SISTEMA SANITARIO REGIONALE
ASL ROMA 1

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

N. 1465 **del** 29/11/2024

OGGETTO: Adesione all'accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i., avente ad oggetto l'affidamento di servizi di sicurezza da remoto, compliance e controllo per le Pubbliche Amministrazioni - ID 2296 - Lotto 1 (Cig Madre: 88846293CA), per un periodo di 48 mesi sino alla data del 31 Dicembre 2028 per un importo di € 7.607.726,94 Iva esclusa corrispondente ad € 9.281.426,87 Iva inclusa - Operatore economico RTI costituito ACCENTURE S.P.A.- FINCANTIERI NEXTECH S.P.A. FASTWEB S.P.A. - DEAS - DIFESA E ANALISI SISTEMI S.P.A). CIG B43A6ED93D.

STRUTTURA PROPONENTE: DIPARTIMENTO TECNICO PATRIMONIALE - UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE

Centro di Costo: BD07 L'Estensore:Dott.ssa SERENA SBRIGLIO Il presente Atto contiene dati sensibili

Il Dirigente e/o il Responsabile del procedimento, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attestano che l'atto è legittimo nella forma e nella sostanza.

Il Responsabile del Procedimento	UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE	DIPARTIMENTO TECNICO PATRIMONIALE
Dott. MASSIMILIANO COLTELLACCI	Dott. MASSIMILIANO COLTELLACCI	Ing. PAOLA BRAZZODURO
Firmatario: MASSIMILIANO COLTELLACCI Data: 26/11/2024 12:02:51 CET	Firmatario: MASSIMILIANO COLTELLACCI Data: 26/11/2024 12:03:36 CET	Firmatario: PAOLA BRAZZODURO Data: 26/11/2024 12:14:45 CET

Il funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta uno scostamento sfavorevole rispetto al budget economico assegnato come di seguito dettagliato per singolo conto:

Costo previsto	Eserciz.	CE/CP	Numero conto	Descrizione conto	Addetto al controllo	Scostamento
€2.596.103,07	2025	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	No
€2.321.046,75	2026	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	No
€2.321.046,75	2027	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	No
€2.043.230,31	2028	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	No

Il Funzionario addetto al controllo di budget

Dott. MASSIMILIANO COLTELLACCI

Firmatario: MASSIMILIANO COLTELLACCI
Data: 26/11/2024 12:05:45 CET

Il Controllo di gestione prende atto degli impegni indicati dal funzionario addetto al controllo del budget per gli esercizi successivi a quello attuale

Il sostituto GIORGIO BACCARI
Data: 27/11/2024 18:19:11 CET

Parere del Direttore Amministrativo Dr. Francesco Quagliariello

Favorevole

Firmatario: FRANCESCO QUAGLIARIELLO
Data: 27/11/2024 18:50:51 CET

(con motivazioni allegate al presente atto)
Non favorevole

Parere del Direttore Sanitario Dr. Gennaro D'Agostino

Favorevole

Firmatario: GENNARO D'AGOSTINO
Data: 28/11/2024 12:15:04 CET

(con motivazioni allegate al presente atto)
Non favorevole

Il presente provvedimento si compone di n.36 pagine di cui n. 29 pagine di allegati

Il Commissario Straordinario
Dr. Giuseppe Quintavalle

Firmatario: GIUSEPPE QUINTAVALLE
Data: 29/11/2024 08:23:22 CET

REGIONE LAZIO

IL DIRETTORE SOSTITUTO DELLA U.O.C. SISTEMI E TECNOLOGIE INFORMATICHE E DI COMUNICAZIONE

VISTA la deliberazione del Commissario Straordinario n. 1 del 1° gennaio 2016, con la quale si è provveduto a prendere atto dell'avvenuta istituzione dell'Azienda Sanitaria Locale Roma 1 a far data dal 1° gennaio 2016, come previsto dalla legge regionale n. 17 del 31.12.2015 e dal DCA n. 606 del 30.12.2015;

VISTO il Decreto del Presidente della Regione Lazio T00013 del 5 aprile 2023 con il quale è stato nominato Commissario Straordinario dell'Azienda Sanitaria Locale Roma 1, il dott. Giuseppe Quintavalle;

VISTO l'Atto di Autonomia Aziendale, approvato con deliberazione n. 1153 del 17/12/2019, recepito con DCA U00020 del 27/01/2020, pubblicato sul BURL del 30/01/2020 n. 9 con il quale, tra l'altro, è stato istituito il Dipartimento Tecnico Patrimoniale di cui fa parte la U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione;

RICHIAMATA la Deliberazione n. 179 del 27/02/2020, avente ad oggetto "Atto aziendale dell'ASL Roma 1, approvato con Deliberazione n. 1153 del 17/12/2019 – Presa d'atto dell'esito positivo del procedimento di verifica regionale – Attuazione del nuovo modello organizzativo" la quale prevede l'attivazione del sopra citato Dipartimento e delle UU.OO.CC. nello stesso ricomprese;

VISTA la Delibera n. 347 del 08/07/2022 avente ad oggetto "*Sistema aziendale di deleghe e conseguente individuazione delle competenze nell'adozione degli atti amministrativi*" con la quale, tra l'altro, sono state individuate le competenze nell'adozione degli atti amministrativi;

la Deliberazione del C.S. n. 329 del 15/03/2024 di integrazione della Deliberazione n. 347 del 08/07/2022;

VISTO il D.LGS. 36 del 31 marzo 2023 "Codice dei contratti pubblici" nel quale è previsto, all'art. 226 comma 2, che a decorrere dalla data in cui il codice acquista efficacia ai sensi dell'articolo 229, comma 2, le disposizioni di cui al decreto legislativo n. 50 del 2016 continuano ad applicarsi ai procedimenti in corso e che per procedimenti in corso, rientrano, tra gli altri, le procedure e i contratti per i quali i bandi o avvisi con cui si indice la procedura di scelta del contraente siano stati pubblicati prima della data in cui il codice acquista efficacia;

PREMESSO CHE con Delibera n. 45 del 18/01/2022 questa Asl procedeva con l'acquisizione in modalità SaaS, l'attivazione e la gestione della piattaforma Cyber Guru per l'attuazione del programma di formazione e addestramento di Cyber Security Awareness (da ora in poi CSA) per tutti i dipendenti ASL Roma 1, per una durata di 12 mesi- Fornitore CYBER-BEE S.R.L. - Spesa complessiva: € 137.150,00 IVA esente - CIG 9049809AA1;

con Delibera n. 262 del 03/03/2023 questa Asl aderiva all'Accordo Quadro Consip "SERVIZI DI SICUREZZA DA REMOTO, COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - Lotto 2" (Cig madre 8884642E81) - SSN - ID 2296" con il Fornitore RTI Deloitte Risk Advisory S.r.l. (Mandataria), per la l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche

Amministrazioni per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 2.272.327,70 iva esclusa, comprensivi delle quote per incentivi funzioni tecniche (€ 2.770.660,69 iva inclusa) per un periodo di 36 mesi. (CIG Derivato 9668894FBA);

con Delibera n. 241 del 25/05/2023 questa Asl procedeva con un affidamento del servizio di manutenzione e supporto sull'infrastruttura di posta elettronica, nonché del servizio di assistenza e manutenzione applicativa e sistemistica sul portale www.aslroma1.it, per le esigenze della ASL Roma 1 fino al 31/12/2023 – costo complessivo € 78.000,00 Iva esclusa, corrispondente a € 95.160,00 Iva inclusa - Fornitore: Laboratori Guglielmo Marconi S.p.A. - CIG: 9806836913;

con Delibera n. 1145 del 01/10/2024 questa Asl procedeva con un affidamento diretto, ai sensi dell'art. 50 comma 1 lett. b) del D. Lgs. 36/2023, tramite mercato elettronico della pubblica amministrazione (Mepa), finalizzata alla fornitura di n. 41 licenze coterm Fortinet "Forti - Coterm -ID 5343879-1" per il funzionamento degli apparati fortigate per le esigenze della Asl Roma 1, sino al 31/12/2024 - Fornitore: Fastweb S.p.A - Spesa complessiva: € 44.800,00 IVA esclusa, corrispondente ad € 54.656,00 IVA inclusa;

con con D.M. del 24 febbraio 2000 pubblicato sulla G.U. della Repubblica Italiana – Serie generale n. 58 del 10 marzo 2000, il Ministero ha affidato alla Consip S.p.A. tra l'altro l'assistenza nella pianificazione e nel monitoraggio dei fabbisogni di beni e servizi delle Pubbliche Amministrazioni;

l'Agenzia per l'Italia Digitale prevede espressamente, fra gli strumenti e le risorse per l'attuazione del Piano triennale per l'informatica nella Pubblica Amministrazione, la realizzazione degli acquisti utilizzando le iniziative Consip e, nello specifico, "Tra le iniziativa Consip, quelle che da una prima analisi possono trovare applicazione nella realizzazione delle linee di azione del Piano da parte delle P, sono gli Accordi quadro e le Convenzioni/Contratti quadro", come indicato nel Piano Triennale 2017-2019, Allegato 2, punto 4 "Iniziative Consip";

