **strumenti di verifica** del livello di formazione acquisito sulla base di meccanismi basati su analytics e AI per la somministrazione di test di verifica specifici, simulazioni (real life assessment) e certificazione / riconoscimento dei risultati raggiunti; ✓Disponibilità di **personale altamente specializzato** e certificato su tematiche di sicurezza informatica e continuità operativa (certificazioni ISO 27001, ISO 22310, CSX, CISA, CISSP, CISM) che predispone, sviluppa specificamente ed eroga i contenuti formativi; ✓Disponibilità, su richiesta, di **interventi formativi dedicati** da erogare in aula o comunque con risorse dedicate alle singole PA.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: IVASS, ASL Frosinone

Private: primario Gruppo assicurativo europeo, primario Gruppo bancario europeo, 2 primari Gruppi bancari italiani, primario operatore in ambito Pagamenti, associazione di categoria di imprese italiane

Descrizione di casi di successo - Si rimanda al §14.2.

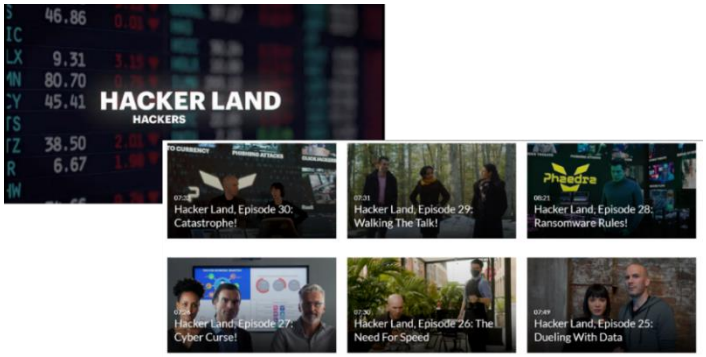
14.1 Metodologia e asset disponibili

I contenuti di sicurezza informatica richiedono approcci specialistici per poter essere efficaci in quanto si rivolgono ad una platea molto eterogenea in termini di competenze e necessità. A tal fine Accenture ha definito una metodologia specifica, denominata **Accenture Security Awareness Journey**, che intende adottare per poter indirizzare al meglio gli interventi verso ciascuna categoria di utenti. Secondo tale metodologia, ciascuna iniziativa deve rispondere a 3 specifiche domande: **Who, What, How**, quali sono i target dell'iniziativa, quali contenuti devono essere sviluppati e qual è il mezzo di comunicazione più efficace tenuto conto dei messaggi da veicolare e dei target a cui questi sono rivolti. È inoltre previsto che lo sviluppo della consapevolezza nelle persone e l'efficacia del programma siano supportati da metriche e strumenti di monitoraggio appropriati. Per ogni iniziativa è impostato e analizzato un KPI specifico.

Tale approccio consente di definire un modello di servizio specifico per le PA che prevede: ✓**Segmentazione audience**: identificazione e clusterizzazione dei target da coinvolgere nel programma di formazione distinguendo il personale operativo dal personale con ruoli di responsabilità ✓**Definizione canale di erogazione**: identificazione del canale di erogazione delle iniziative (privilegiando il canale e-learning ritenuto il più efficace per raggiungere il personale delle PA) ✓**Sviluppo dei contenuti**: definizione dei contenuti da erogare in funzione del target identificato e aggiornamento degli stessi con cadenza periodica in base all'evoluzione

delle minacce di sicurezza e del contesto operativo delle PA ✓**Erogazione dei contenuti**: fornitura del servizio di e-learning tramite piattaforma dedicata su cui vengono abilitati gli utenti e che include i moduli di verifica dell'apprendimento e programmazione, su specifica richiesta, di sessioni in aula e/o da remoto con specialisti di sicurezza per l'approfondimento di specifiche tematiche ✓**Verifica apprendimento**: introduzione di strumenti di verifica delle competenze tramite campagne interattive (es. simulazioni di phishing) e campagne di gaming.

In termini di asset Accenture dispone di una propria piattaforma e-Learning descritta nel §14.4 che include strumenti di formazione già utilizzati e testati in tema di security awareness. Tale piattaforma, include in particolare i moduli **Hackerland**, una serie di video, di pillole formative e di test specificamente sviluppati per utenti esperti e non esperti su tematiche di Cyber Security tra cui, a titolo esemplificativo: ✓Come lavorare in sicurezza da casa; ✓Come evitare attacchi ransomware; ✓Come gestire le mail di phishing. Questi contenuti sono per altro conformi a quanto messo a disposizione in termini metodologici **da AgID per le PA**. La piattaforma è adottata da Accenture a livello globale per tutti i propri dipendenti e potrà essere sviluppata ad hoc in base alle esigenze formative delle PA contraenti.



14.2 Competenze

L'erogazione di servizi di Security Awareness richiede l'integrazione di diverse competenze su cui Accenture dispone di risorse riconosciute a livello di mercato: ✓**Competenze in ambito Cyber security** al fine di proporre e definire contenuti adeguati alle esigenze delle PA; ✓**Competenze in ambito comunicazione/media** per poter identificare le migliori metodologie per il coinvolgimento degli utenti; ✓**Competenze in ambito sviluppo e gestione applicativa** per poter implementare strumenti di e-learning in modalità efficace. Accenture dispone di competenze fortemente specialistiche in tema di Security Awareness e le valorizza integrando risorse con formazione in ambito cyber security con risorse con formazione finalizzata a sviluppare ed erogare contenuti agli utenti finali. L'utilizzo di queste competenze ha permesso di raggiungere risultati estremamente significativi presso i Clienti italiani ed europei di Accenture: ✓Presso un **primario Gruppo assicurativo europeo** la prima campagna di security awareness ha raggiunto il 98% - quasi 13.000 - dipendenti; il successo dell'iniziativa, oltre all'elevatissima numerosità degli utenti che hanno aderito, è dimostrata dalle attività di verifica eseguite tramite campagne di phishing che hanno portato ad una diminuzione del tasso di esecuzione di operazioni malevole (click sui link malevoli riportati nelle mail) al 20% rispetto ad un tasso di partenza pari al 39%. ✓Presso un **primario Gruppo bancario italiano** sono stati erogati interventi di security awareness finalizzati ad aumentare il livello di consapevolezza dei dipendenti di tutto il Gruppo (oltre 90.000 dipendenti in 108 Legal Entities) su svariati aspetti di cyber security; Accenture ha implementato e gestito una specifica Security Academy predisponendo contenuti formativi specifici e definendo metriche specifiche di misurazione dei risultati che hanno evidenziato come circa il 98% degli utenti hanno completato il percorso formativo nei tempi predefiniti. ✓Presso un **primario operatore in ambito Payments** sono stati erogati interventi formativi predisponendo materiale dedicato quali brochure, screensaver, newsletter, ecc.; l'intervento ha coinvolto circa 1.300 dipendenti e ha portato a una riduzione del tasso di esecuzione di operazioni malevole dal 42% al 26%. ✓Presso **un'associazione di categoria di imprese italiane** è stata condotta una campagna di alfabetizzazione alla sicurezza informatica, volta a fornire ai propri dipendenti un set di conoscenze utili a prevenire, tramite adeguata consapevolezza, incidenti di sicurezza che avrebbero potuto mettere a rischio la sicurezza dei dati trattati, alcuni anche particolari, in ottica GDPR; il successo dell'iniziativa è testimoniato dalla progressiva estensione dell'intervento ad un parco utenti sempre più esteso, sia di natura IT che non IT.

In aggiunta Accenture eroga servizi di Security Awareness tramite **interventi diretti nelle Università italiane** al fine di promuovere la diffusione della cultura di sicurezza, oltre che tramite la partecipazione a Osservatori e Centri di Ricerca nazionali e istituzionali. Lo stesso avviene nell'ambito di eventi specifici dedicati alla community di cybersecurity aperti al pubblico o per specifici Clienti. Si evidenzia inoltre: ✓**Accenture Cybergame** organizzato in diverse sedi, tra cui il Cybertech Europe, uno degli eventi più importanti in ambito cyber security e che, tramite l'adozione di modalità interattive e di gaming, ha consentito a studenti/ricercatori di sfidarsi tentando di violare i sistemi di un'ipotetica azienda e ricevendo supporto/formazione da parte degli esperti di Accenture ✓la **CISO Academy**, un evento formativo specificamente dedicato ai CISO delle più grandi aziende mondiali al fine di discutere le modalità di sviluppo delle soluzioni di cyber security e condividere ambiti di miglioramento anche tramite sessioni di design thinking specifiche.

14.3 Proposte innovative - Canali e strumenti

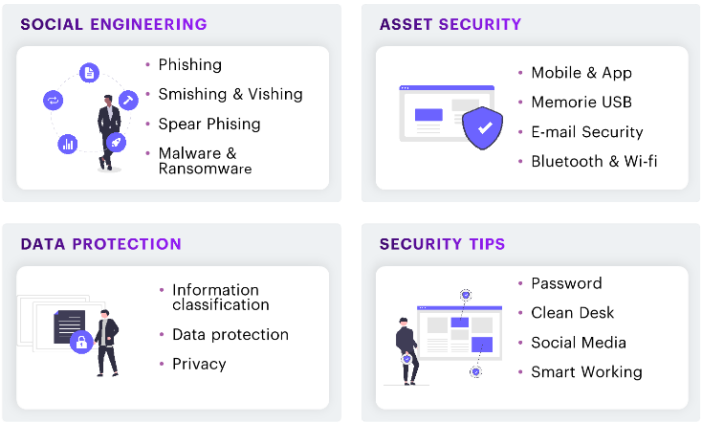
- Erogheremo i servizi di awareness utilizzando canali e strumenti che saranno studiati specificamente per rispondere alle esigenze dei singoli utenti e che saranno definite in funzione di: ✓**rischi di sicurezza** indotti da ruolo/mansione ricoperti e dagli strumenti informatici utilizzati ✓**livello di conoscenza** di partenza verificato tramite test di valutazione ✓**disponibilità di tempo e strumenti** per accedere ai servizi di awareness. Tra i canali e gli strumenti che si intende utilizzare si evidenziano: ✓**Training online**: corsi di formazione basati sul web, di alta qualità e con un design reattivo. Offrono ai discenti l'opportunità di comprendere i principali argomenti relativi alla sicurezza informatica in un brevissimo lasso di tempo utilizzando esempi pratici. Gli elementi interattivi trasformano il corso in una vera esperienza per il discente e forniscono quindi un modo efficiente per custodire i messaggi chiave rilevanti; ✓**Corsi in aula**: sessioni dedicate a specifici gruppi di utenti su tematiche

predefinite o studiate ad hoc rispetto alle esigenze delle PA erogate da personale specializzato su tematiche di cyber security; ✓**Newsletter e E-Card**: invio di messaggi puntali tramite newsletter o eCard per condividere informazioni e aggiornamenti in modo rapido e conciso a molte persone, garantendo una diffusione efficace delle informazioni senza un sovraccarico delle stesse; ✓**Webinar**: lezioni da remoto di esperti riconosciuti. A seconda del livello di dettaglio e dell'argomento desiderato, la gamma di possibili relatori spazia da specialisti IT a criminologi, giornalisti e autori accademici. Da brevi discorsi di apertura a presentazioni dettagliate: il tipo e l'ambito della lezione possono essere organizzati individualmente; ✓**Flyer e brochure**: vasta gamma di prodotti stampati relativi alla sicurezza informatica. Ogni prodotto è pensato per un target specifico e si distingue per il suo design unico. Sono un formato accessibile per presentare in modo conciso argomenti complessi in modo che possano essere visualizzati a colpo d'occhio; ✓**Quiz**: gli argomenti sulla sicurezza informatica sono ottimi contenuti per i quiz. Un quiz combina un'attività interattiva e informazioni in un formato perfetto sia per testare che per aggiornare le conoscenze esistenti sulla gestione sicura dei dati digitali; ✓**Campagne di simulazioni**: le simulazioni vanno oltre il puro contenuto di apprendimento, sono dimostrazioni realistiche, come l'invio di e-mail sospette, che possono essere utilizzate per evidenziare l'importanza di essere cauti con le e-mail e, in generale, aumentare la consapevolezza dei discenti; ✓**Podcast**: i podcast sono un modo ideale per trasmettere regolarmente brevi informazioni in un formato stimolante e compatto, soprattutto per contenuti a lungo termine. I discenti possono essere informati a lungo termine attraverso discussioni con esperti ed esperienze reali sui temi della sicurezza informatica; ✓**Consigli del giorno**: il formato "consigli del giorno" offre l'opportunità di fornire ai discenti consigli utili sulla sicurezza informatica. Brevi consigli, domande o inviti all'autoriflessione posti all'interno di questo formato aiutano ad aggiornare e consolidare le proprie conoscenze e a renderne più facile l'attuazione; ✓**Ebook periodici** su aspetti di cyber security per tutti i dipendenti da inviare tramite mail; forniscono strumenti utili, suggerimenti pratici e tutto quello che è necessario sapere per proteggere i dispositivi e i dati personali degli utenti quando connessi in rete. Il gradimento dei discenti su canali e strumenti sarà raccolto tramite questionari somministrati su **LimeSurvey** (cfr. indicatore IQA_SUTR, §14.5).

