

|  |  |  |  |
| --- | --- | --- | --- |
| **Rev.** | **Data** | **Descrizione delle modifiche** | **Autore** |
| 00 | XX/XX/2022 | Prima emissione |  |
|  |  |  |  |
|  |  |  |  |

Tabella 1 – Registro delle versioni

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.

Sommario

[1 INTRODUZIONE 5](#_Toc114747637)

[1.1 Scopo 5](#_Toc114747638)

[1.2 Ambito di Applicabilità 5](#_Toc114747639)

[1.3 Assunzioni 8](#_Toc114747640)

[2 RIFERIMENTI 9](#_Toc114747641)

[2.1 Normativa di riferimento 9](#_Toc114747642)

[2.2 Documenti Applicabili 9](#_Toc114747643)

[3 DEFINIZIONI E ACRONIMI 10](#_Toc114747644)

[3.1 Acronimi 10](#_Toc114747645)

[4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO 12](#_Toc114747646)

[4.1 Attività in carico alle aziende del RTI 14](#_Toc114747647)

[4.2 Organizzazione e figure di riferimento del Fornitore 14](#_Toc114747648)

[4.3 Luogo di erogazione e di esecuzione della Fornitura 15](#_Toc114747649)

[5 AMBITI E SERVIZI 16](#_Toc114747650)

[5.1 Ambiti di intervento 16](#_Toc114747651)

[5.2 Servizi richiesti 16](#_Toc114747652)

[5.3 Indicatore di progresso 16](#_Toc114747653)

[6 SOLUZIONE PROPOSTA 18](#_Toc114747654)

[6.1 Descrizione dei servizi richiesti 18](#_Toc114747655)

[6.2 Utenza interessata / coinvolta 18](#_Toc114747656)

[6.3 Eventuali riferimenti / vincoli normativi 18](#_Toc114747657)

[7 PIANO DI PROGETTO 19](#_Toc114747658)

[7.1 Cronoprogramma 19](#_Toc114747659)

[7.2 Data di Attivazione e Durata del Servizio 19](#_Toc114747660)

[7.3 Gruppo di Lavoro 19](#_Toc114747661)

[7.4 Modalità di esecuzione dei Servizi 19](#_Toc114747662)

[7.5 Modalità di ricorso al Subappalto da parte del Fornitore 20](#_Toc114747663)

[8 DIMENSIONAMENTO ECONOMICO 22](#_Toc114747664)

[8.1 Modalità di erogazione dei Servizi 22](#_Toc114747665)

[8.2 Quadro economico di riferimento 22](#_Toc114747666)

[9 ALLEGATI 24](#_Toc114747667)

[9.1 Piano di Lavoro Generale 24](#_Toc114747668)

[9.2 Piano di Presa in Carico 24](#_Toc114747669)

[9.3 Piano della Qualità Specifico 24](#_Toc114747670)

[9.4 Curriculum Vitae dei Referenti 24](#_Toc114747671)

[9.5 Misure di Sicurezza poste in essere 24](#_Toc114747672)

[9.6 Indicazioni in ordine alla fatturazione ed ai termini di pagamento 24](#_Toc114747673)

Indice delle tabelle

[Tabella 1 – Emissione del documento 2](#_Toc114747674)

[Tabella 2 – Lista distribuzione 2](#_Toc114747675)

[Tabella 3 – Registro delle versioni 2](#_Toc114747676)

[Tabella 4 - Assunzioni 8](#_Toc114747677)

[Tabella 5 - Documenti Applicabili 9](#_Toc114747678)

[Tabella 6 - Definizioni 10](#_Toc114747679)

[Tabella 7 - Acronimi 11](#_Toc114747680)

[Tabella 8 - Ripartizione attività in carico 14](#_Toc114747681)

[Tabella 9 - Figure di riferimento e referenti del Fornitore 15](#_Toc114747682)

[Tabella 10 - Servizi richiesti 16](#_Toc114747683)

[Tabella 12 - Schema definizione Indicatore di Progresso 17](#_Toc114747684)

[Tabella 13 – Cronoprogramma 19](#_Toc114747685)

[Tabella 14 - Descrizione milestone per obiettivo 20](#_Toc114747686)

[Tabella 15 - Modalità di ricorso al Subappalto da parte del Fornitore 21](#_Toc114747687)

[Tabella 16 - Modalità di erogazione dei Servizi 22](#_Toc114747688)

[Tabella 17 - Quadro economico di riferimento 23](#_Toc114747689)

Indice delle figure

[Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST 6](#_Toc114747690)