CONSIDERATO CHE la vigente normativa in materia di acquisizione beni e servizi, come da ultimo modificata dalla legge 28 dicembre 2015, n. 208, prevede l'obbligo per gli Enti del SSN:

- di approvvigionarsi utilizzando le convenzioni stipulate dalle centrali regionali di riferimento ovvero, qualora non siano operative convenzioni regionali. le convenzioni-quadro stipulate da Consip S.p.A.; (art. 1, comma 449, l. 296/2006; art. 1 comma 548, l. 208/2015);

ATTESTATO che in data 24/05/2022 è stato aggiudicato da Consip S.p.A. al RTI ACCENTURE S.P.A. - FINCANTIERI NEXTECH S.P.A. FASTWEB S.P.A. – DEAS - DIFESA E ANALISI SISTEMI S.P.A, l'Accordo Quadro per i servizi di sicurezza da remoto, di complicance e controllo per le Pubbliche Amministrazioni (ID 2296) – Lotto 1;

che a partire dal mese di Novembre 2022 il nuovo Accordo Quadro è stato reso attivo per le pubbliche amministrazioni interessate;

che con Delibera n. 262 del 03/03/2023, sopra indicata, si aderiva all'Accordo Quadro Consip "Servizi di sicurezza da remoto, compliance e controllo per le pubbliche amministrazioni - ID 2296 – Lotto 2" con la quale si provvedeva all'affidamento dei soli servizi di compliance e controllo Pubbliche Amministrazioni Locali ovvero alla sola

gestione di formazione e adeguamento normativo del NIS, al RTI Deloitte Risk Advisory S.r.l. (Mandataria);

che la medesima Convenzione al Lotto 1 prevede la gestione dei servizi di sicurezza da remoto;

che, pertanto, la Asl Roma 1 ha necessità di procededere all'adesione della suddetta convenzione al fine di assicurare, in caso di riscontro di eventuali anomalie, vulnerabilità critiche e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali in modo da ottenere interventi di natura correttiva mediante sistema di monitoraggio;

ALTRESI' che, secondo quanto previsto nella Guida al contratto quadro per "Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296), la scrivente Azienda ha redatto un "Piano dei Fabbisogni" contenente la descrizione delle esigenze aziendali e le indicazioni di tipo quantitativo dei servizi ritenuti necessari, inoltrandolo al RTI Aggiudicatario con Pec Prot. n. 149309 del 25/09/2024;

che con PEC prot. n. 173698/2024 del 04/11/2024 l'RTI suindicato ha inviato il Piano Operativo identificato come AQSEC-2296L1, che forma parte integrante del presente provvedimento (All.1);

DATO ATTO che secondo quanto previsto dalla citata Guida al contratto quadro, l'Amministrazione, entro 30 giorni solari dalla relativa ricezioni, ha facoltà di approvare il Piano Operativo e che il Contratto si perfeziona a seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione del Piano operativo da parte dell'operatore economico;

che, come previsto dalla normativa sulla tracciabilità dei flussi finanziari, di cui alla legge n. 136/2010, è stato generato il CIG derivato B43A6ED93D;

che, pertanto, il costo complessivo derivante dal presente provvedimento, per un importo pari a Euro **7.607.726,94** Iva esclusa corrispondente ad Euro **9.281.426,87** Iva inclusa per un periodo di 48 mesi sino alla data del 31 Dicembre 2028, verrà imputata, sul conto di bilancio C.E 502020106 "Servizi di Assistenza Informatica", come di seguito specificato:

€ 2.596.103,07 iva inclusa – Bilancio 2025
€ 2.321.046,75 iva inclusa – Bilancio 2026
€ 2.321.046,75 iva inclusa – Bilancio 2027
€ 2.043.230,31 iva inclusa – Bilancio 2028

che il RUP è il Dott. Massimiliano Coltellacci, Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione ed il Direttore dell'esecuzione del contratto (DEC) del servizio in oggetto, ai sensi dell'art. 114 del D.lgs. n.36/2016, è la D.ssa Michela Mazzotta della UOC Sistemi e Tecnologie Informatiche e di Comunicazione;

ATTESO che il Responsabile del Procedimento è il Dott. Massimiliano Coltellacci, Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione, cui compete la verifica e l'accertamento della regolarità e qualità della fornitura resa, anche ai fini della liquidazione;

ATTESTATO che il presente provvedimento a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge n. 241/1990 e successive modifiche ed integrazioni;

PROPONE

Per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire all'accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i., avente ad oggetto l'affidamento di servizi di sicurezza da remoto, compliance e controllo per le Pubbliche Amministrazioni - ID 2296 – Lotto 1 (Cig Madre: 88846293CA), per un periodo di 48 mesi sino alla data del 31 Dicembre 2028 per un importo di € 7.607.726,94 Iva esclusa corrispondente ad € 9.281.426,87 Iva inclusa – Operatore economico RTI costituito ACCENTURE S.P.A. - FINCANTIERI NEXTECH S.P.A. FASTWEB S.P.A. – DEAS - DIFESA E ANALISI SISTEMI S.P.A). CIG B43A6ED93D;

di approvare il Piano Operativo pervenuto con PEC prot. n. 173698/2024 del 04/11/2024 che forma parte integrante del presente provvedimento;

di dare atto che la spesa di pari ad Euro 9.281.426,87 Iva inclusa, derivante dal presente provvedimento verrà imputato sul C.E 502020106 "Servizi di Assistenza Informatica" cosi come di seguito dettagliato:

€ 2.596.103,07 iva inclusa – Bilancio 2025
€ 2.321.046,75 iva inclusa – Bilancio 2026
€ 2.321.046,75 iva inclusa – Bilancio 2027
€ 2.043.230,31 iva inclusa – Bilancio 2028

di indicare come RUP il Dott. Massimiliano Coltellacci, Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione; come Direttore dell'esecuzione del contratto (DEC) del servizio in oggetto, ai sensi dell'art. 114 del D.lgs. n.36/2016, la D.ssa Michela Mazzotta della UOC Sistemi e Tecnologie Informatiche e di Comunicazione;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile del procedimento	Il Direttore sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione	Il Direttore Dipartimento Tecnico Patrimoniale
Dott. Massimiliano Coltelacci	Dott. Massimiliano Coltelacci	Ing. Paola Brazzoduro

IL COMMISSARIO STRAORDINARIO

IN VIRTÚ dei poteri previsti:

- dall'art. 3 del D. Lgs 502/1992 e ss.mm.ii;

- dall'art. 8 della L.R. n. 18/1994 e ss.mm.ii;

nonché delle funzioni e dei poteri conferitigli con Decreto del Presidente della Regione Lazio n. T00013 del 5 aprile 2023;

Letta la proposta di delibera sopra riportata presentata dal Dirigente Responsabile dell'Unità in frontespizio indicata;

PRESO ATTO che il Direttore della Struttura proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge 241/1990 e successive modifiche ed integrazioni;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario riportati in frontespizio;

DELIBERA

di adottare la proposta di deliberazione avente per oggetto "*Adesione all'accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i., avente ad oggetto l'affidamento di servizi di sicurezza da remoto, compliance e controllo per le Pubbliche Amministrazioni - ID 2296 – Lotto 1 (Cig Madre: 88846293CA), per un periodo di 48 mesi sino alla data del 31 Dicembre 2028 per un importo di € 7.607.726,94 Iva esclusa corrispondente ad € 9.281.426,87 Iva inclusa – Operatore economico RTI costituito ACCENTURE S.P.A. - FINCANTIERI NEXTECH S.P.A. FASTWEB S.P.A. – DEAS - DIFESA E ANALISI SISTEMI S.P.A). CIG* B43A6ED93D" e conseguentemente, per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire all'accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i., avente ad oggetto l'affidamento di servizi di sicurezza da remoto, compliance e controllo per le Pubbliche Amministrazioni - ID 2296 – Lotto 1 (Cig Madre: 88846293CA), per un periodo di 48 mesi sino alla data del 31 Dicembre 2028 per un importo di € 7.607.726,94 Iva esclusa corrispondente ad € 9.281.426,87 Iva inclusa – Operatore economico RTI costituito ACCENTURE S.P.A. - FINCANTIERI NEXTECH S.P.A. FASTWEB S.P.A. – DEAS - DIFESA E ANALISI SISTEMI S.P.A). CIG B43A6ED93D;

di approvare il Piano Operativo pervenuto con PEC prot. n. 173698/2024 del 04/11/2024 che forma parte integrante del presente provvedimento;

di dare atto che la spesa di pari ad Euro 9.281.426,87 Iva inclusa, derivante dal presente provvedimento verrà imputato sul C.E 502020106 "Servizi di Assistenza Informatica" cosi come di seguito dettagliato:

€ 2.596.103,07 iva inclusa – Bilancio 2025
€ 2.321.046,75 iva inclusa – Bilancio 2026
€ 2.321.046,75 iva inclusa – Bilancio 2027
€ 2.043.230,31 iva inclusa – Bilancio 2028

di indicare come RUP il Dott. Massimiliano Coltellacci, Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione; come Direttore dell'esecuzione del contratto (DEC) del servizio in oggetto, ai sensi dell'art. 114 del D.lgs. n.36/2016, la D.ssa Michela Mazzotta della UOC Sistemi e Tecnologie Informatiche e di Comunicazione;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della

normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile della struttura proponente provvederà all'attuazione della presente deliberazione curandone altresì la relativa trasmissione agli uffici/organi rispettivamente interessati.