14.4 La piattaforma di formazione

Al fine di indirizzare le esigenze delle Amministrazioni, rendiamo disponibile la piattaforma di e-learning **"Accenture Security Training"** sviluppata negli anni anche sulla base dell'esperienza interna di utilizzo dei moduli Hackerland, installata presso il Centro Servizi e aggiornata di continuo in termini di contenuti informativi. Gli utenti potranno accedere tramite il Portale della fornitura che gestirà i processi di accesso e autenticazione in modalità sicura e reindirizzerà direttamente gli utenti sulla piattaforma target. La piattaforma prevede una struttura modulare che include: ✓**Sezione di Awareness**. Un innovativo sistema integrato di e-Learning che consente di coinvolgere tutta l'organizzazione in un percorso di apprendimento che sia al contempo educativo e stimolante; ✓**Sezione Phishing**. Un innovativo sistema di e-training, in funzione AntiPhishing, che produce risultati efficaci grazie alla sua metodologia di training on the job e alle caratteristiche di automazione e ML; ✓**Sezione Informativa**. Un percorso di formazione video basato su una metodologia induttiva e realizzato con tecniche di produzione avanzata e con uno storytelling particolarmente coinvolgente. All'interno di questa sezione sono collocati i moduli Hackerland.

La **Sezione di Awareness** è progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, con un approccio a rilascio costante e graduale: ✓la formazione impegna il partecipante per pochi minuti a settimana, con un percorso che ne mantiene elevata l'attenzione ✓tutte le lezioni sono disponibili in formato multimediale, con la possibilità di fruire dei contenuti sia in formato video sia in formato testo ✓il linguaggio divulgativo è pensato per poter essere fruito dal personale non specializzato nella Cyber Security ✓ogni lezione è corredata da test di valutazione del livello di apprendimento ✓la metodologia di Gamification, corredata da premi e riconoscimenti, stimola l'apprendimento e premia l'eccellenza ✓l'organizzazione in team consente di attivare competizioni virtuose e coinvolgenti tra team diversi ✓le funzioni di Student Caring automatiche, attraverso sollecitazioni e reminder ad hoc, motivano la partecipazione ✓ogni modulo formativo è auto-consistente perché affronta uno specifico argomento critico ✓ogni modulo è disponibile multilingua.



In figura alcuni dei contenuti, che tengono conto dell'analisi svolta relativamente al corso reso disponibile dall'AgID e ai relativi contenuti affrontati, resi disponibili sulla piattaforma che saranno progressivamente aggiornati nel tempo, per poterli adattare alle esigenze delle PA e al contesto dinamico delle minacce di sicurezza.

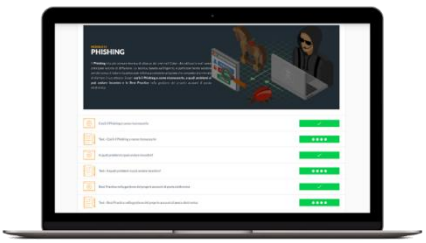
La **Sezione Phishing** è focalizzata su quello che si conferma essere il principale punto di vulnerabilità delle organizzazioni pubbliche e private. Il programma di esercitazione si basa sull'apprendimento esperienziale. L'utente viene sottoposto con frequenza variabile, ma con continuità, ad attacchi simulati che tendenzialmente sono destinati a diventare sempre più complessi e sfidanti.

Il modulo segue un processo adattivo per modellare le campagne di simulazione, con lo scopo di aumentare l'efficacia dell'esercitazione, riproducendo l'esperienza reale dell'utente e le strategie di attacco adottate dai criminali Cyber. Le simulazioni vengono specializzate automaticamente sulla base del profilo comportamentale dell'utente, seguendo la logica del "personal training", con una metodologia che sottopone l'utente a un programma di esercitazione che tiene conto della capacità dell'individuo di resistere agli attacchi. Ogni volta che l'utente fallirà la simulazione, attivando l'azione ingannevole verrà esposto direttamente a un intervento formativo di Awareness, intervento che fornirà dettagli sulla tipologia di attacco subito.

È prevista una specifica funzionalità di reportistica, fruibile attraverso una **dashboard**, che consente, grazie a metriche avanzate, di valutare il rischio e di seguire la sua concreta riduzione durante l'avanzare del programma.

La **Sezione Informativa** è composta da una serie di video focalizzati sulle principali minacce Cyber e su come queste possono concretamente colpire individui e

organizzazioni. I contenuti sono arricchiti di tutte le componenti di access control, engagement e monitoring proprie della piattaforma e sono raccontati con stili diversi, da quello cyber-investigativo a quello cyber-news, per renderlo ancora più attrattivo e ingaggiante.

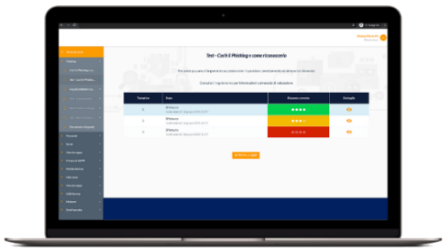


La piattaforma sarà resa disponibile secondo 2 percorsi, definiti **base** e **avanzato**, così da indirizzare l'esigenza di cluster differenti. Il percorso base include un subset di contenuti per ciascun modulo ed è destinato agli utenti che hanno minori necessità formative in ambito cyber security, mentre il percorso avanzato include tutti i contenuti resi disponibili.

Nello specifico il percorso base include 4 contenuti del modulo di Awareness, 4 video del modulo informativo e 4 attacchi simulati per il modulo di phishing. Il percorso avanzato include invece 36 contenuti del modulo di Awareness (erogati agli intervalli che si ritiene di definire), 6 video del modulo informativo e non prevede un limite di attacchi simulati, così da garantire un percorso modulare basato sul profilo comportamentale del singolo utente. In fase di attivazione del servizio, si procederà con l'Amministrazione richiedente ad articolare le modalità di accesso ai 2 percorsi e a valutare la necessità di attivare anche una o più lezioni in aula con specialisti di sicurezza su specifiche tematiche.

14.5 Tecniche innovative di verifica dei livelli di awareness raggiunti

All'interno delle attività previste sono incluse quelle finalizzate alla raccolta degli esiti di ciascuna iniziativa aventi lo scopo di monitorare l'andamento del programma di awareness e di verificare i risultati raggiunti ed il livello di sensibilizzazione degli utenti. Sono previste differenti modalità per le attività di verifica e sensibilizzazione volte a garantire: ✓Un monitoraggio costante durante il rilascio delle iniziative previste per garantire che tali iniziative siano sempre efficaci e che eventuali lesson learnt possano essere sfruttate per le iniziative non ancora lanciate ✓La misurazione del livello di consapevolezza che i discenti hanno raggiunto partecipando ad ogni singola iniziativa ✓La misurazione del livello di consapevolezza che i target hanno raggiunto partecipando al programma di Security Awareness nel suo complesso, attraverso un innovativo sistema di e-training, con una funzione Anti-Phishing e Anti-Smishing, che produce risultati efficaci grazie alla sua metodologia di training on the job e alle sue caratteristiche di automazione e adattività con l'ausilio di AI ✓La misurazione del livello di consapevolezza che l'Amministrazione ha raggiunto partecipando al programma di Security Awareness ✓Un costante coinvolgimento dei target che devono essere raggiunti dalle iniziative previste dal programma di Security Awareness.



Le componenti della piattaforma per la verifica delle conoscenze acquisite dall'utente e dell'effettiva capacità di mettere in atto quanto appreso, sono: ✓**Quiz** (verifica di tipo formale, attraverso test di verifica relativi agli argomenti delle singole lezioni): ✓Ogni lezione è corredata da test di valutazione del livello di apprendimento; ✓Trimestralmente è proposta agli utenti una verifica intermedia dell'apprendimento che ha il duplice scopo di verificare le conoscenze apprese e consolidare le nozioni apprese fino a quel momento. ✓**Campagna di phishing** (verifica di tipo esperienziale, attraverso "verifiche sul campo" della capacità di reazione dell'utente alla minaccia cyber attraverso un simulatore di campagne di Phishing e Smishing): ✓Le simulazioni sono gestite attraverso un sistema di AI, per essere automaticamente modulate sulla base del profilo comportamentale del singolo utente e della sua capacità di resistere agli attacchi ✓Le simulazioni sono organizzate, come impostazione predefinita, a cadenza mensile, tale cadenza può essere modificata e personalizzata in base alle esigenze dell'azienda ✓Ogni volta che l'utente fallirà la simulazione, verrà indirizzato direttamente ad un intervento formativo di Awareness con dettagli sulla tipologia di attacco subito.

In aggiunta, attraverso la funzionalità di recupero del debito formativo, il sistema individua gruppi di utenti la cui curva di apprendimento è inferiore alla media aziendale e suggerisce attività di training / verifica esperienziale al fine di recuperare il gap comportamentale, in termini di Cyber Strenght.

La piattaforma offre, inoltre, un'efficace reportistica, in grado di soddisfare le esigenze di tutte le figure professionali coinvolte nelle attività di verifica e i ruoli specifici che sono coinvolti nei programmi formativi e addestrativi, quale: ✓**Reportistica per gli utenti**, che fornisce una fotografia chiara dell'andamento del percorso individuale, fornendo anche un metro di paragone altrettanto chiaro con il resto dell'azienda. Di particolare impatto la reportistica relativa alle funzioni di gamification, con l'esposizione delle classifiche. ✓**Reportistica** per **i supervisori**, con l'analisi aggregata e di dettaglio di numerosi KPI di partecipazione e con l'esposizione degli indicatori relativi alla gamification "a squadre"; reportistica facilmente esportabile ai fini della comunicazione interna. ✓**Reportistica per le risorse** umane, con indicatori di partecipazione tracciati al livello massimo di dettaglio (lezione/utente). ✓**Reportistica dedicata alla** competizione **"a squadre"**, con la possibilità di identificare la figura del "team leader", in grado di agire da motivatore della propria squadra, anche grazie ad una serie di tool a supporto della funzione. ✓**Reportistica specifica delle "**verifiche **sul campo"** (Phishing e Smishing), di particolare interesse anche per le funzioni di Cyber Security, con analisi aggregata e di dettaglio, non solo dei dati relativi al click-rate, ma anche ad una serie di indicatori di rischio particolarmente sofisticati, in grado di diventare supporto indispensabile ad eventuali azioni di remediation. ✓**Un report**, creato automaticamente **in formato presentazione**, che consente di comunicare i risultati degli interventi **ai livelli direzionali**.

Infine, nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "FORMAZIONE E SECURITY AWARENESS"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_SUTR	Soddisfazione utenti training valutata tramite questionario somministrato ai discenti e-learning	% di risposte "Soddisfatto" / risposte complessive	Trimestre	SUTR>80%
PCI_SLCS	Come SLCS	Come SLCS ma frequenza maggiore e soglia più bassa	Mensile	PCI_SLCS =1
KPI_FTAP	Fallimento test anti-phishing	% di soggetti che hanno fallito il test anti-phishing per ciascuna campagna	Evento	Riduzione rispetto misura precedente

15 PRESENZA DI ULTERIORI FUNZIONALITÀ AGGIUNTIVE

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

16 PORTALE DELLA FORNITURA

Principale strumento a supporto dei processi di interazione e comunicazione è il **Portale della Fornitura**, punto di accesso alle informazioni e ai repository sull'AQ e agli strumenti di gestione e di erogazione dei servizi da parte di tutti gli stakeholder, secondo vari livelli di abilitazione. Il suo disegno è frutto dell'esperienza di successo che le aziende dell'RTI hanno accumulato sui portali di fornitura (es. Accenture nel CQ Sistemi Gestionali Integrati e negli AQ Digital Transformation e Servizi Applicativi Cloud nonché Fastweb nel CQ SPC Cloud L2), dalla quale traiamo spunto per alimentare una costante evoluzione di funzionalità erogate e tecnologie sottostanti. Il Portale rappresenta sia la vetrina sui servizi in essere e uno strumento di collaborazione e condivisione delle esperienze tra le PA sia lo strumento di gestione dell'AQ; è realizzato con una **soluzione robusta e rapidamente adattabile** a ogni esigenza, grazie a molti strumenti **nativamente integrati** che abilitano gli stakeholder all'uso di numerose funzioni di collaborazione. Lo strumento integra: ✓un front-end pubblico realizzato su tecnologia open source Drupal ✓un back-end basato su prodotti MS Office365 e funzionalità realizzate ad-hoc ✓piattaforme di monitoraggio (Power BI) per l'analisi dell'utilizzo del portale e degli indicatori di sintesi dei contratti ✓funzionalità di knowledge management supportate da algoritmi di AI. Particolare importanza è data agli aspetti di Business Intelligence ad uso sia delle singole PA ma soprattutto di Consip e degli Organismi di Controllo; le funzioni di monitoraggio implementate permettono dunque di avere una vista su tutti gli aspetti di performance relativi all'AQ.