[Figura 2 - Organizzazione dell'AQ proposta dal RTI 12](#_Toc114747691)

# INTRODUZIONE

*Inserire una breve descrizione dell’Amministrazione contraente e del suo compito istituzionale. Indicare qui sinteticamente la natura dei servizi e dell’intervento richiesto in termini di obiettivi e dei benefici attesi dall’Amministrazione che si vogliono perseguire.*

## Scopo

*Personalizzare in funzione agli obiettivi dell’Amministrazione.*

## 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.

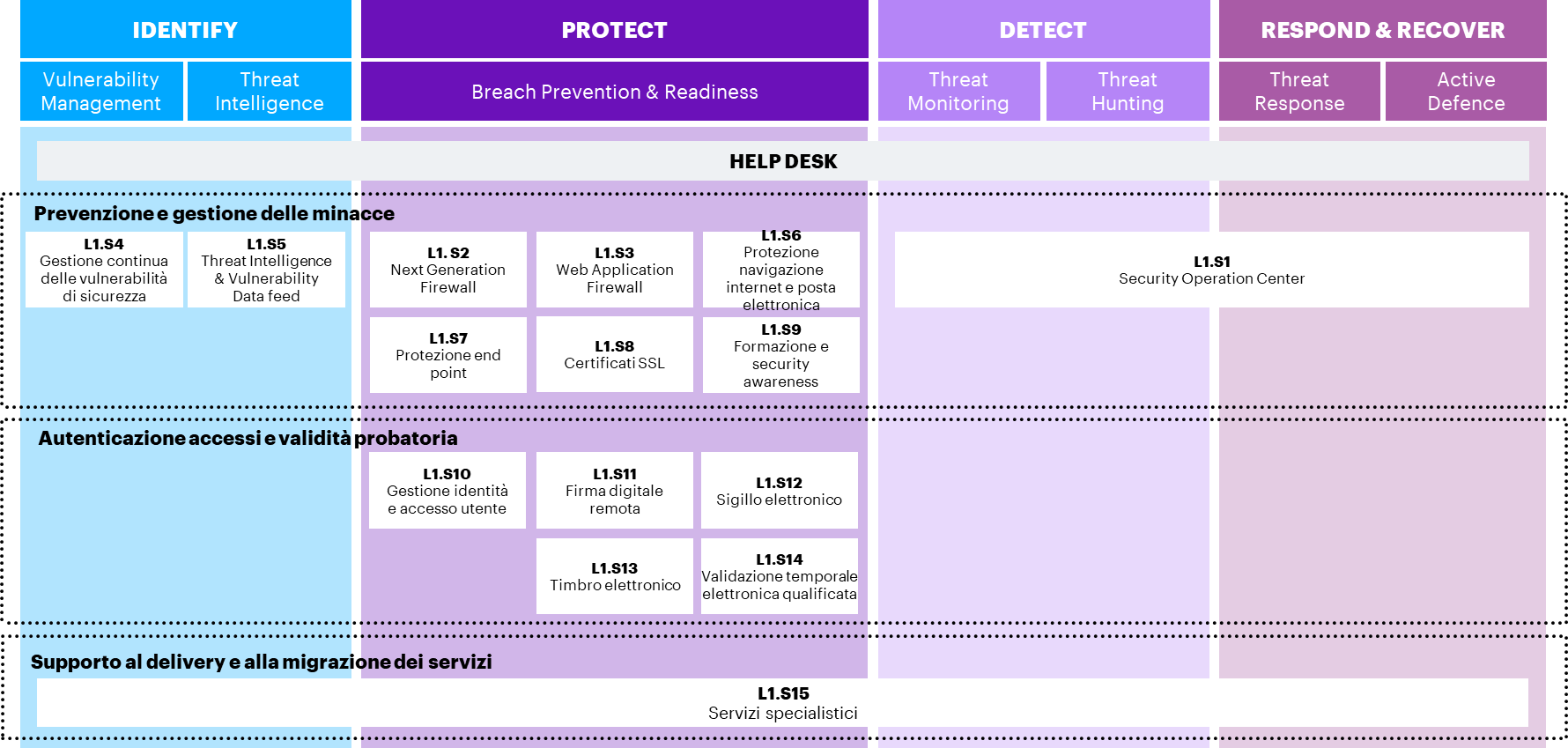


Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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.

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.

In riferimento a quanto sopra riportato, **NOME PA**, 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 di 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, **NOME PA**, 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.