Il COMMISSARIO STRAORDINARIO
Dr. Giuseppe Quintavalle
FIRMATO DIGITALMENTE

ASL RM/1
ALLEGATO 1
Prot. n. 173693/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

Accordo quadro avente ad oggetto l'affidamento
di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

ID 2296 - **LOTTO** 1

Piano Operativo

AQ SICUREZZA

accenture | FASTWEB | FINCANTIERI | DEAS

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

Rev.	Data	Descrizione delle modifiche	Autore
01	31/10/2024	Prima emissione	RTI

Tabella 1 – Registro delle versioni

Il PO inviato in data 14/10/2024 è sostituito integralmente dal presente PO del 31/10/2024.

Il presente PO è difforme dal precedente PO inviato in data 14/10/2024 nelle sezioni di seguito riportate:

- All'Art. "4.1 Attività in carico alle aziende del RTI" in "Tabella 5 – Ripartizioni attività in carico" sono state aggiornate le quote dell'RTI ed i relativi importi.
- All'Art. 7.5 "Modalità di ricorso al Subappalto da parte del Fornitore" è stata aggiornata la "Tabella 11 - Modalità di ricorso al Subappalto da parte del Fornitore".

Relativamente agli allegati riportati in calce devono essere considerati validi quelli trasmessi in data 14/10/2024; pertanto non si procederà alla loro sostituzione.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

Le informazioni contenute nel presente documento sono di proprietà di Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A. e non possono, al pari di tale documento, essere riprodotte, utilizzate o divulgate in tutto o in parte a terzi senza preventiva autorizzazione scritta delle citate aziende.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

Sommario

Indice delle tabelle

Indice delle figure

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

1 INTRODUZIONE

L'Azienda Sanitaria Locale Roma 1, (nel seguito anche "Amministrazione", “Azienda” o “ASL Roma 1”) è un nuovo soggetto giuridico pubblico, nato il 1° gennaio 2016 a seguito della fusione tra la ASL Roma A e la ASL Roma E ed include gli Ospedali Santo Spirito, San Filippo Neri, oltre ad Ambulatori e Case della Salute. La ASL Roma 1 è, dunque, l’esito di un percorso di trasformazione in un’unica realtà di tre aziende sanitarie, in attuazione dei programmi operativi della Regione Lazio 2013-2015. La nascita della nuova Azienda non si configura come una mera crescita dimensionale, ma implica la costruzione di una nuova identità, per una Azienda chiamata ad essere il punto di riferimento per i bisogni di salute di una gran parte dei cittadini residenti sul territorio romano.

Di seguito vengono indicate le strutture territoriali direttamente gestite (poliambulatori, consultori, centri di salute mentale, SERT, etc.).

- N° 44 Poliambulatori
- N° 33 Consultori
- N° 16 Centri di Salute mentali
- N° 6 SERT
- N° 6 Case della Salute
- N° 34 DSM - Centri Diurni e Residenzialità
- N° 3 Strutture riabilitative ex art. 26
- N° 1 Residenze Sanitarie Assistite (RSA)
- N° 6 Disabili Adulti
- N° 1 Hospice Santa Francesca Romana

Le sedi principali della Azienda, tutte site in Roma, sono le seguenti:

- Via Ludovico Ariosto, 3
- Borgo Santo Spirito, 3
- San Filippo Neri – Via Giovanni Martinotti, 20
- P.zza S. Maria della Pietà, 5
- Via Eugenio Di Mattei, 60
- Nuovo Regina Margherita – Via Emilio Morosini, 30
- Circ.ne Nomentana, 498

1.1 Scopo

L'ASL Roma 1, una delle più grandi strutture sanitarie presenti sul territorio nazionale, è composta da una rete capillare di ospedali, centri medici, e strutture di supporto che forniscono servizi sanitari essenziali a una vasta popolazione. La crescente digitalizzazione dei servizi sanitari e la necessità di proteggere dati sensibili richiedono un'infrastruttura IT robusta, sicura e affidabile. In questo contesto, emerge la necessità di monitorare e proteggere l'ampio perimetro IT dell'ASL, che include endpoint su vari sistemi operativi, dispositivi medici, server e infrastrutture di rete distribuite su più distretti.

L'infrastruttura IT di ASL Roma 1 rappresenta il cuore pulsante delle operazioni sanitarie quotidiane, supportando una vasta gamma di servizi essenziali che vanno dalla cura del paziente alla ricerca medica, dalla gestione delle risorse umane alla comunicazione interna ed esterna. Questo capitolo offre una panoramica dettagliata delle componenti chiave dell'infrastruttura IT, evidenziando la complessità e la diversità dei sistemi e dei dispositivi in uso.

Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

ASL Roma 1 si estende su un'area che comprende 89 Sedi, divise tra 6 distretti (municipi), tra cui quattro principali: SAN FILIPPO NERI, SANTO SPIRITO, NUOVO REGINA MARGHERITA e SANTA MARIA DELLA PIETÀ. Ogni distretto ospita strutture sanitarie, uffici amministrativi e laboratori di ricerca, creando una rete eterogenea di sedi che necessitano di connettività, sicurezza e supporto IT coordinati.

Sintesi delle Risorse IT

La rete IT dell'ASL Roma 1 è costituita da circa 1352 elementi attivi (switch/firewall/router/apc) oltre 4.100 endpoint, divisi tra dispositivi che operano su sistemi operativi Windows e Linux, 401 dispositivi medici, e 586 server che supportano le operazioni giornaliere e la gestione dei dati dei pazienti e delle funzioni amministrative e tecniche di questa Azienda. Questi dispositivi sono distribuiti in tutto il territorio di competenza dell'ASL ROMA 1, inclusi ospedali, cliniche, e uffici amministrativi, richiedendo una gestione IT centralizzata e sicura.

Endpoint

Gli endpoint includono computer di lavoro, laptop e dispositivi mobili utilizzati dal personale medico e amministrativo. Sono monitorati attraverso soluzioni di sicurezza come Wazuh, Sophos, e Sysmon per i sistemi Windows, con l'obiettivo di garantire la protezione da malware, ransomware e altre minacce informatiche.

Sintesi componenti sistema di sicurezza

Di seguito si riportano le funzionalità/sistemi principali dell’attuale sistema di sicurezza di ASL Roma 1:

Gestione e Monitoraggio degli Endpoint	Migrazione verso Elastic Agent (attualmente sono in uso Sonde Wazuh e Sophos
Ingestion dei Log	Integrazione tra Wazuh ed Elasticsearch
Acquisizione IDS/IPS	Basato su server Suricata distribuiti su 4 sedi principali di San Filippo Neri, Santo Spirito, Santa Maria della Pietà e Nuovo Regina Margherita
WAF Pubblico	Piattaforma Cloud Barracuda
Autenticazione a Doppio Fattore MFA	Basato su FortiAuthenticator di Fortinet
Asset Management e Controllo dei Dispositivi	Basato su piattaforma LANSWEEPER
Threat Intelligence e modeling	Aggregazione ed analisi dei dati di intelligence ed uso di tecniche di Modeling quali ATT&CK di MITRE, nonché collegamento con i sistemi di Allerta Compromissione Nazionale (ACN)
Controllo e Gestione di Tutti gli Eventi di Sistema	Basato su piattaforma PRTG Network Monitor
Privileged Access Management (PAM)	Basato su FortiPAM di Fortinet
Network Access Control (NAC)	Basato su FortiNAC di Fortinet

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

Dashboard Principali e Reportistica	Basati su Server Kibana e Dashboard Medigate
Backup dell'Infrastruttura IT	Utilizzo di Veeam che opera su piattaforme tecnologiche come VMware e Nutanix
Monitoraggio dei Dispositivi Medici	Basato su Claroty Medigate

ASL Roma 1 necessita dei servizi di seguito indicati, al fine di assicurare, in caso di riscontro di eventi anomalie, vulnerabilità critiche e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati da ASL Roma 1. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio.