In particolare, attraverso l'accesso profilato alle singole PA e alla fruibilità multicanale il portale si pone come lo strumento di knowledge sharing abilitante la condivisione tempestiva delle best practice e delle informazioni tra le Amministrazioni.

Il Portale funge da principale punto di accesso grazie alla sua integrazione con le soluzioni adottate per l'esecuzione dei contratti quali, ad esempio, la piattaforma **ServiceNow** (leader nel workflow e knowledge management, cfr. §4), le componenti ITSM, PPM, Performance Analytics e SLA Management. La massima integrazione tra gli strumenti di governo della fornitura e le soluzioni tecnologiche utilizzate per l'erogazione dei contratti di fornitura è abilitata da uno strato di API, realizzate in formato standard SOAP e REST seguendo le indicazioni di AgID. ServiceNow mette a disposizione anche una innovativa soluzione di **knowledge management** basata sull'impiego di un datalake di fornitura che consentirà di implementare la knowledge base, fruibile da tutte le risorse del RTI e delle Amministrazioni secondo modalità innovative (es. ricerche in linguaggio naturale) e sulla quale si potranno effettuare attività di correlazione dati/ML producendo razionali/report a supporto della successiva erogazione (es. elementi tecnici impiegabili nell'analisi di nuovi contesti o per velocizzare il problem solving nell'ambito della maintenance) o avere accesso ad informazioni particolarmente importanti (es. le lessons learned).

16.1 Soluzioni tecnologiche e funzionalità del Portale di fornitura

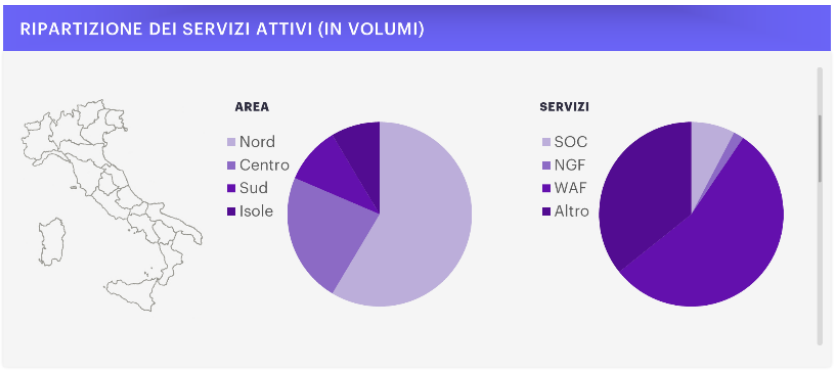
Il Portale della Fornitura è realizzato in modo da essere utilizzabile secondo le indicazioni dell'AgID e nel rispetto delle linee guida di **accessibilità** che garantiscono la fruizione a tutte le categorie di utente. Il progetto di implementazione segue a tale scopo un approccio di **User Center Design** (UCD) e reattivo, grazie alla dinamicità delle soluzioni proposte, e un approccio di **Continuous Improvement** basato sui feedback ricevuti dagli utenti e sulle analisi condotte sui dati di web analytics, questi ultimi raccolti grazie a **Google Analytics** o strumenti analoghi. L'intero Portale è realizzato con interfacce **responsive** per essere fruibile indipendentemente dalla piattaforma utilizzata (desktop, tablet, smartphone). Ulteriore potenziamento dell'esperienza **Mobile** è fornito dalla funzionalità offerte out of the box dall'app mobile Teams che, in quanto integrata con il portale, permette all'utente di accedere alle **funzioni di collaborazione** e di ricevere le notifiche rilevanti anche attraverso lo smartphone. Per assicurare il raggiungimento dei più alti livelli di usabilità, in accordo e in collaborazione con Consip, potranno essere condotti in corso d'opera dei test di usabilità individuando un campione di utenti e utilizzando il **protocollo eGLU LG 2018.1**, citato anche all'interno del **Piano triennale per l'Informatica nella PA 2020–2022**, che permette una semplice e immediata valutazione del portale da parte degli utenti finali e la conseguente individuazione di interventi migliorativi; questo anche grazie all'ampia esperienza maturata in portali compatibili con le linee guida AGID (es. INAIL, MEF). Per la realizzazione del portale prevediamo l'integrazione con il sistema di autenticazione **SPID** (Sistema Pubblico di Identità Digitale), in modo da agevolare l'accesso alle aree post-login da parte degli utenti PA, e l'integrazione con strumenti **Office 365** e funzionalità custom che permettono non solo di coprire tutte le richieste del Capitolato Tecnico ma anche di fornire ulteriori funzioni, nell'ottica di formulare una proposta migliorativa rispetto ai requisiti di base. Il portale, i cui oneri di hosting, gestione e aggiornamento mensile dei contenuti sono a carico del RTI, è supportato da un'attenta configurazione della profilazione degli utenti, al fine di gestire in sicurezza l'accesso alle informazioni presenti. In particolare, l'utente non accreditato naviga l'Area Pubblica a disposizione senza necessità di registrazione, mentre le altre aree del portale sono riservate a utenti profilati che accedono tramite l'inserimento di credenziali appositamente create o grazie all'integrazione con SPID. Gli utenti possono essere appartenenti ai fornitori di servizi, alle PA, agli **Organismi di coordinamento e controllo** o a terze strutture appositamente indicate. La soluzione può contare su un alto livello di sicurezza applicativa, in parte garantito direttamente dalla tipologia delle licenze che saranno utilizzate. Si elencano di seguito alcune peculiarità: ✓**abilitazione del**

doppio fattore di autenticazione, particolarmente utile per le utenze amministrative e con ampi permessi (es. utenze dedicate agli organismi controllori); accesso condizionale basato su dispositivo per bloccare o limitare l'accesso su dispositivi non gestiti; criteri per disconnettere gli utenti dalle sessioni dopo un periodo di inattività ✓**prevenzione perdita dei dati** su più livelli, quali: criteri per identificare i documenti e impedirne la condivisione; Limite alla sincronizzazione dei dispositivi in domini specificati ✓**crittografia** per l'utilizzo di **Microsoft Teams** e SharePoint Online, mantenendo al sicuro la messaggistica istantanea, riunioni e siti dei team. È consentito solo l'accesso sicuro. Non verranno effettuate connessioni autenticate tramite HTTP, ma verranno invece reindirizzate a HTTPS. I dati sono crittografati a livello di disco usando la crittografia BitLocker e a livello di file tramite chiavi. ✓ **La rete Yammer è privata**. Solo gli utenti con un indirizzo di posta elettronica valido e verificato possono accedere a Yammer, social network di Enterprise con sicurezza integrata a tutti i livelli. Yammer è conforme al livello C nel framework di conformità di Office 365, che soddisfa le clausole del modello SOC 1, SOC 2 e ISO 27001.

Per maggiori dettagli sulla strutturazione delle aree del Portale, le relative funzionalità e modalità di interazione con le Amministrazioni si invita alla consultazione del §16.2 Soluzioni e/o processi e/o strumenti di comunicazione e di collaborazione in chiave "social" con le Amministrazioni.

16.1.1 Strumenti di analisi dei dati e reporting

Tutte le funzionalità di reportistica sono progettate grazie al framework **Accenture Data Driven**: una tecnica di gestione e visualizzazione dei dati volta ad acquisire Data Fluency, vale a dire la capacità di leggere i dati e trarne **insights a supporto delle decisioni**. Proponiamo l'utilizzo di **Power BI** per tutti gli aspetti legati alla reportistica, in particolare nelle aree **Collaborazione e Monitoraggio** e **Osservatori**. Lo strumento, tramite **report statici e dinamici**, offre agli Organismi di Coordinamento e alle PA la possibilità di effettuare analisi multidimensionali su tutti i parametri espressi all'interno del Capitolato: ✓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 Servizi sottoscritti. Particolare attenzione è rivolta alla realizzazione dei cruscotti di monitoraggio relativi ai Piani dei Fabbisogni, Piani Operativi e Servizi in Esecuzione. 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.



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

16.2 Soluzioni e/o processi e/o strumenti di comunicazione e di collaborazione in chiave "social" con le Amministrazioni

Tra gli obietti del Portale della Fornitura c'è quello di favorire la collaborazione e la comunicazione tra le varie PA che partecipano all'AQ: in questo modo le soluzioni implementate presso un'amministrazione possono essere condivise e riutilizzate dalle altre PA. Il portale prevede l'implementazione di funzioni abilitanti per la collaborazione tra le PA tramite l'utilizzo di **MS Teams** e **MS Yammer**, opportunamente integrati nel Portale della Fornitura. Gli utenti hanno quindi la possibilità di creare ambienti virtuali di collaborazione, gruppi di lavoro, organizzare riunioni e web conference. L'efficacia e la potenza di questi strumenti di **Digital Workplace** trova conferma nella capacità del RTI di garantire il funzionamento senza soluzione di continuità di sistemi strategici nazionali. Un ruolo fondamentale viene svolto dall'Area **Collaborazione e Monitoraggio**, all'interno della quale la componente **Yammer** permette di creare un vero e proprio **Entreprise Social Network** in grado di favorire la condivisione delle esperienze e del know how in modalità social. Lo streaming social permette alle PA di condividere i propri risultati ma anche di consultare i risultati ottenuti dalle altre PA, con la possibilità di accedere alle informazioni di dettaglio. Grazie all'implementazione di un **motore di raccomandazione**, verranno mostrati dei post generati in automatico che consigliano all'utente di consultare determinati contenuti, quali schede di altre PA che hanno intrapreso percorsi affini, schede di descrizioni di nuove tecnologie/framework/soluzioni, risultati raggiunti da altre PA, condivisi per favorire il knowledge sharing e la collaborazione. Sulla piattaforma sono svolte analisi di **social listening**, volte a trovare e tracciare le conversazioni online attorno a specifiche keyword, frasi ed eventi e attorno allo specifico servizio o alla specifica PA. Ciò permette di ottenere feedback in real-time che aiuteranno a migliorare lo sviluppo dei servizi.

Area Comunicazione

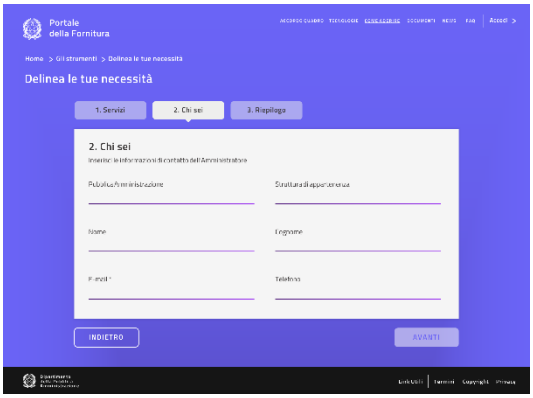
L'area in oggetto, aperta al pubblico, funge da vetrina per tutti i contratti in corso relativi all'AQ con l'obiettivo di esporre in maniera eloquente e completa tutte le informazioni necessarie alle singole PA per comprendere: ✓i vantaggi nell'aderire all'AQ e i benefici derivanti dall'accesso alle best practice e alla reportistica accessibile agli aderenti ✓le modalità di partecipazione. Gli strumenti che la landing page ha a disposizione sono: ✓**contenuti informativi e interattivi** esaustivi in formato testuale, grafico e video ✓**social proof** costituita dalle testimonianze delle PA aderenti raccolte nel corso dell'erogazione ✓**reportistica e documentazione** relativa alle iniziative svolte o in corso ✓strumenti **di simulazione e di contatto avanzati**. In accordo con Consip, è disponibile già in questa sezione il **Pre-Configuratore del piano dei fabbisogni,** ovvero lo strumento che permette alla PA di creare una prima versione del piano dei fabbisogni in modo semplice e intuitivo - attraverso una **user experience** mutuata dalle best practice dell'interazione dei portali e-commerce. La base dati del portale è costantemente aggiornata (tecnologie, trend, framework, procedure, ecc.) nel tempo. Al termine del processo, l'utente è invitato a eseguire il primo step per la registrazione al portale, propedeutico per l'adesione all'AQ, verificando l'utenza prima di procedere agli ulteriori step e dare i permessi di navigazione relativi. Per seguire l'andamento dell'AQ, nella parte bassa della pagina sono predisposti i canali Telegram, tramite iscrizione, mailing list e notifiche tramite WhatsApp, previo consenso a ricevere i contenuti.