## Assunzioni

*Indicare le assunzioni (N.A. se non ce ne sono).*

| **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 NOME PA e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale |

Tabella 4 - Assunzioni

# RIFERIMENTI

## Normativa di riferimento

Trovano applicazione le normative e gli standard internazionali riportate al “Capitolato Tecnico Generale” (§ 4.6) [DA-1].

## Documenti Applicabili

| **Rif.** | **Titolo** |
| --- | --- |
|  | 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. |
|  | ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO |
|  | Accordo Quadro |
|  | 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 |
|  | Appendice 1 al CTS Lotto 1\_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto |
|  | Piano dei Fabbisogni |
|  |  |
|  |  |

Tabella 5 - Documenti Applicabili

# DEFINIZIONI E ACRONIMI

## 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, interruzione, anche parziali |

Tabella 6 - 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](https://it.wikipedia.org/wiki/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 7 - Acronimi

# ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

*Descrivere l’organizzazione del Fornitore per l’erogazione dei servizi richiesti dall’Amministrazione nello specifico Piano dei Fabbisogni in risposta al quale si predispone il presente documento.*

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:

Graphical user interface

Description automatically generated

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 TecnicoCE 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:

* 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.

## 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** |  |  |  |  |
| **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 – Formazione e Security Awareness** |  |  |  |  |
| **L1.S10 – Gestione dell’Identità e dell’accesso dell’utente** |  |  |  |  |
| **L1.S12 – Sigillo Elettronico** |  |  |  |  |
| **L1.S13 – Timbro Elettronico** |  |  |  |  |
| **L1.S14 – Validazione temporale elettronica qualificata** |  |  |  |  |
| **L1.S15 – Servizi Specialistici** |  |  |  |  |
| **TOTALE (%)** |  |  |  |  |
| **TOTALE (€)** |  |  |  |  |

Tabella 8 - Ripartizione attività in carico

## 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 9 - Figure di riferimento e referenti del Fornitore

## Luogo di erogazione e di esecuzione della Fornitura

*Indicare il / i luogo/ghi di esecuzione della fornitura*

1. AMBITI E SERVIZI

## Ambiti di intervento

*Riportare, dettagliandoli, gli ambiti d’intervento oggetto di fornitura*

## Servizi richiesti

*Riportare in tabella i servizi richiesti e le relative quantità, con riferimento allo specifico Accordo Quadro nell’ambito del Lotto 1 della gara Servizi di Sicurezza da Remoto per le PAL che l’Amministrazione intende utilizzare. Motivare il dimensionamento.*

| **SERVIZIO** | | **FASCIA** | **IMPORTO I ANNO** | **IMPORTO II ANNO** | **IMPORTO III ANNO** | **IMPORTO IV ANNO** |
| --- | --- | --- | --- | --- | --- | --- |
| **L1.S1 – Security Operation Center** |  | |  |  |  |  |
| **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 – Formazione e Security Awareness** |  | |  |  |  |  |
| **L1.S10 – Gestione dell’Identità e dell’accesso dell’utente** |  | |  |  |  |  |
| **L1.S12 – Sigillo Elettronico** |  | |  |  |  |  |
| **L1.S13 – Timbro Elettronico** |  | |  |  |  |  |
| **L1.S14 – Validazione temporale elettronica qualificata** |  | |  |  |  |  |
| **L1.S15 – Servizi Specialistici** |  | |  |  |  |  |

Tabella 10 - Servizi richiesti

## Indicatore di progresso

Di seguito l’indicatore di progresso identificato in questa fase per l’erogazione della fornitura:

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

Graphical user interface, text, application, email

Description automatically generated

Tabella 12 - 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.

1. SOLUZIONE PROPOSTA

*Descrivere i servizi richiesti, nel caso in cui sia fattibile vista la struttura stessa del Progetto. Se si prospetta una soluzione unica, è possibile redigere un unico paragrafo.*

## Descrizione dei servizi richiesti

*Riportare qui la descrizione dei servizi richiesti con la contestualizzazione del caso all’ambito del cliente.*

## Utenza interessata / coinvolta

*Dettagliare le tipologie interne di utenti/stakeholder coinvolti nell’utilizzo della soluzione risultante dall’erogazione dei servizi.*

## Eventuali riferimenti / vincoli normativi

*Dettagliare i riferimenti e i vincoli normativi applicabili.*

1. PIANO DI PROGETTO

## Cronoprogramma

*Nei sotto-paragrafi di questa sezione è necessario delineare cronoprogramma, milestone, deliverables per ogni soluzione/fase.*