1.2 Ambito di Applicabilità

Il **Piano Triennale per l'informatica della Pubblica Amministrazione** è uno strumento essenziale per promuovere la trasformazione digitale dell'amministrazione italiana e del Paese e, in particolare quella della Pubblica Amministrazione (PA) italiana. Tale trasformazione dovrà avvenire nel contesto del mercato unico europeo di beni e servizi digitali, secondo una strategia che in tutta la UE si propone di migliorare l'accesso online ai beni e servizi per i consumatori e le imprese e creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi per massimizzare il potenziale di crescita dell'economia digitale europea. In tale contesto dove quindi i servizi digitali rappresentano un elemento indispensabile per il funzionamento di un Paese, la PA ne è parte fondamentale e indispensabile.

È ampiamente noto che la minaccia cibernetica è sempre più attiva e cresce continuamente in qualità e quantità minacciando infrastrutture critiche, processi digitali e rappresentando anche un elevato rischio di natura militare visto l'utilizzo che è sempre più diffuso verso quello che chiamiamo il perimetro di sicurezza cibernetico. In questo scenario di notevole fermento, il Piano delle Gare Strategiche ICT, concordato tra Consip e AgID, ha l'obiettivo, tra le altre cose, di mettere a disposizione delle Pubbliche Amministrazioni delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza. Il Piano mantiene l'attenzione rispetto al passato ponendosi anche il cruciale problema della protezione del dato. Questo elemento è fondamentale perché tale protezione è strettamente connessa alla sua qualità e agire correttamente consente di attuare anche gli obblighi normativi europei in materia di protezione dei dati personali (GDPR).

Il Piano si focalizza sulla **Cyber Security Awareness**, poiché tale consapevolezza fa scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche. Nella PA ci sono frequenti attacchi a portali che bloccano i servizi erogati e costituiscono danno di immagine. È in crescita anche il fenomeno denominato data breach (violazione dei dati) che rappresenta anche una grave violazione del GDPR. Le azioni stabilite nel Piano sono tutte indispensabili rispetto allo scenario possibile. Oltre agli attori coinvolti nel Piano resta indispensabile e cruciale il supporto del Garante per la protezione dei dati personali quantomeno per verificare se la PA ha nominato un adeguato DPO (figura obbligatoria per il GDPR) ed è organizzata, almeno ai minimi termini, in linea con le regole del GDPR (Regolamento europeo 679/2016). Il Piano affida a Linee guida e regole specifiche ma anche alle strutture specifiche di AgID il supporto alle Pubbliche Amministrazioni.

In particolare, AgID ha concordato l'indirizzo strategico per la progettazione della presente iniziativa con particolare riferimento sui contenuti tecnici e sui meccanismi di coordinamento e controllo dell'utilizzo dello strumento di acquisizione; Consip S.p.A., in qualità di soggetto Stazione Appaltante, ha aggregato i fabbisogni e predisposto la procedura di gara e gestirà la stipula dei contratti per le amministrazioni centrali e locali. Le PA devono intraprendere

misure ed azioni per l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi definiti nel Piano Triennale.

In capo ai Fornitori è la responsabilità di supportare le Amministrazioni mediante i servizi resi disponibili dalla presente iniziativa e supportare i soggetti deputati al coordinamento e controllo, secondo quanto previsto dalla documentazione di gara.

L'RTI ha basato il modello di tali servizi 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), integrando i requisiti normativi co-genti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al Framework Nazionale per la Cybersecurity e la Data Protection.

In particolare, nella figura sottostante è riportata la mappatura dei servizi offerti al Framework, al fine di illustrare come tali servizi siano funzionali a ciascuna area del Framework.

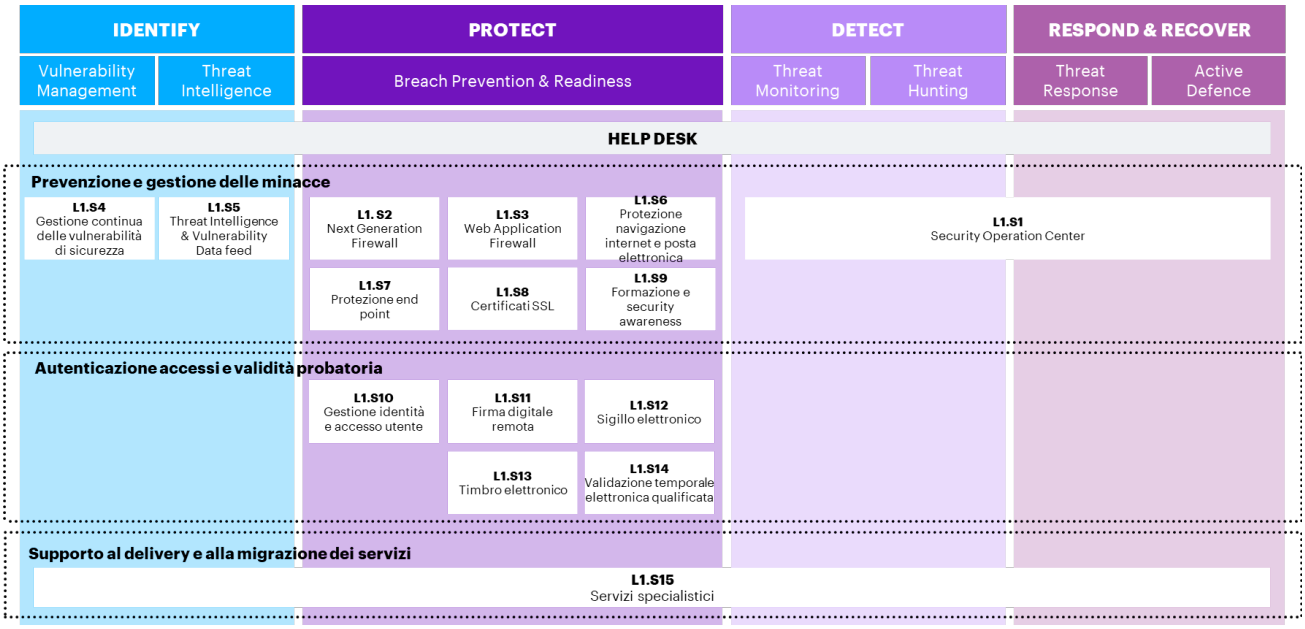

Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

In linea con le previsioni del Piano Triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, sono previste la definizione e l'implementazione di misure di governance centralizzata, anche mediante la costituzione di **Organismi di coordinamento e controllo**, finalizzati alla direzione strategica e alla direzione tecnica della stessa. In particolare, le attività di direzione strategica prevedono il coinvolgimento di soggetti istituzionali, mentre nell'ambito delle attività di direzione tecnica saranno coinvolti anche soggetti non istituzionali, individuati nei Fornitori Aggiudicatari della presente acquisizione. Si precisa che per "Organismi di coordinamento e controllo", si intendono i soggetti facenti capo alla Presidenza del Consiglio e/o al Ministero per l'Innovazione tecnologica e la Digitalizzazione (es: Agid, Team Digitale), che, in base alle funzioni attribuite ex lege, sono ad oggi deputati, per quanto di rispettiva competenza, al monitoraggio e al controllo delle iniziative rientranti nel Piano Triennale per l'informatica nella Pubblica Amministrazione. Nell'ambito di tali Organismi è ricompresa altresì Consip S.p.A., per i compiti di propria competenza. Rimangono salve eventuali modifiche organizzative che interverranno a livello istituzionale nel corso della durata del presente Accordo Quadro.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

Gli Organismi di coordinamento e controllo saranno normati da appositi Regolamenti che, resi disponibili alla stipula dei contratti relativi alla presente iniziativa o appena possibile, definiranno gli aspetti operativi delle attività di coordinamento e controllo, sia tecnico che strategico.

I meccanismi di governance sopra introdotti e applicati anche a tutte le iniziative afferenti al Piano Triennale riguarderanno:

i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip;
l'inquadramento o categorizzazione degli interventi delle Amministrazioni, realizzati mediante la sottoscrizione di uno o più contratti esecutivi afferenti alle iniziative del Piano Strategico, nel framework del Piano Triennale;
l'individuazione, da parte delle Amministrazioni beneficiarie, secondo quanto fornito in documentazione di gara, degli indicatori di digitalizzazione coi quali gli Organismi di coordinamento e controllo analizzeranno e valuteranno gli interventi realizzati dalle Amministrazioni con i contratti afferenti alle Gare strategiche;
la valutazione e l'attuazione della revisione dei servizi previsti dagli Accordi Quadro e/o dei relativi prezzi, per le Gare Strategiche che lo prevedono in documentazione di gara e in funzione dell'evoluzione tecnologica del mercato e/o della normativa applicabile;
l'analisi e la verifica di coerenza, rispetto al perimetro di ogni Gara Strategica, degli interventi delle Amministrazioni realizzati mediante contratti attuativi afferenti alle Gare Strategiche;
le modalità e le tempistiche con cui i fornitori dovranno consegnare i dati relativi ai contratti esecutivi, con particolare riferimento alla fase di chiusura degli Accordi Quadro.