L'utente PA dispone inoltre di **strumenti automatici per la richiesta di informazioni**: ✓**Assistente Virtuale**, addestrato per rispondere a tutti i quesiti relativi al funzionamento e alle modalità di adesione all'AQ formulati in linguaggio naturale, per apprendere e migliorare la capacità di risposta durante le interazioni ✓**FAQ** costantemente aggiornate per ricevere assistenza personalizzata: ✓**WhatsApp**, con un numero dedicato monitorato da un bot ✓**form** per richiedere di essere contattato ✓pagina social.

L'area Comunicazione, inoltre, costituisce lo strumento di promozione proattiva delle iniziative e dei servizi relativi all'AQ. I contenuti vengono constantemente aggiornati anche in base all'esperienza maturata dalle PPAA che già usufruiscono degli stessi, in modo tale da facilitarne la condivisione e la divulgazione. A tal proposito, i contenuti promozionali possono essere condivisi tramite l'utilizzo delle **funzionalità di social sharing integrate nel portale.** Ciò consente sia di aumentare la visibilità dei contenuti del portale verso una platea estesa, sia di **recepire e stimolare,** al suo interno, **le discussioni che nascono sui social sui contenuti condivisi**.

Area Informativa

Con le informazioni e gli strumenti che guidano concretamente la PA nell'aderire all'AQ, costituisce l'area di supporto e comunicazione di dettaglio riservata alle PA. In particolare, in una sotto-area dedicata la PA ha accesso a tutta la documentazione di riferimento per i servizi offerti all'interno dell'AQ, aggiornata e scaricabile, tra cui la guida alla stima e alla misurazione degli effort progettuali con dettagli su servizio/intervento. In un'apposita sottosezione sono inoltre contenute le descrizioni di tutte le soluzioni migliorative che il RTI mette a disposizione, e le pagine all'interno delle quali i modelli operativi sono resi in forma grafica, con spiegazioni di dettaglio a supporto; in questo modo viene fornita una chiara descrizione sulle caratteristiche specifiche, per indirizzare la scelta su un modello operativo piuttosto che un altro. Da quest'area è infine possibile accedere al **Configuratore del piano dei fabbisogni,** che costituisce lo strumento che il RTI mette a disposizione delle PA per supportarle nel delineare le proprie esigenze, con l'obiettivo finale di rendere l'adesione all'AQ il più efficace possibile. Il Configuratore guida l'utente attraverso tre passi: ✓il **primo** step prevede una serie predefinita di domande volte a delineare il contesto all'interno del quale la PA opera, identificare e quantificare le esigenze sulle quali si baserà il piano dei fabbisogni con il duplice obiettivo di tracciare le caratteristiche specifiche della PA e di definire una prima profilazione utile sia per il secondo step, sia per le funzioni implementate nelle altre sezioni del portale ✓il **secondo** step, grazie al supporto di un **motore di raccomandazione** e sulla base di un database all'interno del quale sono raccolte le esperienze delle altre PA e i dati di benchmark di mercato, guida l'utente in una serie di scelte che configurano ulteriormente la sua richiesta consigliando tecnologie, soluzioni, framework e altre specifiche ✓il **terzo** step permette di scaricare una prima versione del piano dei fabbisogni, salvata nella propria area personale e che costituisce il punto di inizio del processo di adesione all'AQ poiché, contestualmente o in qualsiasi altro momento, è possibile inviare il piano generato in modo da organizzare la consulenza di supporto con lo scopo di delineare definitivamente le esigenze. Quest'ultima fase viene abilitata dall'utilizzo di **riunioni online e strumenti di collaborazione** che permettono il confronto real time per perfezionare il piano condiviso.



A supporto del processo di individuazione e configurazione dei fabbisogni interviene la componente **Yammer** che favorisce la socializzazione delle esigenze e delle esperienze pregresse, sulla quale si innesta sia il dialogo diretto con **i** consulenti esperti dei bisogni della specifica PA e in grado di anticiparne le necessità, sia la shared knowledge, che si fonda sulla condivisione delle esperienze/deliverable. Gli esperti dell'AQ HUB ✓verificano con i Responsabili Tecnici dei servizi i deliverable e li rendono disponibili nel Portale debitamente sanitizzati ✓promuovono storytelling da parte dei protagonisti dei CE per sviluppare "forme di riconoscimento" in PA analoghe ✓inseriscono i contenuti all'interno di Yammer per favorire la discussione e la condivisione tra le PA.

Area Project Management

In quest'Area, ad accesso riservato e profilato, un PA può attivare, monitorare e gestire i contratti e i servizi/interventi affidati. Accedendo all'area Project Management, l'utente abilitato della PA inizia la navigazione con la selezione del Contratto di interesse, sia attivo che chiuso. La prima sezione nella parte superiore della pagina riguarda i **servizi in evidenza** che possono richiedere l'attenzione dell'utente per: recente cambio di stato, intervento di attivazione/approvazione richiesto, alert su indicatori di qualità, aggiunta di una nuova issue, superamento delle scadenze, ecc. L'utente ha quindi la possibilità di selezionare uno dei servizi per verificarne lo stato, entrando nella pagina specifica del servizio. Tale sezione incorpora le funzionalità di workflow per il ciclo di vita documentale (elaborazione documenti, approvazioni, review e modifiche tramite strumenti di collaboration). In particolare:

- **Funzionalità di validazione dei documenti e di approvazione da parte dell'Amministrazione**: L'approvazione di un documento si delinea come un processo fatto di diversi step, ognuno dei quali coinvolge determinati attori, che devono effettuare specifici controlli e decidere se il documento può procedere al prossimo step del flusso. L'utente abilitato della PA inizia la navigazione con la selezione del Contratto di interesse, all'interno del quale è presente la sezione dedicata alla gestione documentale e relativa archiviazione. È possibile generare/caricare a sistema differenti tipologie di documento, il cui **flusso approvativo** è preventivamente definito con l'individuazione dei "poteri di firma" sia lato PA sia lato RTI (Il ciclo di vita dei documenti ufficiali è definito nel Piano della Qualità Generale e verificabile nella Prima Release del Portale) e che saranno implementati a sistema tramite gestione della profilazione delle utenze, facendo ricorso ove necessario, a SPID e/o alla firma elettronica qualificata. La configurazione avviene attraverso lo strumento di **Workflow grafico**, completamente configurabile. I processi approvativi possono essere gestiti in modo centralizzato, tramite applicazione desktop o client web. Lo **stato di avanzamento** può essere mantenuto sotto controllo grazie ad un cruscotto: per ogni documento è possibile visualizzare a quale punto del flusso di approvazione si è arrivati, quali azioni sono state svolte da ogni utente e quando. In caso di necessità, inoltre, vi è la possibilità di delegare l'approvazione di un documento ad un altro collega abilitato.

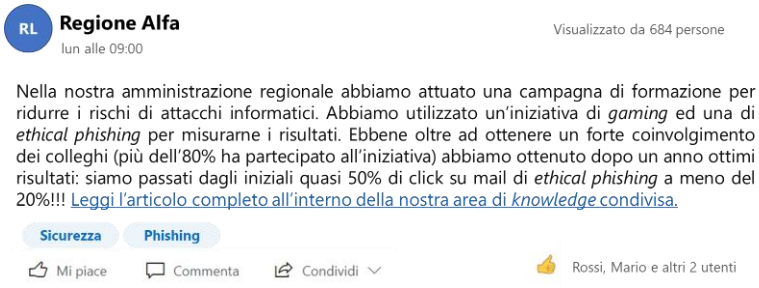
Ogni documento è classificato per tipologia, contraddistinto da un **codice identificativo univoco**, ne viene tracciato il versioning e lo storico dei cambi di stato, ivi incluso lo step approvativo. Lo scambio del documento tra i vari utenti è sempre tracciato in real time e le diverse versioni sono sempre disponibili, senza il rischio che qualcun altro lavori sul documento prima che l'utente incaricato della fase precedente abbia terminato il proprio task o ricevuto l'approvazione di quanto inserito. Inoltre, ogni utente riceve una **notifica** nel momento in cui è richiesto qualche tipo di approvazione.

- **Esecuzione del contratto esecutivo**: fase operativa in cui sono erogati i servizi: ✓il Team di PMO coordina le attività di Project/Program Management e di Risk Management ✓i Responsabili Tecnici dei Servizi coordinano le attività richieste. Al suo interno è presente la funzionalità di pianificazione e gestione, in particolare quella per richiedere l'Estensione dell'orario di servizio: l'utente abilitato della PA inizia la navigazione con la selezione del Contratto di interesse, all'interno del quale è presente la sezione dedicata alla gestione delle richieste di estensione dell'orario di servizio. In tale sezione è possibile inserire la richiesta, dettagliandone le nuove tempistiche/esigenze, con possibilità di aggiungere note esplicative o di supporto. Tale richiesta, che può essere effettuata anche via posta elettronica ad apposito indirizzo dedicato, genererà un "documento di richiesta", visualizzabile ed approvabile nella sezione dedicata alla validazione dei documenti.

- **Funzionalità di accesso ai CV**: il RTI pubblicherà i CV delle risorse proposte, compresi i Referenti tecnici e i ruoli aggiuntivi offerti. L'utente abilitato della PA potrà visionare i CV che saranno resi disponibili secondo i vincoli temporali previsti da bando di gara, con la possibilità di procedere con la richiesta di colloquio, approvare la risorsa o ritenerla non idonea, nel caso in cui seguirà sostituzione e nuovo colloquio.

Area Monitoraggio e Collaborazione

L'area ha un duplice obiettivo: 1) fornire una visione d'insieme sull'andamento dell'AQ mostrando dati relativi a tutte le iniziative intraprese dalle PA aderenti, elaborati attraverso strumenti di analisi dei dati e reporting; 2) favorire lo scambio di esperienze e informazioni tra le PA, per confrontare i risultati ottenuti e condividere il know how acquisito, attraverso le soluzioni e gli strumenti di collaboration messi a disposizione dal Portale. Le attività in esecuzione sono monitorate al fine di individuare criticità, attivare contromisure opportune e rendicontare ai Referenti della PA l'andamento dei servizi. Le PA, nella configurazione ed esecuzione di un servizio, generano nuove esperienze e nuove conoscenze che vanno a costituire parte della loro proprietà intellettuale. Le **funzionalità di Yammer aiutano a consolidare e capitalizzare tali esperienze**, a favore del miglioramento continuo dei servizi. Qualsiasi dubbio durante la routine lavorativa può essere risolto in pochi click in quanto le risposte arriveranno direttamente dalle persone più competenti. Crea un canale di formazione informale: possono essere creati canali di interesse sui quali è possibile caricare le risorse utili per affrontare tematiche ricorrenti, per accedervi ogni qualvolta è necessario, da qualsiasi dispositivo. Le comunità sono un modo potente per consentire agli utenti di condividere approfondimenti e domande. I feed delle chat vengono creati ad hoc per ogni utente sulla base dell'utilizzo dell'AI per evidenziare gli argomenti più critici, le personalizzazioni dell'interfaccia in base al servizio di interesse, l'organizzazione di discussione ottimizzata e la rapida condivisione dei messaggi tramite l'applicazione mobile.



Area Osservatori

In tale area, messa a disposizione degli **Organismi di coordinamento e controllo,** è possibile consultare la reportistica e i dati relativi agli aspetti di **qualità** dei singoli Contratti Esecutivi. Dal punto di vista dell'analisi dei dati e disponibilità di reportistica, oltre a poter richiedere tramite un'apposita funzione presente in menu l'accesso a tutte le aree del portale, hanno infatti a disposizione una Homepage specificatamente realizzata che permette, in modo semplificato, l'accesso alle funzioni di cui necessitano. In particolare, **nella parte superiore della pagina,** trova posto la casella di ricerca che permette di individuare i servizi o le amministrazioni a seconda delle esigenze. All'interno della Homepage, nella parte superiore, vengono riepilogati i servizi sui quali sono state rilevate delle criticità nei parametri

di monitoraggio: tramite questa vista, l'utente può accedere direttamente alla scheda di dettaglio del servizio e rilevare le eventuali problematiche in corso. A seguire è presente una sezione di reportistica, che anticipa in maniera aggregata i dati relativi a tutti i Contratti, eseguiti e in esecuzione, all'interno dell'AQ e infine, nella parte sottostante, vengono elencate le amministrazioni e i progetti afferenti all'AQ in modo da permettere un rapido accesso alle schermate di dettaglio.