L’erogazione dei servizi avrà durata XX mesi, 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:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ANNO I | | | | | | | | | | | | | ANNO II | | | | | | | | | | | | | ANNO III | | | | | | | | | | | | | ANNO IV | | | | | | | | | | |
|  | M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 | M10 | M11 | M12 | M1 | | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 | M10 | M11 | M12 | M1 | | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 | M10 | M11 | M12 | M1 | | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 | M10 | M11 |
| ***Servizio 1*** |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |
| ***Servizio 2*** |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |
| ***Servizio …*** |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |
| ***Servizio n*** |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |

Tabella 13 – Cronoprogramma

## Data di Attivazione e Durata del Servizio

*Inserire la data di attivazione del Progetto indicata dall’Amministrazione e concordata oltre alla durata del Servizio. NOTA: Il contratto esecutivo avrà una durata massima di 48 mesi, decorrenti dalla data di conclusione dell’attività di presa in carico.*

*Inserire specifica relativa ai collaudi previsti*

## Gruppo di Lavoro

*Descrivere il gruppo o i gruppi di lavoro individuati per ciascun servizio richiesto. Qualora nel piano dei fabbisogni siano state indicate figure professionali, andranno esplicitati i nominativi delle persone ed allegato il relativo CV.*

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.

## Modalità di esecuzione dei Servizi

*Descrivere le modalità operative previste per lo svolgimento delle attività richieste.*

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 14 - 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.

## Modalità di ricorso al Subappalto da parte del Fornitore

*Elencare, per ogni azienda, le attività fra quelle oggetto del piano operativo, che l’azienda intende subappaltare e relativa quota massima per l’insieme di tali attività.*

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.S1 – Security Operation Center** |  |  |
| **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 – Formazione e Security Awareness** |  |  |
| **L1.S10 – Gestione dell’Identità e dell’accesso dell’utente** |  |  |
| **L1.S12 – Sigillo Elettronico** |  |  |
| **L1.S13 – Timbro Elettronico** |  |  |
| **L1.S14 – Validazione temporale elettronica qualificata** |  |  |
| **L1.S15 – Servizi Specialistici** |  |  |

Tabella 15 - Modalità di ricorso al Subappalto da parte del Fornitore

1. DIMENSIONAMENTO ECONOMICO

*Il Fornitore, per ciascun servizio richiesto, descriverà in questo paragrafo le modalità operative per l’attivazione dello stesso, ed in particolare fornirà le informazioni di seguito riportate.*

## Modalità di erogazione dei Servizi

*Descrivere per ogni attività prevista le metriche e le modalità di erogazione.*

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** | **VALORE**  **ECONOMICO** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L1.S1** |  |  |  |  |  |  |  |
| **L1.S2** |  |  |  |  |  |  |  |
| **L1.S3** |  |  |  |  |  |  |  |
| **L1.S4** |  |  |  |  |  |  |  |
| **L1.S5** |  |  |  |  |  |  |  |
| **L1.S6** |  |  |  |  |  |  |  |
| **L1.S7** |  |  |  |  |  |  |  |
| **L1.S8** |  |  |  |  |  |  |  |
| **L1.S9** |  |  |  |  |  |  |  |
| **L1.S10** |  |  |  |  |  |  |  |
| **L1.S12** |  |  |  |  |  |  |  |
| **L1.S13** |  |  |  |  |  |  |  |
| **L1.S14** |  |  |  |  |  |  |  |
| **L1.S15** |  |  |  |  |  |  |  |

Tabella 17 - Quadro economico di riferimento

L’importo complessivo dell’ordinativo di fornitura ammonta a **XXXXXXXXXXXXXXX €.**

## Indicazioni in ordine alla fatturazione ed ai termini di pagamento

eliminare quella N/A

**OPZIONE A** *“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”*

**OPZIONE B** nel caso abbiate concordato con il Cliente 60 gg in luogo dei 30 gg, la previsione sarà

*“La fatturazione sarà eseguita in accordo con quanto previsto nello Schema di Contratto Esecutivo. I termini di pagamento concordati sono 60 giorni.”*

1. ALLEGATI

## Piano di Lavoro Generale

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

## Piano di Presa in Carico

*Come riportato al paragrafo XX del Piano dei Fabbisogni, una prima pianificazione di queste attività, che tiene conto di quanto riportato nel già citato paragrafo XX è riportata nell’allegato Piano di Presa in Carico.*

## Piano della Qualità Specifico

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

## Curriculum Vitae dei Referenti

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

## Misure di Sicurezza poste in essere

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