L'iniziativa in oggetto si affianca alle gare strategiche previste da AgID ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese. Storicamente, il Sistema Pubblico di Connettività (SPC) ha seguito la rete unitaria della pubblica amministrazione (RUPA), nata con l'intento di connettere le pubbliche amministrazioni, almeno quelle centrali. Il Sistema Pubblico di Connettività (SPC), è posto alla base delle infrastrutture materiali dell'architettura disegnata nel Piano Triennale l'informatica nella Pubblica Amministrazione 2017-2019 di AgID, il cosiddetto Modello Strategico. È un sistema composto da molti servizi stratificati, dalla connettività ai servizi Cloud, ed è stato aggiornato nel 2016 con nuove gare Consip SPC2, SPC Cloud ampliando il portafoglio dei servizi e delle infrastrutture.

L'iniziativa Sicurezza da remoto si pone un **duplice obiettivo**:
quello di garantire la continuità e l'evoluzione dei servizi già previsti nella precedente iniziativa SPC Cloud – Lotto 2 avente ad oggetto servizi di sicurezza volti alla protezione dei sistemi informativi in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema pubblico di connettività;
quello di rendere disponibili alle Amministrazioni servizi con carattere di innovazione tecnologica per l'attuazione del Codice dell'Amministrazione Digitale, nonché del Piano Triennale ICT della PA.

Lo scenario è contestualmente caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo. Tale specializzazione si innesta in considerazione dei diversi obiettivi a cui i due Lotti rispondono.
In particolare:
il **Lotto di servizi di Sicurezza da remoto (Lotto 1)** ha l'obiettivo di mettere a disposizione delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati;
il **Lotto di servizi di Compliance e controllo (Lotto 2)** ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di salute della sicurezza del sistema informativo dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 nonché sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

In riferimento a quanto sopra riportato**, ASL Roma 1** intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

Nell'ambito di tale lotto, si riportano di seguito i **servizi fruibili**, così come previsto dall'Accordo Quadro:
L1.S1 - Security Operation Center (SOC)
L1.S2 - Next Generation Firewall
L1.S3 - Web Application Firewall
L1.S4 - Gestione continua delle vulnerabilità di sicurezza
L1.S5 - Threat Intelligence & Vulnerability Data Feed
L1.S6 - Protezione navigazione Internet e Posta elettronica
L1.S7 - Protezione degli endpoint
L1.S8 - Certificati SSL
L1.S9 - Servizio di Formazione e Security awareness
L1.S10 - Gestione dell'identità e l'accesso utente
L1.S11 - Firma digitale remota
L1.S12 - Sigillo elettronico
L1.S13 - Timbro elettronico
L1.S14 - Validazione temporale elettronica qualificata
L1.S15 - Servizi specialistici

A tal fine, **ASL Roma 1**, ha individuato il Raggruppamento Temporaneo di Imprese (RTI) composto da Accenture S.p.A. (Accenture, impresa mandataria), Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri), e Difesa e Analisi Sistemi S.p.A. (DEAS) , quale aggiudicatario dell'Accordo Quadro che effettuerà la prestazione, sulla base di decisione motivata in relazione alle specifiche esigenze dell'amministrazione e in relazione a quanto stipulato nell'Accordo Quadro di riferimento.

1.3 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra ASL Roma 1 e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

Tabella 1 - Assunzioni

Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

2 RIFERIMENTI

1.4 Normativa di riferimento

Trovano applicazione le normative e gli standard internazionali riportate al “Capitolato Tecnico Generale” (§ 4.6) [].

1.5 Documenti Applicabili

Rif.	Titolo
DA-1.	ALLEGATO 1 - CAPITOLATO TECNICO GENERALE - 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.
DA-2.	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
DA-3.	Accordo Quadro
DA-4.	Offerta Tecnica – Lotto 1 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
DA-5.	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
DA-6.	Piano dei Fabbisogni nominato: “ASL Roma 1 - AQ 2296_Lotto 1_Sicurezza da Remoto_Piano dei fabbisogni_ver 1.0” PEC del 25/09/2024

Tabella 2 - Documenti Applicabili

ASL_RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

3 DEFINIZIONI E ACRONIMI

1.6 Acronimi

Definizione	Descrizione
Accordo Quadro (AQ)	L'Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A. all'esito della procedura di gara di prima fase
Aggiudicatario / Fornitore	Se non diversamente indicato vanno intesi gli aggiudicatari previsti per ciascun AQ per ciascuno dei Lotti della fornitura
Amministrazioni	Pubbliche Amministrazioni
Amministrazione Aggiudicatrice	Consip S.p.A.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato o intendono affidare un contratto esecutivo con il Fornitore per l'erogazione di uno dei servizi oggetto dell'Accordo Quadro
Capitolato Tecnico Generale	Documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa
Capitolati Tecnici Speciali	Integrano il Capitolato Tecnico Generale e definiscono i contenuti di dettaglio e i requisiti minimi in termini di quantità, qualità e livelli di servizio, relativamente al Lotto 1 avente ad oggetto i Servizi di Sicurezza da remoto e al Lotto 2 avente ad oggetto i Servizi di Compliance e controllo
Collaudo e verifica di Conformità	Effettuati dall'Amministrazione e corrispondenti alla valutazione con verifica di merito dei prodotti consegnati
Componente	Il singolo elemento della configurazione di un sistema sottoposto a monitoraggio
Contratto Esecutivo	Il Contratto avente ad oggetto Servizi di Sicurezza da remoto, di Compliance e di Controllo per le Pubbliche Amministrazioni (Lotto 1)
Piano dei Fabbisogni	Il documento inviato dall'Amministrazione al Fornitore, al quale l'Amministrazione medesima affida il singolo Contratto Esecutivo e nel quale dovranno essere riportate, tra l'altro, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore
Piano Operativo	Il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel presente documento
Prodotto della Fornitura	Tutto ciò che viene realizzato dal fornitore. Comprende tutta la documentazione contrattuale e gli artefatti come definiti nell'appendice Livelli di servizio
Modalità di erogazione da remoto	Servizio erogato - in modalità *managed* - attraverso i Centri Servizi del Fornitore
Modalità di lavoro *On-site*	Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa o in alternativa presso la sede del Fornitore
Milestone	In ingegneria del software e Project Management indica ciascun traguardo intermedio e il traguardo finale dello svolgimento del progetto. Sono i punti di controllo all'interno di ciascuna fase oppure di consegna di specifici deliverable o raggruppamenti di deliverable. Sono normalmente attività considerate convenzionalmente a durata zero che servono per isolare nella schedulazione i principali momenti di verifica e validazione. Di fatto ciascun punto di controllo serve per approvare quanto fatto a monte della milestone ed abilitare le attività previste a valle della milestone
Sistema	Per Sistema si intende la singola immagine del sistema operativo, comprensiva di tutte le periferiche fisiche e/o logiche e di tutti i prodotti e/o servizi necessari al corretto funzionamento delle applicazioni, oppure l'insieme delle componenti HW e SW inserite in un unico chassis atto alla interconnessione e l'estensione di reti TLC (ad esempio apparati che gestiscono i primi quattro livelli della pila ISO-OSI)
Centro Servizi (CS)	La/e sede/i da cui l'Aggiudicatario eroga i servizi in modalità "da remoto" di cui al presente Capitolato per lo specifico Lotto di fornitura
Perimetro di Sicurezza Nazionale Cibernetica	Ai sensi del DL. Del 21 settembre 2002 n.105, il Perimetro è composto dai sistemi informativi e dai servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento,

Definizione	Descrizione
	interruzione, anche parziali

Tabella 3 - Definizioni

Vocabolo	Titolo
AgID	Agenzia per l'Italia Digitale
AQ	Accordo Quadro
BC	Business Continuity
CE	Contratto Esecutivo
CS	Centro Servizi
CTS	Capitolato Tecnico Speciale
DA	Documenti Applicabili
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
HVAC	Heating, Ventilation and Air Conditioning
HW	Hardware
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LRP	Livello di Rischio Previsto
LRR	Livello di Rischio Residuo
MGMT	Management
MPLS	MultiProtocol Label Switching
NDA	Non-Disclosure Agreement
OLO	Other Licensed Operators
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PMO	Project Management Office
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Impresa
RTO	Recovery Time Objective
SAN	Storage Area Network
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SIEM	Security Information and Event Management
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SSL	Secure Sockets Layer
SW	Software
UPS	Uninterruptible Power Supply
UTP	Unified Threat Protection
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

Tabella 4 - Acronimi

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

L'approccio organizzativo che il RTI propone è volto a 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.