17 INNOVAZIONE

La attività svolta dal RTI nell'**identificazione di attori chiave per l'innovazione**, porta allo sviluppo di relazioni con realtà emergenti da acquisire e in cui investire per favorirne la crescita e includerne le competenze nella propria offerta di servizi e/o prodotti in un'ottica di miglioramento continuo del processo di innovazione. Forrester ha recentemente classificato Accenture quale leader assoluto per gli "Innovation Consulting Services" ed "Innovation Consulting Service Providers" (Current Offering in the Forrester Wave™: Innovation Consulting Services, Q2 2021), evidenziando soprattutto come il portfolio di servizi di innovazione fornisca una offerta completa ed un processo end-to-end che va dal disegno di strategie di innovazione fino alla prototipizzazione ed al deployment su larga scala di quanto ideato e realizzato. Volano dell'innovazione per il RTI, Accenture e Fastweb fanno della collaborazione con soggetti innovativi e con i principali player tecnologici uno dei pilastri della propria *value proposition* che viene continuamente alimentata dalle costanti interazioni con università e centri di ricerca, oltre che da significativi investimenti in strutture di innovazione interne tra cui i centri di ricerca multidisciplinari, gli Accenture Labs, il network di centri di ricerca e laboratori di sicurezza di Fastweb, i molteplici poli di innovazione tematici e Accenture Ventures, **intera struttura dedicata all'*Open Innovation***: attraverso un rigoroso processo di selezione e affiancamento, le migliori start up entrano nel virtuoso processo di innovazione che consente di portare ai clienti soluzioni nuove ed efficaci a problemi complessi; la struttura opera in 45 paesi, con oltre 35 partner prioritari (cui sono destinati i maggiori investimenti) distribuiti su 10 *innovation segments* di industria tra cui la **cybersecurity** ha un ruolo primario con **oltre 100 startup** in portfolio.

Relativamente a Fastweb, grazie al suo profilo internazionale, ha investito in oltre 70 aziende tecnologiche, di cui numerose in ambito Cyber Security, attraverso la struttura, denominata "Venture Capital", che si compone di numerose collaborazioni nell'ambito del panorama delle start up. In questo quadro di attenzione focalizzata sull'innovazione, e in linea con i modelli che Accenture e le altre aziende del RTI promuovono per favorire la crescita e il coinvolgimento sul mercato di PMI e start-up innovative, si innesta la partecipazione della PMI innovativa **Difesa e Analisi Sistemi** (DEAS) che proponiamo come partner in grado di integrare le specializzazioni presenti nelle sue strutture sul tema della gestione delle vulnerabilità, della *threat intelligence* e della protezione dei sistemi.

17.1 Soggetti coinvolti e le loro principali caratteristiche

DEAS – Difesa E Analisi Sistemi nasce con l'idea di creare in Italia un polo di Cybersecurity e offrire un supporto globale alle Istituzioni e alle grandi imprese italiane. L'obiettivo di DEAS è diventare un modello di riferimento di Ricerca e Sviluppo nel Sistema Paese utilizzando innovative infrastrutture tecnologiche e fornendo soluzioni integrate di AI e servizi di sicurezza conformi ai più alti standard del settore. DEAS si presenta al mercato quale soggetto abilitatore sia per attività di audit centrale idonea alla legge-perimetro 105/2019 (PSNC) e alla compliance richiesta dal Centro di valutazione e certificazione nazionale (CVCN), sia per attività cyber a sostegno delle misure minime AgID, nel rispetto degli standard qualitativi previsti per operatori della PA centrale e locale non incluse nel PSNC. L'apporto di DEAS al RTI è rappresentato non soltanto dalla sua esperienza nella progettazione di soluzioni innovative di IA/ML ed erogazione di servizi di compliance, con percorsi per l'ottimizzazione e l'hardening dei sistemi informativi secondo gli standard AgID, ma soprattutto dalle capacità di sviluppo e implementazione di soluzioni integrate di difesa (Database Security, Endpoint Protection, Vulnerability Assessment, Security Probing) per il rafforzamento delle infrastrutture perimetrali.

Accenture è ad oggi il più grande player italiano in ambito cybersecurity per volumi di business e numero di risorse. Dispone in ambito cybersecurity di una fitta rete di **Cyber Fusion Centers (CFC)**, centri multidisciplinari di ricerca in cui professionisti cyber lavorano per monitorare la sicurezza e prevenire attacchi. Il **CFC di Napoli** è la principale struttura di tecnologia e innovazione nell'ambito della fornitura, sia a livello di AQ sia di CE, per offrire alle PA contraenti protezione e difesa, reattive e proattive, dalle minacce emergenti o esistenti. Il centro, cuore pulsante degli smart hub, è uno spazio di lavoro immersivo di oltre 600mq, che eroga servizi di Threat Intelligence, Managed Digital Identity, Managed Threat Operations, Managed Cloud Security, Digital Forensics ed Incident Response. Il CFC, che sfrutta la rete di strutture di innovazione su menzionate e il nutrito ecosistema di partnership tecnologiche, svolge il ruolo di collettore delle esperienze e del capitale, tangibile e intangibile, che esse mettono a disposizione. Il CFC di Napoli, inoltre, è il luogo in cui si concretizzano le iniziative di innovazione e formazione derivanti dalle collaborazioni di Accenture con gli atenei campani tra cui, le numerose attività di tesi specialistiche e la Cyberhackademy – corso di formazione basato su metodi di formazione innovativi voluto da Accenture e oggi alla sua seconda edizione in collaborazione con l'Università degli studi di Napoli Federico II.

Altre strutture **Accenture** coinvolte per apportare alla fornitura competenze in ambito PA e Cloud sono **a) Accenture Government Innovation Center** (**AGIC**), centro di Innovazione per la PA in cui le Amministrazioni possono conoscere le potenzialità dell'innovazione disponibile sul mercato e che fornisce uno spazio in cui sperimentare l'applicazione di nuove tecnologie e **b) Accenture Cloud Innovation Center** (**ACIC**) che offre competenze dedicate allo sviluppo e alla sperimentazione di soluzioni cloud con i partner tecnologici più rilevanti, per la prototipazione rapida di soluzioni *cloud-based* intrinsecamente sicure.

DEAS e Accenture forniscono al RTI i principali contributi di innovazione, descritti nel dettaglio al §17.2. Un fattivo supporto deriva, poi, dal contributo delle strutture di ricerca ed innovazione messe a disposizione dagli altri partner del RTI qui di seguito descritte.

Fincantieri NexTech è una società tecnologica di Fincantieri che sviluppa soluzioni nei settori della sicurezza e della protezione di informazione, rappresentando un **centro di competenza tecnologico del Gruppo**. Grazie alle esperienze nel settore militare e della sicurezza, alle competenze nell'analisi degli scenari operativi e alla capacità di realizzare sistemi complessi in "ambienti ostili", essa può supportare lo sviluppo e l'integrazione sia di soluzioni "legacy" - infrastrutture di campo basate su piattaforme tradizionali (SCADA) o su architettura SOA (Service Oriented Architecture) – e di erogare servizi SOC. Il contributo di **Fincantieri NexTech** in termini di innovazione deriva principalmente dalla collaborazione con le principali università e centri di ricerca, ad esempio grazie ai tre dottorati di ricerca finanziati in ambito cyber, e la partecipazione a progetti di ricerca nazionali e internazionali sui temi della sicurezza per ambienti militari e della difesa.

Fastweb è un MSSP (Managed Security Service Provider) ed eroga servizi di gestione operativa della sicurezza tramite il proprio SOC. Attraverso un **competence center e un osservatorio dedicati alla sicurezza,** da considerarsi integrati nella erogazione dei servizi connessi alla fornitura, Fastweb fornisce supporto ai servizi per adeguarsi in modo flessibile ed efficiente alle esigenze delle PA. Il principale contributo deriva da laboratori di sicurezza equipaggiati con **tecnologie all'avanguardia** per l'analisi di apparati embedded, strumentazioni di test e misura, centri dedicati a collaudi e prove tecniche per la certificazione di servizi e prodotti di sicurezza per la PA (es. Web Farm di **Roma** e **Milano**). Inoltre, Fastweb ha sviluppato un'infrastruttura IT, attraverso i propri Data Center distribuiti sul territorio

nazionale, che permette di erogare i più avanzati e complessi servizi a valore aggiunto (VAS) di cyber security. Fastweb dispone di una gamma completa e integrata di servizi di sicurezza, in modalità "on premise" e "as a service", in grado di soddisfare le esigenze di tutti i segmenti di mercato e di aziende di tutte le dimensioni, dalle start-up alle società di grandi dimensioni fino al settore pubblico. Con particolare riferimento ai servizi oggetto di gara, si citano a) **Fast Security 360°** che fornisce una difesa perimetrale completa e in tempo reale della rete aziendale da attacchi informatici, attraverso funzionalità implementate su apparati UTM (Unified Threat Management); b) **Fast KaleiDoS** per difendere le aziende e le PA dagli attacchi informatici DDoS (Distributed Denial of Service); c) **FAST Security Intelligence**, servizio di ricerca e Data Analytics, in grado di monitorare l'esposizione degli asset aziendali; d) **Fast Mail Security,** servizio di protezione della posta disponibile per Clienti con mail server ospitati on premises o con servizi di posta basati su infrastrutture di terze parti, e) **Fast Security - Advanced Protection** servizio che, utilizzando una tecnologia unica di analisi del traffico dell'endpoint, fornisce una protezione completa dagli attacchi APT, noti e non noti.

17.2 Ambito di intervento e valore aggiunto

Le strutture a supporto dell'innovazione proposte dal RTI sono parte integrante degli **smart hub,** sia a livello di AQ sia di singolo CE, e si focalizzano su ambiti di intervento specifici al fine di offrire valore aggiunto ai servizi oggetto della fornitura.

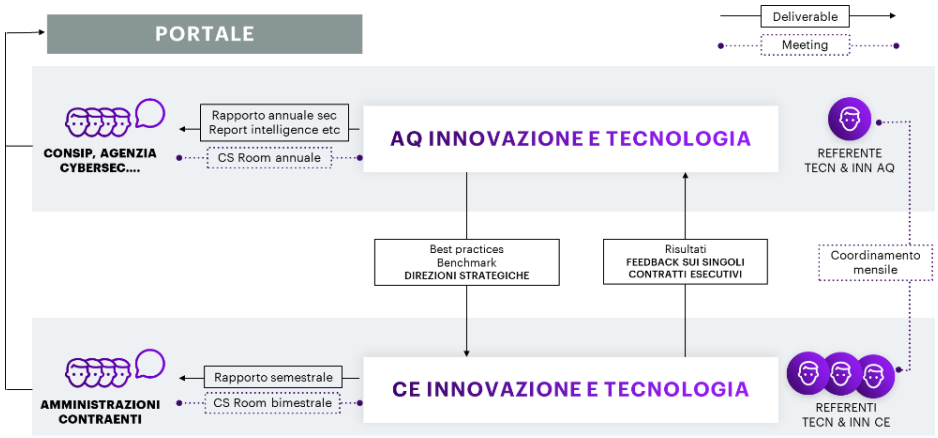
DEAS si propone per le attività di gestione continua delle vulnerabilità di sicurezza, Threat Intelligence & Vulnerability Data Feed e dei servizi di sicurezza specialistici. A tal fine, mette a disposizione competenze e tool sviluppati internamente per il rafforzamento della difesa perimetrale (**L1.S7** - Protezione degli end-point) e per lo sviluppo di soluzioni integrate di Cyber Threat Intelligence (**L1.S5** - Threat Intelligence & Vulnerability Data Feed). Essa dà valore aggiunto ai servizi oggetto della fornitura attraverso i seguenti asset innovativi:

- **DFC - Data Fusion Center (L1.S1, L1.S4)**, una piattaforma di Threat Awareness, disponibile in modalità as-a-service o stand-alone, che si configura come piattaforma di cybersecurity integrata con moduli IA/ML. Essa apporta alle tecnologie di Unified Threat Management (UTM) esistenti sul mercato la funzionalità innovativa di Situational Awareness, data dalla somma di più moduli integrati (Network Security Monitoring, Log Management Correlation, User Awareness, Network Awareness). DFC supporta le attività di Data Center Operations e Managed Security Services predisposte dal SOC per PA centrale, locale, e Grandi Aziende. Attraverso una gestione nativa degli incidenti (secondo le modalità CSIRT), DFC permette di gestire tutte le fasi operative del servizio SOC, agevolato da moduli di IA cognitiva e da molteplici e innovativi sistemi di visualizzazione grafica. In tal senso, le competenze di DEAS comprendono, nel complesso, un patrimonio operativo capace di garantire assistenza alle attività di cybersecurity del RTI (L1.S4 - Gestione continua delle vulnerabilità di sicurezza).
- **LVS - Laboratorio per la Valutazione della Sicurezza (L1.S15)**, struttura laboratoriale omologata OCSI (Organismo di Certificazione Sicurezza Informatica), per la ricerca e l'addestramento nelle pratiche aziendali collegate al disegno dei processi e delle operazioni di tool e soluzioni ICT. A supporto di un'innovazione rispondente al paradigma della security-by-design, il LVS è in grado di verificare gli obiettivi di sicurezza, la descrizione dell'ambiente in cui un oggetto di valutazione (ODV) è utilizzato, le minacce alle quali è soggetto, i requisiti funzionali e di fiducia, nonché la specifica delle funzioni di sicurezza.
- **Poligono cibernetico (L1.S9)**, infrastruttura hw/sw funzionale alla riproduzione di un ambiente operativo di simulazione di attacchi informatici e orchestrazione della risposta attraverso un training di gruppo basato su livelli diversi di automazione del Cyber Risk Management. Il Poligono abilita soluzioni di knowledge-transfer orizzontale e verticale capaci di integrare moduli didattici tradizionali con esperimenti coinvolgenti e una user-experience innovativa per la formazione di personale tecnico e non. Il Poligono supporta lo sviluppo di attività di apprendimento, in modo proattivo e interattivo, simulando ambienti reali, rendendo possibili attività di addestramento non sarebbero realizzabili su sistemi in produzione.
- **RaPToR, (L1.S7)**, la soluzione di endpoint protection, inclusa all'interno del "SPC Cloud L2 per i Servizi di Identità Digitale e Sicurezza Applicativa" che abilita misure avanzate anti-ransomware di Relevation, Response, Remediation secondo la logica R3 per endpoint (PC, dispositivi) e computer embedded (es. IoT).

Il **CFC Accenture** di Napoli rappresenta la struttura di riferimento per le attività di **tecnologia e innovazione.** Oltre a garantire una costante attività di **monitoraggio delle tecnologie emergenti**, esso è il principale attore nel garantire che le soluzioni proposte apportino nativamente valore aggiunto in termini di innovazione ai servizi oggetto della fornitura. In particolare, Accenture **propone i seguenti asset ed acceleratori** quali parte integrante del modello di erogazione dei servizi:

- **Next Generation Security Operation** (L1.S1, L1.S7, L1.S6, L1.S10) - il servizio di Next Generation Security operation descritto al §6 estende il concetto di **Security Orchestration and Response (SOAR)** a tutto il ciclo di vita della gestione degli incidenti, riducendo il tempo di rilevazione e risoluzione e garantendo consistenza in termini di risposta e scalabilità. Con l'evoluzione dell'Internet of Things è importante che gli strumenti e i processi del SOC possano adattarsi ad integrare anche i nuovi **device OT/IoT/IIoT all'interno degli scenari** di analisi. Accenture grazie alle recenti acquisizioni e agli investimenti in ambito OT ha realizzato piattaforme e acceleratori basati su algoritmi innovativi in grado di assicurare la stessa qualità del servizio nel caso di dispositivi connessi, per loro natura peculiari sia dal punto di vista tecnologico sia dei requisiti di sicurezza. Il servizio fa leva sulle principali tecnologie di mercato (es. Nozomi) in ambito OT per le quali Accenture vanta un robusto network di relazioni con i principali vendor e personale altamente qualificato.
- **Autonomous Identity** (L1.S10) - un approccio innovativo all'Identity & Access management, sviluppato da Accenture, che utilizza ML e AI per analizzare le caratteristiche degli accessi autorizzati e portare automazione nella autorizzazione, gestione e bonifica delle identità. Inoltre, esso consente di ridurre al minimo l'overprovisioning di risorse, riducendo automaticamente il rischio di accessi non autorizzati a risorse specifiche, e di realizzare il provisioning automatizzato e proattivo delle utenze (es. per nuovi utenti), riducendo il volume delle richieste di supporto e velocizzando significativamente il processo di on-boarding. La soluzione consente di incrementare la produttività con una diminuzione dei costi fino al 40% e di ridurre il rischio di accessi anomali fino al 30% con un alto grado di confidenza.
- **MultiCloud Security** (L1.S1, L1.S4, L1.S6) - Accenture ha implementato dal 2020 il programma "**Journey to Cloud**" ($3B di investimento globale) in cui la sicurezza è elemento fondante per mitigare i rischi associati alla migrazione e alle nuove minacce in cloud. Per il controllo delle misconfigurazioni in ambiente cloud, che ad oggi rappresentano la principale causa di attacco, Accenture ha sviluppato acceleratori in grado di apportare una riduzione massima dell'effort di remediation dell'85% ed una riduzione del 75% del 'time-to-compliance'. Attraverso l'uso di tecniche di hyperautomation, essi consentono l'esecuzione di controlli complessi nell'ordine di pochi minuti e abilitano controlli proattivi per bloccare l'occorrenza di potenziali incidenti in ambienti cloud pubblici, ibridi e privati indipendentemente dalla tecnologia.

17.3 Modalità organizzative del coinvolgimento



I soggetti del RTI deputati all'innovazione afferiscono all'ambito di competenza **Tecnologia e Innovazione** degli **Smart Hub**.

Secondo un modello operativo, coordinato dal **Referente Tecnologia e Innovazione,** essi operano sia a livello di AQ sia di CE garantendo un continuo allineamento in ottica di collaborazione, condivisione di conoscenza e *cross-fertilization* tra le PA a beneficio della sicurezza dell'intero sistema paese. A livello di AQ, il **Referente Tecnologia e Innovazione** coordina le attività della struttura ed è il punto di riferimento diretto per CONSIP e per tutti gli attori chiave coinvolti nelle decisioni strategiche per il paese. Per ogni CE, un **Referente Tecnologia e Innovazione** è a sua volta responsabile del coordinamento delle attività del singolo contratto e lavora in costante coordinamento con il **Referente Tecnologia e Innovazione** di AQ, oltre che con le PA contraenti. I referenti delle strutture di Tecnologia e Innovazione a livello di AQ e CE si coordinano mensilmente per un avanzamento sullo stato complessivo delle attività e per favorire lo scambio di informazioni, idee e risultati che alimentano il processo di innovazione. Per garantire il governo strategico e continuo delle iniziative di innovazione e il loro costante monitoraggio, è istituito un **presidio di steering**, denominato **Cybersecurity Room**, sia a livello AQ sia CE.

La **Cybersecurity Room di AQ** si configura come presidio di advisory strategica dedicato a Consip oltre che come presidio tematico-tecnologico costantemente attivo e osservatorio per la sicurezza nazionale a beneficio del sistema paese. Essa ha il compito di a) coordinare le Cybersecurity Room istituite a livello di CE, b) elaborare **rapporti annuali** sullo stato della sicurezza nella PA anche attingendo alle strutture di Cyber Threat Intelligence del RTI , c) elaborare le direzioni strategiche e di innovazione da diramare alle strutture dei singoli CE e d) recepire feedback dalle Cybersecurity room dei singoli CE al fine di elaborare best practices e lessons learned (es. materiale per la formazione in ambito cyber su nuove minacce). La Cybersecurity Room di AQ si riunisce con cadenza semestrale o su specifica richiesta del cliente e vede la partecipazione di almeno un esponente di ogni azienda del RTI, del Referente Tecnologia e Innovazione e di Referenti preposti all'innovazione identificati da Consip.

La **Cybersecurity Room di CE** si configura come presidio di supporto operativo e tecnologico per le amministrazioni contraenti oltre che come osservatorio sulle nuove tecnologie. Essa ha il compito di a) recepire le istanze strategiche e gli obiettivi specifici stabiliti a livello di AQ, b) raccogliere e recepire feedback e criticità riscontrate durante l'operatività dei servizi in ambito, c) elaborare **rapporti semestrali** sulla sicurezza dei sistemi interni dell'Amministrazione Contraente che riepiloga le attività effettuate e lo stato dei servizi e d) avanzare proposte per migliorare la qualità dei servizi, suggerendo ad esempio l'introduzione di nuove tecnologie e/o di gradi crescenti di automazione. Essa si riunisce con cadenza bimestrale o all'occorrenza su specifica richiesta del cliente e vede la partecipazione di almeno un esponente di ogni azienda del RTI, del referente Tecnologia e Innovazione e di referenti preposti all'innovazione identificati dalle amministrazioni contraenti. Per ogni CE, il RTI s'impegna annualmente a fornire una POC su tecnologie innovative in collaborazione con partner tecnologici, la attivazione di una o più tesi di laurea e/o tirocini con uno o più atenei e l'organizzazione di una o più sessioni di co-creazione con le amministrazioni contraenti.

Al presidio di steering costituito dalle **Cybersecurity Room**, gli specialisti di alto profilo che fanno parte delle strutture di Tecnologia e Innovazione offrono un presidio operativo a supporto della esecuzione delle attività ordinarie. Essi interagiscono con il cliente sia in modalità **proattiva**, facendosi promotori di proposte innovative quali progetti finalizzati alla realizzazione di POC, prototipi per l'attivazione di nuove soluzioni o evoluzione di quelle in uso anche attraverso seminari e workshop, sia **reattiva**, rispondendo a specifiche richieste che richiedono disegno, progettazione e/o implementazione di soluzioni innovative sia in termini tecnologici (facendo leva sui partner di ecosistema) sia di modelli e metodologie (facendo leva su partner accademici e centri di competenza), anche attraverso sessioni di co-creazione per fornire risposte tempestive aderenti ai requisiti. In caso di modalità reattiva, il RTI si impegna ad attivare la struttura entro **due settimane** dalla ricezione della richiesta della PA, sia a livello di AQ sia di CE.I **rapporti prodotti e gli output delle Cybersecurity Room**, sia di AQ sia di CE, contribuiranno a popolare il Portale di Fornitura (cfr. §16), riportando ad esempio i trend sullo stato della sicurezza nella PA o lo stato della security o i trend di miglioramento della sicurezza osservati nel tempo per le singole Amministrazioni, nel rispetto della profilazione dei ruoli e preservando la confidenzialità dei dati condivisi.

18 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ - TIIS – Tempo di prima investigazione per incidenti di sicurezza

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico "Indicatori di qualità", il Raggruppamento s'impegna a garantire una riduzione dei valori di soglia previsti per l'indicatore TIIS secondo le indicazioni di seguito riportate:

Gravità Alta, TIIS <=2 ore solari e Gravità Media, TIIS <=4 ore solari.

19 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ - TCIS – Tempo di primo contenimento per incidenti di sicurezza

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico "Indicatori di qualità", il Raggruppamento s'impegna a garantire una riduzione dei valori di soglia previsti per l'indicatore TCIS secondo le indicazioni di seguito riportate:

Gravità Alta, TCIS <=6 ore solari e Gravità Media, TCIS <=10 ore solari.

20 ASSUNZIONE DELLE RISORSE PROFESSIONALI

Rispetto al complesso delle assunzioni necessarie per ogni contratto esecutivo finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, e fermo restando il rispetto del requisito necessario di cui al Capitolato tecnico generale al par. 7.1 il Raggruppamento si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, nella seguente misura: **>35%.**

ALLEGATO B – OFFERTA ECONOMICA DEL FORNITORE

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	ACCENTURE S.P.A. (mandataria) Società per Azioni
Partita IVA	13454210157
Codice Fiscale Impresa	13454210157
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	13454210157
Codice Ditta INAIL	5225761 CC 43
n. P.A.T.	MILANO CORSO DI PORTA NUOVA, 19 20121 IMPIEGATI 06354916/02 DIRIGENTI 06354915/57 ROMA PIAZZA CINQUE GIORNATE, 3 00192 IMPIEGATI 08309753/36 DIRIGENTI 08309752/80 TORINO CORSO G. FERRARIS, 1 10121 IMPIEGATI 07996552/95 DIRIGENTI 07996553/40 VERONA CORSO

	CAVOUR, 6 37121 IMPIEGATI 08113579/24 DIRIGENTI 08113580/41 NAPOLI VIA G.PORZIO 80100 IMPIEGATI 021931970
Matricola aziendale INPS	4946954414 – 03
CCNL applicato	METALMECCANICO
Settore	INDUSTRIA
Indirizzo sede legale	VIA PRIVATA NINO BONNET, 10 - MILANO (MI)
Telefono	0659566287
Fax	0659566619
PEC Registro Imprese	UFFICIO.GARE.ACCENTURE@LEGALMAIL.IT
Ragione Sociale	DEAS - DIFESA E ANALISI SISTEMI S.P.A. (mandante) Società per Azioni
Partita IVA	14961281004
Codice Fiscale Impresa	14961281004
Provincia sede registro imprese	RM
Numero iscrizione registro imprese	14961281004
Codice Ditta INAIL	20351528/46
n. P.A.T.	P.A.T. : 95501111/11
Matricola aziendale INPS	7070525941
CCNL applicato	METALMECCANICO
Settore	INDUSTRIA
Indirizzo sede legale	VIA DELLA COLONNA ANTONINA, 46 - ROMA (RM)
Telefono	3495669316
Fax	3495669316
PEC Registro Imprese	DEAS-SPA@LEGALMAIL.IT
Ragione Sociale	FASTWEB (mandante) Società per Azioni
Partita IVA	12878470157
Codice Fiscale Impresa	12878470157
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	12878470157
Codice Ditta INAIL	5754889
n. P.A.T.	10953364-10954139-91683426
Matricola aziendale INPS	4959627727
CCNL applicato	TELECOMUNICAZIONI
Settore	TLC
Indirizzo sede legale	PIAZZA ADRIANO OLIVETTI 1 - MILANO (MI)
Telefono	0245451
Fax	0245453022
PEC Registro Imprese	FASTWEB@PEC.FASTWEB.IT