L'organizzazione del RTI proposta per la conduzione dell'Accordo Quadro è mostrata nella figura di seguito riportata:

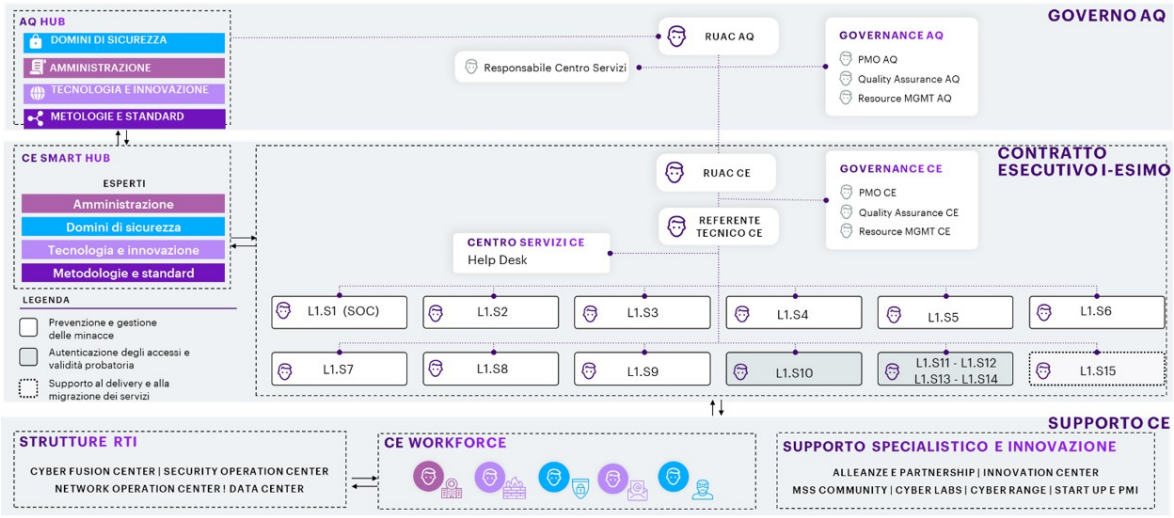

Figura 2 - Organizzazione dell'AQ proposta dal RTI

L'organigramma proposto prevede che il coordinamento delle attività del presente Accordo Quadro venga svolto dal Responsabile Unico della Attività Contrattuali dell'Accordo Quadro.

Il modello proposto si articola sui tre livelli di seguito illustrati:

- **Livello di Governo dell'AQ -** rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera Fornitura. 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 aziende in esso contenute e dal Responsabile del Centro Servizi, 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.
- **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* - 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, 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* - Garantito da:
    - ✓ 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 (FDA-Fastweb Digital Academy), 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.
- **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.

Per quanto concerne invece i **Centri Servizi**, questi vengono coordinati da uno specifico Responsabile che opera a livello "Governo AQ" e in accordo ai seguenti criteri:

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

- 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.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

1.7 Attività in carico alle aziende del RTI

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

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center		X		
L1.S2 – Next Generation Firewall		X		
L1.S3 – Web Application Firewall		X		
L1.S9 – Formazione e Security Awareness		X		
L1.S15 – Servizi Specialistici	X	X		
TOTALE (%)	20,94%	79,06%	0,00%	0,00%
TOTALE (€)	€ 1.592.832,00	€ 6.014.894,94	€ 0,00	€ 0,00

Tabella 5 - Ripartizione attività in carico

1.8 Organizzazione e figure di riferimento del Fornitore

Nella tabella che segue sono riportate le principali figure di riferimento del Fornitore, cui ruoli e responsabilità sono stati illustrati nella parte introduttiva del Capitolo:

FIGURE DI RIFERIMENTO E REFERENTI DEL FORNITORE
RUAC AQ
GOVERNANCE AQ (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
RESPONSABILE CENTRO SERVIZI
RESPONSABILE DI SICUREZZA INFORMATICA E CONTINUITÀ OPERATIVA
RESPONSABILE DI SEDE OPERATIVA
RUAC CE
GOVERNANCE CE (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
REFERENTE TECNICO CE
RESPONSABILI DELL'EROGAZIONE DEI SERVIZI

Tabella 6 - Figure di riferimento e referenti del Fornitore

1.9 Luogo di erogazione e di esecuzione della Fornitura

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

Accenture
Fastweb
Fincantieri NexTech
DEAS

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

- per i servizi erogati da remoto: attraverso i Centri Servizi del Fornitore;
- per i servizi on-site: presso le sedi dell’Amministrazione ove specificato dall’Amministrazione stessa, principalmente presso la sede di Via Ariosto, 8 in Roma.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

2 AMBITI E SERVIZI

2.1 Ambiti di intervento

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti di **ASL Roma 1** così come riportati nel Piano dei Fabbisogni:

- L1.S1 – Security Operation Center
- L1.S2 – Next Generation Firewall
- L1.S3 – Web Application Firewall
- L1.S9 – Formazione e Security Awareness
- L1.S15 – Servizi Specialistici

2.2 Servizi richiesti

Con specifico riferimento ai Servizi L1.S15 Servizi Specialistici, dal momento che vengono richiesti nel Piano dei Fabbisogni, senza uno specifico riferimento al relativo dimensionamento, il RTI propone le quantità come di seguito riportate per l'esecuzione dei relativi servizi come descritti nei paragrafi seguenti.

SERVIZIO	FASCIA	IMPORTO I ANNO/Q.TA	IMPORTO II ANNO/Q.TA	IMPORTO III ANNO/Q.TA	IMPORTO IV ANNO/Q.TA
L1.S1 – Security Operation Center	Fascia 5 - > 6.000 Eps	€ 131.400,00 /Q.TA 584	€ 131.400,00 /Q.TA 584	€ 131.400,00 /Q.TA 584	€ 131.400,00 /Q.TA 584
L1.S2 – Next Generation Firewall	Fascia 2 – Fino a 2 Gbps	€ 35.025,54 /Q.TA 31	€ 35.025,54 /Q.TA 31	€ 35.025,54 /Q.TA 31	€ 35.025,54 /Q.TA 31
	Fascia 3 – Fino a 4 Gbps	€ 64.758,40 /Q.TA 10	€ 64.758,40 /Q.TA 10	€ 64.758,40 /Q.TA 10	€ 64.758,40 /Q.TA 10
	Fascia 4 – Fino a 7 Gbps	€ 21.411,00 /Q.TA 2	€ 21.411,00 /Q.TA 2	€ 21.411,00 /Q.TA 2	€ 21.411,00 /Q.TA 2
	Fascia 5 – Fino a 15 Gbps	€ 184.140,00 /Q.TA 4	€ 184.140,00 /Q.TA 4	€ 184.140,00 /Q.TA 4	€ 184.140,00 /Q.TA 4
L1.S3 – Web Application Firewall	Fascia 1 – Fino a 500 Mbps	€ 5.600,00 /Q.TA 2	€ 5.600,00 /Q.TA 2	€ 5.600,00 /Q.TA 2	€ 5.600,00 /Q.TA 2
L1.S9 – Formazione e Security Awareness	GG/P – Team Ottimale		€ 227.718,40 /Q.TA 920	€ 227.718,40 /Q.TA 920	€ 227.718,40 /Q.TA 920
L1.S15 – Servizi Specialistici	GG/P – Team Ottimale	€ 1.457.900,00 /Q.TA 5.975	€ 1.232.444,00 /Q.TA 5.051	€ 1.232.444,00 /Q.TA 5.051	€ 1.232.444,00 /Q.TA 5.051

Tabella 7 - Servizi richiesti

2.3 Indicatore di progresso

Di seguito l'indicatore di progresso (IP) identificato in questa fase per l'erogazione della fornitura, che sarà determinato come da schema seguente:

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

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 8 - Schema definizione Indicatore di Progresso

Tale indicatore sarà oggetto di revisione con l'Amministrazione a valle della fase di presa in carico. In particolare, sarà attivato uno specifico tavolo di lavoro mirato a:

- valutare il grado di maturità digitale dei servizi offerti e il grado di maturità atteso;
- consolidare l'indicatore;
- definire le misure iniziali dell'indicatore;
- stabilire i target e cioè le misure attese alla fine del contratto.

ASL_RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

3 SOLUZIONE PROPOSTA

3.1 Descrizione dei servizi richiesti

Di seguito i servizi proposti in linea con le esigenze espresse da **ASL Roma 1.**

1.1.1 L1.S1 – Security Operation Center

Il servizio prevede di implementare, attraverso adeguati strumenti tecnologici, un servizio di monitoraggio e alerting degli eventi/minacce di sicurezza al fine di consentire una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle raccomandazioni relative alle azioni di contenimento e ripristino/prevenzione futura.