Ragione Sociale	FINCANTIERI NEXTECH S.P.A. (mandante) Società per Azioni
Partita IVA	00890740111
Codice Fiscale Impresa	00890740111
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	00890740111
Codice Ditta INAIL	3684993
n. P.A.T.	7277569/52;7275516/92;92803431/26
Matricola aziendale INPS	3901835366
CCNL applicato	INDUSTRIA METALMECCANICA
Settore	INDUSTRIA
Indirizzo sede legale	VIA CARLO OTTAVIO CORNAGGIA, 10 MILANO (MI) - MILANO (MI)
Telefono	0697614061
Fax	0187981251
PEC Registro Imprese	FINCANTIERINXT@LEGALMAIL.IT
Offerta sottoscritta da	**CARRINO FRANCESCO, RANZATO STEFANIA, LODA' RICCARDO, TURCONI FRANCO, VIERO ANDREA**

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 (€)	87,100
2 - L1.S1 - Security Operation Center (SOC) - Fascia 2 - Fino a 600 Eps - Prezzo unitario offerto (€)	165,2
3 - L1.S1 - Security Operation Center (SOC) - Fascia 3 - Fino a 1.200 Eps - Prezzo unitario offerto (€)	239,4
4 - L1.S1 - Security Operation Center (SOC) - Fascia 4 - Fino a 6.000 Eps - Prezzo unitario offerto (€)	218,4
5 - L1.S1 - Security Operation Center (SOC) - Fascia 5 - > 6.000 Eps - Prezzo unitario offerto (€)	225
6 - L1.S2 - Next Generation FW - Fascia 1 - Fino a 250 Mbps - Prezzo unitario offerto (€)	308,55
7 - L1.S2 - Next Generation FW - Fascia 2 - Fino a 2 Gbps - Prezzo unitario offerto (€)	1129,856
8 - L1.S2 - Next Generation FW - Fascia 3 - Fino a 4 Gbps - Prezzo unitario offerto (€)	6475,84
9 - L1.S2 - Next Generation FW - Fascia 4 - Fino a 7 Gbps - Prezzo unitario offerto (€)	10705,5
10 - L1.S2 - Next Generation FW - Fascia 5 - Fino a 15 Gbps - Prezzo unitario offerto (€)	46035
11 - L1.S2 - Next Generation FW - Fascia 6 - > 15 Gbps - Prezzo unitario offerto (€)	57330
12 - L1.S3 - Web Application FW - Fascia 1 - Fino a 500 Mbps - Prezzo unitario offerto (€)	2800
13 - - Fascia 2 - Fino a 5 Gbps - Prezzo unitario offerto (€)	51500
14 - - Fascia 3 - > 5 Gbps - Prezzo unitario offerto (€)	75600
15 - L1.S4 -Gestione continua delle	23

vulnerabilità di sicurezza - Fascia 1 - Fino a 50 IP - Prezzo unitario offerto (€)	
16 - - Fascia 2 - Fino a 200 IP - Prezzo unitario offerto (€)	13,8
17 - - Fascia 3 - > 200 IP - Prezzo unitario offerto (€)	13,8
18 - L1.S5 -Threat Intelligence & Vulnerability Data Feed - Fascia 1 - fino a 10 datafeed - Prezzo unitario offerto (€)	280
19 - L1.S5 -Threat Intelligence & Vulnerability Data Feed - Fascia 2 - fino a 50 datafeed - Prezzo unitario offerto (€)	240
20 - L1.S5 -Threat Intelligence & Vulnerability Data Feed - Fascia 3 - > 50 datafeed - Prezzo unitario offerto (€)	200
21 - L1.S6 - Protezione navigazione Internet e Posta elettronica - Fascia 1 - Fino a 1.000 utenti - Prezzo unitario offerto (€)	6,647
22 - - Fascia 2 - Fino a 5.000 utenti - Prezzo unitario offerto (€)	4,037
23 - - Fascia 3 - Fino a 10.000 utenti - Prezzo unitario offerto (€)	3,314
24 - - Fascia 4 - Fino a 20.000 utenti - Prezzo unitario offerto (€)	2,561
25 - - Fascia 5 - > 20.000 utenti - Prezzo unitario offerto (€)	1,783
26 - L1.S7 -Protezione End point - Fascia 1 - Fino a 500 nodi - Prezzo unitario offerto (€)	18,19
27 - - Fascia 2 - Fino a 1.000 nodi - Prezzo unitario offerto (€)	16,538
28 - - Fascia 3 - Fino a 5.000 nodi - Prezzo unitario offerto (€)	12,863
29 - - Fascia 4 - > 5.000 nodi - Prezzo unitario offerto (€)	11,025
30 - L1.S8 -Certificati SSL - SSL OV - Prezzo unitario offerto (€)	32,717
31 - L1.S8 -Certificati SSL - SSL OV Wildcard - Prezzo unitario offerto (€)	74,102
32 - L1.S8 -Certificati SSL - SSL EV - Prezzo unitario offerto (€)	74,723
33 - L1.S8 -Certificati SSL - SSL DV - Prezzo unitario offerto (€)	15,224

34 - L1.S8 -Certificati SSL - SSL Code signing - Prezzo unitario offerto (€)	68,976
35 - L1.S8 -Certificati SSL - SSL Client Auth - Prezzo unitario offerto (€)	9,633
36 - L1.S9 -Formazione e security awareness - gg/p Team ottimale - Prezzo unitario offerto (€)	247,52
37 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 1 - Fino a 10.000 utenti - Prezzo unitario offerto (€)	0,276
38 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 2 - Fino a 100.000 utenti - Prezzo unitario offerto (€)	0,221
39 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 3 - Fino a 500.000 utenti - Prezzo unitario offerto (€)	0,178
40 - L1.S10 -Gestione dell'identità e l'accesso utente - Fascia 4 - > 500.000 utenti - Prezzo unitario offerto (€)	0,134
41 - L1.S11 - Firma digitale remota - Fascia 1 - > 50 e fino a 200 utenti - Prezzo unitario offerto (€)	6,143
42 - L1.S11 - Firma digitale remota - Fascia 2 - > 200 e fino a 500 utenti - Prezzo unitario offerto (€)	5,648
43 - L1.S11 - Firma digitale remota - Fascia 3 - > 500 e fino a 1.000 utenti - Prezzo unitario offerto (€)	4,973
44 - L1.S11 - Firma digitale remota - Fascia 4 - > 1.000 utenti - Prezzo unitario offerto (€)	3,89
45 - L1.S11 - Firma digitale remota - Garantita - N. 1 firma - Prezzo unitario offerto (€)	3890,25
46 - L1.S11 - Firma digitale remota - Garantita - N. 5 firme aggiuntive - Prezzo unitario offerto (€)	8947,575
47 - L1.S12 -Sigillo elettronico - Garantita - N. 1 firma - Prezzo unitario offerto (€)	3890,25
48 - L1.S12 -Sigillo elettronico - Garantita - N. 5 firme aggiuntive - Prezzo unitario offerto (€)	8947,575

49 - L1.S13 - Timbro elettronico - Fascia 1 - Fino a 1.000 timbrature - Prezzo unitario offerto (€)	0,608
50 - L1.S13 - Timbro elettronico - Fascia 2 - Fino a 10.000 timbrature - Prezzo unitario offerto (€)	0,562
51 - L1.S13 - Timbro elettronico - Fascia 3 - Fino a 100.000 timbrature - Prezzo unitario offerto (€)	0,468
52 - L1.S13 - Timbro elettronico - Fascia 4 - Fino a 1.000.000 timbrature - Prezzo unitario offerto (€)	0,398
53 - L1.S13 - Timbro elettronico - Fascia 5 - Fino a 10.000.000 timbrature - Prezzo unitario offerto (€)	0,005
54 - L1.S13 - Timbro elettronico - Fascia 6 - > 10.000.000 timbrature - Prezzo unitario offerto (€)	0,006
55 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 1 - Fino a 1.000 Marcature - Prezzo unitario offerto (€)	0,056
56 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 2 - Fino a 10.000 Marcature - Prezzo unitario offerto (€)	0,043
57 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 3 - Fino a 100.000 Marcature - Prezzo unitario offerto (€)	0,023
58 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 4 - Fino a 1.000.000 Marcature - Prezzo unitario offerto (€)	0,012
59 - L1.S14 - Validazione temporale elettronica qualificata - Fascia 5 - Fino a 10.000.000 Marcature - Prezzo unitario offerto (€)	0,004
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 (€)	3217,5

62 - L1.S14 - Validazione temporale elettronica qualificata - Garantita - N. 1 marcatura aggiuntiva - Prezzo unitario offerto (€)	3217,5
63 - L1.S15 -Servizi specialistici - gg/p Team ottimale - Prezzo unitario offerto (€)	244
Ribasso medio ponderato - Calcolato dal Sistema	0,51000

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

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

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

ALLEGATO C – CORRISPETTIVI E TARIFFE PAL

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 Locali (PAL)

Servizio	Voce economica	Id voce	Prezzo offerto
L1.S1 - Security Operation Center (SOC)	Fascia 1 - Fino a 300 Eps	1	€ 87,10
	Fascia 2 - Fino a 600 Eps	2	€ 165,20
	Fascia 3 - Fino a 1.200 Eps	3	€ 239,40
	Fascia 4 - Fino a 6.000 Eps	4	€ 218,40
	Fascia 5 - > 6.000 Eps	5	€ 225,00
L1.S2 - Next Generation FW	Fascia 1 - Fino a 250 Mbps	6	€ 308,55
	Fascia 2 - Fino a 2 Gbps	7	€ 1.129,856
	Fascia 3 - Fino a 4 Gbps	8	€ 6.475,84
	Fascia 4 - Fino a 7 Gbps	9	€ 10.705,50
	Fascia 5 - Fino a 15 Gbps	10	€ 46.035,00
	Fascia 6 - > 15 Gbps	11	€ 57.330,00
L1.S3 - Web Application FW	Fascia 1 - Fino a 500 Mbps	12	€ 2.800,00
	Fascia 2 - Fino a 5 Gbps	13	€ 51.500,00
	Fascia 3 - > 5 Gbps	14	€ 75.600,00
L1.S4 - Gestione continua delle vulnerabilità di sicurezza	Fascia 1 - Fino a 50 IP	15	€ 23,00
	Fascia 2 - Fino a 200 IP	16	€ 13,80
	Fascia 3 - > 200 IP	17	€ 13,80
L1.S5 - Threat Intelligence & Vulnerability Data Feed	Fascia 1 - fino a 10 datafeed	18	€ 280,00
	Fascia 2 - fino a 50 datafeed	19	€ 240,00
	Fascia 3 - > 50 datafeed	20	€ 200,00
	Fascia 1 - Fino a 1.000 utenti	21	€ 6,647

L1.S6 - Protezione navigazione Internet e Posta elettronica	Fascia 2 - Fino a 5.000 utenti	22	€ 4,037
	Fascia 3 - Fino a 10.000 utenti	23	€ 3,314
	Fascia 4 - Fino a 20.000 utenti	24	€ 2,561
	Fascia 5 - > 20.000 utenti	25	€ 1,783
L1.S7 - Protezione End point	Fascia 1 - Fino a 500 nodi	26	€ 18,19
	Fascia 2 - Fino a 1.000 nodi	27	€ 16,538
	Fascia 3 - Fino a 5.000 nodi	28	€ 12,863
	Fascia 4 - > 5.000 nodi	29	€ 11,025
L1.S8 - Certificati SSL	SSL OV	30	€ 32,717
	SSL OV Wildcard	31	€ 74,102
	SSL EV	32	€ 74,723
	SSL DV	33	€ 15,224
	SSL Code signing	34	€ 68,976
	SSL Client Auth	35	€ 9,633
L1.S9 - Formazione e security awareness	gg/p Team ottimale	36	€ 247,52
L1.S10 - Gestione dell'identità e l'accesso utente	Fascia 1 - Fino a 10.000 utenti	37	€ 0,276
	Fascia 2 - Fino a 100.000 utenti	38	€ 0,221
	Fascia 3 - Fino a 500.000 utenti	39	€ 0,178
	Fascia 4 - > 500.000 utenti	40	€ 0,134
L1.S11 - Firma digitale remota	Fascia 1 - > 50 e fino a 200 utenti	41	€ 6,143
	Fascia 2 - > 200 e fino a 500 utenti	42	€ 5,648
	Fascia 3 - > 500 e fino a 1.000 utenti	43	€ 4,973
	Fascia 4 - > 1.000 utenti	44	€ 3,89
	Garantita - N. 1 firma	45	€ 3.890,25
	Garantita - N. 5 firme aggiuntive	46	€ 8.947,575
L1.S12 - Sigillo elettronico	Garantita - N. 1 firma	47	€ 3.890,25
	Garantita - N. 5 firme aggiuntive	48	€ 8.947,575
	Fascia 1 - Fino a 1.000 timbrature	49	€ 0,608

L1.S13 - Timbro elettronico	Fascia 2 - Fino a 10.000 timbrature	50	€ 0,562
	Fascia 3 - Fino a 100.000 timbrature	51	€ 0,468
	Fascia 4 - Fino a 1.000.000 timbrature	52	€ 0,398
	Fascia 5 - Fino a 10.000.000 timbrature	53	€ 0,005
	Fascia 6 - > 10.000.000 timbrature	54	€ 0,006
L1.S14 - Validazione temporale elettronica qualificata	Fascia 1 - Fino a 1.000 Marcature	55	€ 0,056
	Fascia 2 - Fino a 10.000 Marcature	56	€ 0,043
	Fascia 3 - Fino a 100.000 Marcature	57	€ 0,023
	Fascia 4 - Fino a 1.000.000 Marcature	58	€ 0,012
	Fascia 5 - Fino a 10.000.000 Marcature	59	€ 0,004
	Fascia 6 - > 10.000.000 Marcature	60	€ 0,004
	Garantita - N. 1 marcatura	61	€ 3.217,50
	Garantita - N. 1 marcatura aggiuntiva	62	€ 3.217,50
L1.S15 - Servizi specialistici	gg/p Team ottimale	63	€ 244,00

ALLEGATO D – PATTO D'INTEGRITA'

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

PATTO DI INTEGRITA' RELATIVO ALLA PROCEDURA DI GARA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296

LOTTO 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.

ALLEGATO E – NOMINA E RESPONSABILE DEL TRATTAMENTO DATI

CONTRATTO ESECUTIVO NELL'AMBITO DELL'ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296

NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI

1. Con la sottoscrizione della presente da parte dell'Amministrazione _____ il Fornitore _____è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche *"Regolamento UE"*), per tutta la durata del contratto attuativo (nel seguito anche "contratto") relativo alla Convenzione _____. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto dell'Amministrazione (Titolare del Trattamento), **le sole operazioni di trattamento necessarie per fornire il servizio oggetto del contratto attuativo e della Convenzione**, nei limiti delle finalità ivi specificate, nel rispetto del Regolamento UE 2016/679, del D.Lgs. 196/2003 e s.m.i e del D. Lgs. n. 101/2018 (nel seguito anche *"Normativa in tema di trattamento dei dati personali"*), e delle istruzioni nel seguito fornite.
2. Il Fornitore/Responsabile si impegna a presentare su richiesta dell'Amministrazione garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.
3. Le finalità del trattamento sono: ***<Valorizzare in ragione dell'oggetto del contratto _____>***
4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: ***<Valorizzare in ragione dell'oggetto del contratto*** i) dati comuni (es. dati anagrafici e di contatto ecc.); ii) dati sensibili; iii) dati giudiziari***>***.
5. Le categorie di interessati sono: ***<Valorizzare in ragione dell'oggetto del contratto*** es. dipendenti e collaboratori, utenti dei servizi, ecc.>.
6. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:
   a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;
   b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
   c) trattare i dati personali conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;
   d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
      - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
      - ricevano la formazione necessaria in materia di protezione dei dati personali;
      - trattino i dati personali osservando le istruzioni impartite dal Titolare al Responsabile;
   e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (*privacy by design*), nonché adottare misure tecniche ed organizzative adeguate

per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (*privacy by default*);

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

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

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

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

7. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Fornitore si impegna a fornire all'Amministrazione un piano di misure di sicurezza rimesse all'approvazione della stessa, che saranno concordate al fine di mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso ***<personalizzare in ragione dell'oggetto del contratto>***:
    - la pseudonimizzazione e la cifratura dei dati personali;
    - la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
    - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
    - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

    La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.
8. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

    A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre <***o diverso termine indicato dalla PA*** > giorni lavorativi,; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque,

inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà le penali previste nella Convenzione e diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

9. ***1) (Autorizzazione generale)*** Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente _____ ***(la PA deve specificare la periodicità)***, il Titolare del trattamento delle nomine e delle sostituzioni dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi dei sub-Responsabili nominati e i dati del contratto di esternalizzazione.
   <Oppure> 2) (Autorizzazione specifica) Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento.
10. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.
    Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento o risulti che il sub responsabile agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà al Fornitore/Responsabile Inziale del trattamento le penali previste nella Convenzione e diffiderà lo stesso a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il contratto attuativo con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ***<selezionare una tra le due opzioni:***
    1) ad informare tempestivamente il Titolare del trattamento, fornendo adeguato riscontro agli interessati, in nome e per conto del Titolare del trattamento, nei termini previsti dalla Regolamento UE; ***oppure>***
    2) ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.
12. Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento,

ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile <***da valorizzare in alternativa***: sub-Responsabile> del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

13. Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto.
14. Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.
15. Al termine della prestazione dei servizi oggetto del contratto, il Responsabile, su richiesta del Titolare, si impegna a: *i)* restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; *ii)* distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
16. Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.
17. Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali, trattati in esecuzione del contratto attuativo, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.
18. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.
19. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.
20. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.
21. Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Protezione dei Dati Personali e/o della disciplina sulla protezione dei dati personali contenuta nella Convezione (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o sub-fornitori.

ALLEGATO F – SCHEMA CONTRATTO ESECUTIVO LOTTO 1

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

21. FORO COMPETENTE

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

22. TRATTAMENTO DEI DATI PERSONALI

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

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

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

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

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

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

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

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

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

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

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

- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;

- ricevano la formazione necessaria in materia di protezione dei dati personali;

- trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

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

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

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

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

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

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

- la pseudonimizzazione e la cifratura dei dati personali;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Letto, approvato e sottoscritto
Roma, lì _____

_____ (per l'Amministrazione)

_____ (per il Fornitore)

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

Letto, approvato e sottoscritto

Roma, lì

_____

(per il Fornitore)

ALLEGATO G – DISPOSIZIONI PER LA GOVERNANCE

Piano Strategico ICT
Governance delle Gare Strategiche

Disposizioni per la governance

Categorizzazione, Indicatori di digitalizzazione

Sommario

Indice delle tabelle

1. PREMESSA

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

2. DEFINIZIONI

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

[1] Comprensivo delle sue evoluzioni.

3. PERIMETRO

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

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

[2] ID 2296 è bandita ai sensi dell'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, che ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311". Per la merceologia trattata è considerata al pari delle gare strategiche.

[3] Tutte le gare che saranno definite.

4. MONITORAGGIO DELL'APPLICAZIONE DEL PIANO TRIENNALE

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

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

4.1 ELEMENTI CARATTERIZZANTI

Il monitoraggio riguarda:

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

[4] Come definita nel par. 2 - Definizioni

5. PRINCIPI GUIDA

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

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

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

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

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

6.1 CATEGORIZZAZIONE DI I LIVELLO DEI CONTRATTI ESECUTIVI

La seguente tabella sintetizza la Categorizzazione e gli obiettivi associati:

Ambito I livello (layer)	Obiettivi Piano Triennale
Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
Dati	• Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese • Aumentare la qualità dei dati e dei metadati • Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
Piattaforme	• Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa • Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA • Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini

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

Ambito I livello (layer)	Obiettivi Piano Triennale
Infrastrutture	• Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio) • Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud) • Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
Interoperabilità	• Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API • Adottare API conformi al Modello di Interoperabilità
Sicurezza Informatica	• Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA • Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

Tabella 1 - Obiettivi del Piano Triennale

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

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

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

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

6.1.2 CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE IN PREDISPOSIZIONE

Per le seguenti iniziative:

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

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

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

6.2 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI

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

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

Ambito I (layer)	Ambito II livello
Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
Dati	• Agricoltura, pesca, silvicoltura e prodotti alimentari • Economia e finanze • Istruzione, cultura e sport • Energia • Ambiente • Governo e Settore pubblico • Salute • Tematiche internazionali • Giustizia e sicurezza pubblica • Regioni e città • Popolazione e società • Scienza e tecnologia • Trasporti
Piattaforme	• Sanità digitale (FSE e CUP) • Identità Digitale; • Pagamenti digitali; • App IO; • ANPR; • NoiPA; • INAD; • Musei; • Siope+
Infrastrutture	• Data Center e Cloud • Connettività
Interoperabilità	• Agricoltura, pesca, silvicoltura e prodotti alimentari • Economia e finanze • Istruzione, cultura e sport • Energia • Ambiente

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

Tabella 3 - Categorizzazione generale di II livello

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

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

Gara strategica	Ambito I livello applicabile	Ambito II livello applicabile
Digital Transformation	Tutti	Tutti
Public Cloud IaaS e PaaS	• Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
	• Infrastrutture	• Agricoltura, pesca, silvicoltura e prodotti alimentari • Economia e finanze • Istruzione, cultura e sport • Energia • Ambiente • Governo e Settore pubblico • Salute • Tematiche internazionali • Giustizia e sicurezza pubblica • Regioni e città • Popolazione e società • Scienza e tecnologia • Trasporti
	• Dati	• Data Center e Cloud • Connettività
Servizi applicativi in ottica cloud	• Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
	• Piattaforme	• Sanità digitale (FSE e CUP) • Identità Digitale • Pagamenti digitali • App IO • ANPR • NoiPA • INAD • Musei

		• Siope+
	• Interoperabilità	• Agricoltura, pesca, silvicoltura e prodotti alimentari • Economia e finanze • Istruzione, cultura e sport • Energia • Ambiente • Governo e Settore pubblico • Salute • Tematiche internazionali • Giustizia e sicurezza pubblica • Regioni e città • Popolazione e società • Scienza e tecnologia • Trasporti
Data Management	• Dati	• Agricoltura, pesca, silvicoltura e prodotti alimentari • Economia e finanze • Istruzione, cultura e sport • Energia • Ambiente • Governo e Settore pubblico • Salute • Tematiche internazionali • Giustizia e sicurezza pubblica • Regioni e città • Popolazione e società • Scienza e tecnologia • Trasporti

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

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

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

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

6.3 CONTRATTI AD ALTA RILEVANZA

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

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

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

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

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

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

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

7. MONITORAGGIO DEI RISULTATI DI DIGITALIZZAZIONE

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

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

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

7.1 INDICATORI GENERALI DI DIGITALIZZAZIONE

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

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

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

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

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

Tabella 6 - Indicatori Generali di digitalizzazione

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

Si precisa che per tutti gli indicatori generali di digitalizzazione:

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

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

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

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

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

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

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

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

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

Tabella 7 - Indicatori Generali quantitativi

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

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

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

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

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

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

Tabella 8 - Indicatori Generali qualitativi

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

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

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

Tabella 9 - Indicatori generali di riuso

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

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

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

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

7.2 INDICATORI SPECIFICI DI DIGITALIZZAZIONE

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

7.2.1 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA DIGITAL TRANSFORMATION

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

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

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

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

Tabella 10 - Indicatori Specifici Digital Transformation

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

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

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

Tabella 11 - Indicatori Specifici Public cloud IaaS e PaaS

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

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

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

Tabella 12 - Indicatori Specifici Servizi Applicativi in ottica cloud

7.2.4 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA DATA MANAGEMENT

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

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

Tabella 13 - Indicatori specifici Data Management

7.2.5 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LE GARE DI SICUREZZA

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

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

Tabella 14 - Indicatore di progresso

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

7.2.6 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LE GARE STRATEGICHE IN PREDISPOSIZIONE

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

7.3 INDICATORI II LIVELLO PER CONTRATTI AD ALTA RILEVANZA

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

Non previsti.

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

Non previsti.

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

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

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

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

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

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

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

Tabella 16 - Indicatori specifici II Data Management

- Fine del documento -

ALLEGATO H – REGOLAMENTO DEGLI ORGANISMI DI COORDINAMENTO E CONTROLLO

consip

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

AGID Agenzia per l'Italia Digitale

Piano Strategico ICT
Governance delle Gare Strategiche

Organismi di coordinamento e controllo

Regolamento

Sommario

1. PREMESSA

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

2. DEFINIZIONI

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

[1] Comprensivo delle sue evoluzioni.
[2] ID 2296 è bandita ai sensi dell'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, che ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311". Per la merceologia trattata è considerata al pari delle gare strategiche.
[3] Tutte le gare che saranno definite.

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

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

3.1 PRINCIPI GENERALI

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

3.2 COMPITI E RESPONSABILITÀ DEL COMITATO TECNICO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[4] Secondo i criteri definiti per ciascuna Gara Strategica

3.3 INDIVIDUAZIONE DEL PRESIDENTE - RIUNIONI DEL COMITATO TECNICO

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

3.4 ATTI DEL COMITATO TECNICO

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

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

4.1 PRINCIPI GENERALI

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

4.2 COMPITI E RESPONSABILITÀ DEL COMITATO STRATEGICO

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

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

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

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

4.3 RIUNIONI DEL COMITATO STRATEGICO

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

4.4 ATTI DEL COMITATO STRATEGICO

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

- fine del documento -