Il servizio SOC si baserà sui dati raccolti e correlati dal SIEM basato su tecnologia IBM QRadar. Sarà pertanto effettuata una ottimizzazione degli eventi raccolti dai sistemi ed inviati al SIEM, selezionando solo quelli significativi in termini di sicurezza e scartando tutte le righe di log non utili al sistema SIEM ed al servizio SOC, al fine di attuare i servizi previsti nell'offerta tecnica del RTI, tra cui il 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).

È prevista, infine, analisi della reportistica e dei log tale da dare la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.

In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 584 device equivalenti /annui equivalenti a 7.000 EPS/annui in Fascia 5.

Il servizio SOC verrà erogato in modalità remota dal Centro Servizi (di seguito "CS") preposto dal RTI e agirà in modalità strettamente coordinata con gli altri servizi oggetto della presente fornitura, beneficiando delle informazioni da essi raccolte, contribuendo in modalità proattiva al miglioramento continuo delle policy e intervenendo con azioni di inibizione/mitigazione a fronte di evidenze di incidenti o potenziali rischi in essere.

Il servizio sarà configurato in modo tale che anche il personale autorizzato dall'Amministrazione possa avere accesso alle informazioni ed agli alert prodotti dal SOC e dal SIEM, secondo le modalità previste dalla Capitolato Tecnico e dalla risposta tecnica di AQ.

Di seguito si elencano i prerequisiti al servizio, in carico all'Amministrazione:

- Configurazione delle sorgenti di log (eventi di sicurezza) e di rete, per la lettura e/o invio degli eventi utili al Centro Servizi;
- Procedure di security incident management, escalation, Crisis Management.

1.1.2 L1.S2 – Next Generation Firewall

Il servizio di "Next Generation Firewall" prevede nuove forniture, aggiornamenti e gestione di apparati firewall presenti presso diverse sedi di ASL Roma 1, con l'obiettivo di filtrare tutto il traffico che i dispositivi di rete scambiano, sia internamente che esternamente, rispetto a un determinato perimetro limitando o bloccando eventi quali accessi non autorizzati, malware o servizi non consentiti, attraverso una serie definita di regole (policy) di controllo degli accessi e tramite l'orchestrazione di più layer di sicurezza. I firewall previsti sono delle seguenti tipologie:

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

- n° 31 L1.S2 NGFW - Fascia 2 - Fino a 2 Gbps
- n° 10 L1.S2 NGFW - Fascia 3 - Fino a 4 Gbps
- N° 2 L1.S2 NGFW - Fascia 4 - Fino a 7 Gbps
- n° 4 L1.S2 NGFW - Fascia 5 - Fino a 15 Gbps

1.1.3 L1.S3 – Web Application Firewall

Il servizio di “Web Application Firewall” consentirà di filtrare, monitorare e bloccare il traffico HTTP da e verso un servizio Web,
esaminando il traffico, utilizzando regole, analisi e firme per rilevare attacchi e quindi proteggendo l’amministrazione dagli attacchi incorporati nei dati trasmessi dalle applicazioni web. Nell’ambito del servizio di Web Application Firewall saranno garantite le seguenti funzionalità:

- Protezione dagli attacchi più critici alle applicazioni web, quali ad esempio Iniezioni SQL, Cross-site scripting (XSS), inclu-sione di file e configurazioni di sistema impropri, dirottamento di sessioni, buffer overflow;
- Capacità evoluta di filtraggio del traffico con possibilità di configurare l’utilizzo di whitelist e blacklist;
- Funzionalità di apprendimento automatico che consentano di individuare un modello di comportamento dell’utente per identificare il traffico benigno e dannoso delle applicazioni;
- Rilevamento automatico della natura dei contenuti e rilevazione di attacchi che comportino la manomissione di cookie, sessioni o parametri;
- Funzionalità di ispezione del traffico SSL criptato per tutti i tipi di minacce integrate;
- Capacità di identificare/bloccare gli allegati XML che nascondono contenuti dannosi e di convalidare gli schemi per i messaggi SOAP;
- Protezione di Api e web services di qualsiasi natura;
- Supporto per le regole di controllo degli accessi a livello di rete e componente basate sulla firma per rilevare le minacce note;
- Produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.

La coppia di apparati prevista per il servizio in oggetto, in HA e dimensionata per supportare fino a 2.000 utenti giornalieri, sarà installata nell’ambiente virtualizzato di ASL Roma 1 che ospita il sito Internet di ASL Roma 1.

1.1.4 L1.S9 – Formazione e Security Awareness

Il servizio, dimensionato per 7.800 utenti per una durata di 3 anni, prevede di aggiornare/formare il personale specialistico - che opera in ambito cyber security - affrontando ed approfondendo, ad esempio, le seguenti tematiche di sicurezza:

- standard e sistemi di gestione della sicurezza delle informazioni;
- best practice in ambito sicurezza informatica tra cui:
    - infrastrutture critiche,
    - architettura di sistemi e reti,

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

- sistemi di controllo degli accessi,
- sicurezza dei sistemi e delle applicazioni,
- ecc.;

- sicurezza nelle tecnolgie DevOps, container e microservizi cloud e mobile;
- analisi e gestione delle principali minacce IT e dei rischi ad esse connesse;
- analisi e gestione delle vulnerabilità;
- gestione degli incidenti;
- aspetti giuridici, normativi e contrattualistici in ambito sicurezza delle informazioni.

Il servizio verrà erogato mediante la messa a disposizione di figure professionali da parte del Fornitore, coadiuvate dall'utilizzo della piattaforma Cyberguru.

1.1.5 L1.S15 – Servizi Specialistici

I servizi di Supporto Specialistico hanno l'obiettivo di supportare ASL Roma 1 nella realizzazione di attività nell'ambito della sicurezza infrastrutturale, comprensive di quelle relative ai servizi di monitoraggio, attraverso l'utilizzo di specifiche figure professionali messe a disposizione dal Fornitore.
Di seguito si riportano le attività previste nell'ambito dei Servizi Specialistici:

- Realizzazione dell'integrazione del Centro Servizi del Fornitore con i sistemi di sicurezza di proprietà dell'Amministrazione;
- Supporto per l'analisi e gestione delle "remediation" delle vulnerabilità censite;
- Supporto per la gestione delle attività delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni per la gestione delle utenze amministrative;
- Mantenimento e aggiornamento della documentazione di sistemi infrastrutturali e tecnologici gestiti, delle policy di sicurezza stabilite, la produzione della reportistica necessaria;
- Supporto in attività di individuazione e pianificazione delle evoluzioni finalizzate a mantenere l'infrastruttura costantemente aggiornata rispetto alle evoluzioni del panorama delle minacce informatiche, in costante trasformazione;
- Supporto ad Analisi e definizione di policy, procedure e linee guida relative al contesto;
- Supporto all'Amministrazione per il mantenimento del livello di sicurezza nel perimetro individuato dei servizi dell'AQ 2296;
- Supporto alle strutture dell'Amministrazione nella gestione e configurazione di apparati di sicurezza, sistemi e server;
- Supporto nell'implementazione di soluzioni atte a censire tutti gli asset, sia fisici che logici, in uso presso l'Amministrazione.

Per l'espletamento di attività del genere, il Fornitore metterà a disposizione di ASL Roma 1 servizi professionali erogati attraverso l'impiego di figure professionali di comprovata esperienza, maturata nel corso degli anni per le tematiche oggetto del servizio e con riferimento a progetti realizzati presso PA e organizzazioni private, sia nel territorio nazionale sia internazionale.
Il Servizio erogato avrà l'obiettivo di supportare l'Amministrazione nella implementazione di soluzioni tecnologiche e di processo finalizzate di sicurezza, in considerazione di quanto previsto dalle normative vigenti.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

3.2 Utenza interessata / coinvolta

Personale di **ASL Roma 1.**

3.3 Eventuali riferimenti / vincoli normativi

N/A

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

4 PIANO DI PROGETTO

4.1 Cronoprogramma

L'erogazione dei servizi avrà durata 36 mesi per il servizio L1.S9 e 48 mesi per i servizi L1.S1, L1.S2, L1.S3 e L1.S15, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

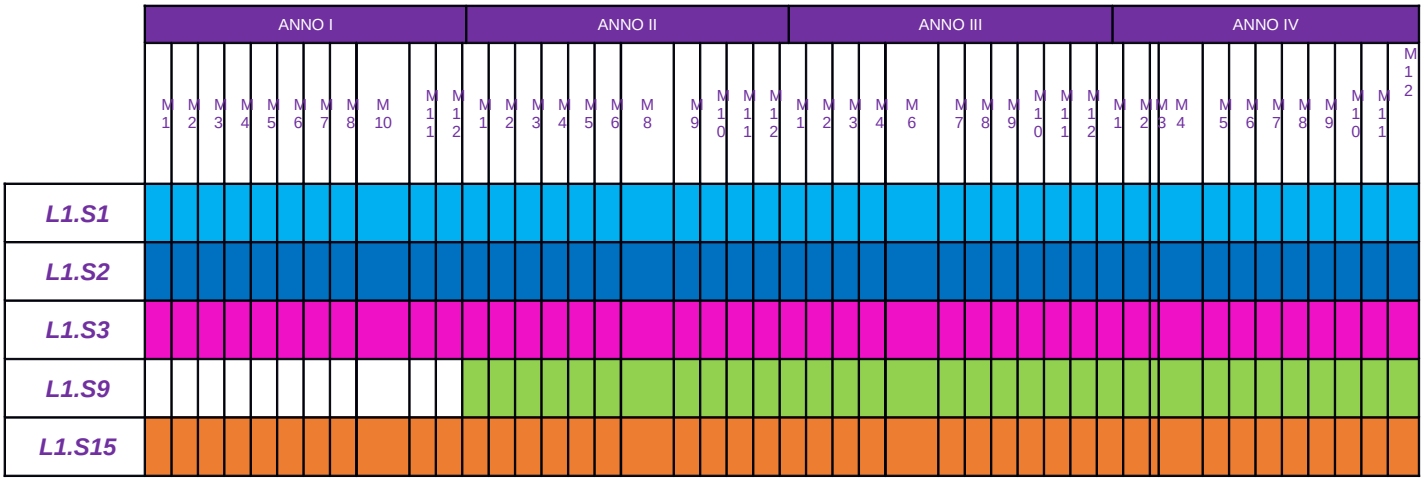

Tabella 9 – Cronoprogramma

4.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo dispiegherà i suoi effetti dalla data di stipula e avrà una durata di 48 mesi, decorrenti dalla data di conclusione delle attività di presa in carico. Si precisa, tuttavia, che la data di attivazione del Progetto è prevista il 1 Gennaio 2025 per i servizi L1.S1, L1.S2, L1.S3 e L1.S15; il 1 Gennaio 2026, invece, per il servizio L1.S9.

4.3 Gruppo di Lavoro

L'approccio organizzativo individuato e descritto all'interno del Capitolo 4 consente di predisporre team e organizzazioni del lavoro secondo condizioni ad hoc per ogni progetto, secondo i carichi di lavoro previsti nella progettualità condivisa ma facilmente scalabili, qualora in corso d'opera maturassero condizioni tali da richiedere una modifica al numero dei team, delle risorse o del perimetro d'intervento. Una volta individuate le peculiarità dell'Amministrazione contraente, la selezione del gruppo di lavoro avviene analizzando il contesto della stessa sia dal punto di vista tecnologico, individuando il personale maggiormente qualificato sulle tecnologie e sui prodotti già in uso o attese, che tematico, andando ad identificare le figure professionali con esperienze e competenze nel settore pubblico.

4.4 Modalità di esecuzione dei Servizi

Per la modalità di esecuzione dei servizi è possibile far riferimento al Capitolo 8 del Capitolato Tecnico Speciale. In generale, a partire dal Piano di Lavoro Generale, l'Amministrazione richiederà la stima ed il Piano di Lavoro del

singolo stream progettuale (obiettivo), fornendo la documentazione di supporto ed i macro-requisiti per poter effettuare una stima dell'obiettivo.
Di seguito si riporta una tabella di sintesi con le principali milestone per ogni servizio:

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	**Amministrazione**
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	**RTI**
Collaudo	Esecuzione del collaudo dei servizi per cui è stato richiesto	**RTI**
Attivazione	Individuazione del ciclo di vita ed avvio del fornitore a procedere con le attività sul servizio. Al momento dell'attivazione saranno noti elementi caratteristici ai quali si associa una valutazione di complessità	**Amministrazione**
Consegna	Rilascio degli artefatti previsti dal piano di lavoro, sia intermedi che finali	**RTI**
Approvazione e Verifica di Conformità	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto	**Amministrazione**
Accettazione e Verifica di Conformità	Verifica e validazione dei prodotti intermedi di servizio, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione	**Amministrazione**
Valutazione difettosità all'avvio e Verifica di Conformità	Verifica della piena fruizione delle funzionalità e dei servizi da parte dell'utente (cittadino/ impresa/ operatore amministrativo/ decisore/ fruitore) tramite l'esame della quantità e della tipologia di malfunzionamenti e non conformità rilevati durante il periodo di avvio in esercizio. Certificazione della corretta esecuzione del servizio	**Amministrazione**

Tabella 10 - Descrizione milestone per obiettivo

Per il Governo della Fornitura, si propone l'adozione delle pratiche di seguito descritte:

- **Stato avanzamenti lavori – tecnico.** Con cadenza mensile (o su richiesta dell'Amministrazione) per le attività progettuali e mensile (o su richiesta dell'Amministrazione) per quelle continuative, verrà prodotto un report di sintesi che sarà discusso nel corso di un meeting ad hoc con l'Amministrazione. Il report riporterà, a livello di progetto e a livello di obiettivo: i) avanzamento e scostamenti rispetto al piano di lavoro; ii) attività svolte e attività previste; iii) rischi e problematiche operative; iv) punti aperti; v) azioni da intraprendere per il corretto svolgimento delle attività.

4.5 Modalità di ricorso al Subappalto da parte del Fornitore

La quota massima di attività subappaltabile – o concedibile in cottimo – da parte del RTI è pari al 50% dell'importo complessivo previsto dal contratto. Di seguito è riportato l'elenco delle attività / prestazioni per parti delle quali il RTI intende ricorrere al subappalto:

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S15 – Servizi Specialistici	**Accenture**	**50%**

Accenture
Fastweb
Fincantieri NexTech
DEAS

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S1 – Security Operation Center; L1.S2 – Next Generation Firewall, L1.S3 – Web Application Firewall; L1.S9 – Formazione e Security Awareness; L1.S15 – Servizi Specialistici	**Fastweb**	**50%**

Tabella 11 - Modalità di ricorso al Subappalto da parte del Fornitore

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

5 DIMENSIONAMENTO ECONOMICO

5.1 Modalità di erogazione dei Servizi

Di seguito è riportato per ogni servizio le metriche di misura e le modalità di erogazione e consuntivazione.

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ TOTALE	VALORE ECONOMICO TOTALE
L1.S1	Device equivalenti /anno	Da remoto	Canone	Mensile	Fascia 5 – € 218,40	2.336	€ 525.600,00
L1.S2	Ngfw Throughput/anno	Da remoto	Canone	Mensile	Fascia 2 – € 1.129,86	124	€ 140.102,14
					Fascia 3 – € 6.475,84	40	€ 259.033,60
					Fascia 4 – € 10.705,50	8	€ 85.644,00
					Fascia 5 – € 46.035,00	16	€ 736.560,00
L1.S3	Throughput http/anno	Da remoto	Canone	Mensile	Fascia 1 – € 2.800,00	8	€ 22.400,00
L1.S9	GG/P – Team Ottimale	Da remoto/on site	Progettuale - A corpo	Mensile	€ 247,52	2.760	€ 683.155,20
L1.S15	GG/P – Team Ottimale	Da remoto/on site	Progettuale - A corpo	Mensile	€ 244,00	21.128	€ 5.155.232,00

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **€ 7.607.726,94 IVA esclusa.**

5.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

La fatturazione sarà eseguita in accordo con quanto previsto nello Schema di Contratto Esecutivo. Per quanto concerne i termini di pagamento si fa riferimento a quanto previsto nell'Accordo Quadro.

ASL RM/1
ALLEGATO 1
Prot. n. 173698/2024 del 04/11/2024
Firmato da: FRANCO TURCONI

6 ALLEGATI

6.1 Piano di Lavoro Generale

Per il piano di lavoro generale si rimanda all'allegato Piano di Lavoro Generale.

6.2 Piano di Presa in Carico

Come riportato nel Piano dei Fabbisogni, una prima pianificazione di queste attività, è riportato nell'allegato Piano di Presa in Carico. Il RTI si impegna a garantire l'esecuzione dei collaudi nelle modalità e con riferimento ai servizi per i quali è richiesto come sarà concordato con l'Amministrazione durante il periodo di Presa in Carico.

6.3 Piano della Qualità Specifico

Per il piano di qualità specifico si rimanda al documento denominato Piano della Qualità Specifico.

6.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Referente Tecnico di CE, il relativo nominativo sarà fornito per la stipula del CE ed il relativo CV sarà fornito entro 5 giorni dalla stipula.

6.5 Misure di Sicurezza poste in essere

Per le misure di sicurezza poste in essere si rimanda al Piano di Sicurezza del Centro Servizi.

6.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH)

Si allega la documentazione trasmessa a Consip tramite pec in data 11/11/2022, relativa al principio "Do No Significant Harm" (DNSH).