***Conclusione di un Accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i, suddiviso in 2 Lotti e avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni***

*Lotto 2 – Pubbliche Amministrazioni Centrali*

*(inserire nome Amministrazione)*

*(inserire Titolo Piano dei Fabbisogni)*

**Piano dei Fabbisogni**

ID Sigef: 2296

*Indice*

[1. INTRODUZIONE 3](#_Toc98781142)

[1.1. Premessa 3](#_Toc98781143)

[1.2. Scopo del documento 4](#_Toc98781144)

[1.3. Campo di applicazione 4](#_Toc98781145)

[1.4. Acronimi 4](#_Toc98781146)

[1.5. Definizioni 4](#_Toc98781147)

[2. ANAGRAFICA DELL’AMMINISTRAZIONE 5](#_Toc98781148)

[3. DESCRIZIONE DELL’INTERVENTO 6](#_Toc98781149)

[3.1. Scopo e obiettivi dell’intervento 6](#_Toc98781153)

[3.2. Benefici attesi 6](#_Toc98781154)

[3.3. Categorizzazione dell’intervento 6](#_Toc98781155)

[3.4. Organizzazione e figure di riferimento dell’Amministrazione 7](#_Toc98781156)

[3.5. Organizzazione e figure di riferimento del fornitore 7](#_Toc98781157)

[4. SERVIZI OGGETTO DI FORNITURA 8](#_Toc98781158)

[4.1. Dimensionamento dei servizi richiesti 8](#_Toc98781160)

[4.2. Pianificazione dei servizi 8](#_Toc98781161)

[4.3. Sintesi dei servizi richiesti 9](#_Toc98781162)

[4.4. Importo e durata del contratto 10](#_Toc98781163)

[4.5. Modalità di consuntivazione dei servizi 11](#_Toc98781164)

[4.6. Luogo di esecuzione dei servizi 11](#_Toc98781165)

[4.7. Indicazione della quota e della prestazione da subappaltare 12](#_Toc98781166)

[5. INDICATORI DI DIGITALIZZAZIONE E PROGRESSO 12](#_Toc98781167)

[5.1. Indicatori di digitalizzazione 12](#_Toc98781173)

[5.2. Indicatore di progresso 12](#_Toc98781174)

1. INTRODUZIONE
   1. Premessa

La minaccia cibernetica cresce continuamente in quantità e qualità ed i servizi informatici e telematici erogati dalla Pubblica Amministrazione diventano sempre più cruciali per il funzionamento del *sistema Paese*. Difatti, secondo quanto emerge dal “*Rapporto Clusit 2022 sulla sicurezza ICT*”, il cui obiettivo è quello di *diffondere la cultura della sicurezza informatica* presso la PA, le aziende ed i cittadini e *promuovere l’uso di metodologie e tecnologie* in grado di migliorarne il livello di sicurezza, il *numero dei cyber attacchi* nel 2021 è aumentato del 10% rispetto all’anno precedente ed emerge un trend positivo di crescita sia in termini di quantità che di qualità. Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata.

In particolare, il Rapporto ha evidenziato come nel 2021 il 79% degli attacchi rilevati abbia avuto un impatto “*elevato*”, contro il 50% dello scorso anno. Più in dettaglio, il 32% è stato caratterizzato da una severity “*critica*” e il 47% “*alta*”, mentre sono diminuiti gli attacchi di impatto “*medio*” (-13%) e “*basso*” (-17%).

Sono state inoltre rilevate “*modifiche comportamentali*” nelle modalità di azione dei cyber criminali: non colpiscono più in maniera indifferenziata obiettivi molteplici, ma mirano a bersagli *ben precisi*. Al primo posto troviamo l’obiettivo *governativo/militare* (15% degli attacchi totali) con una crescita del 36,4% rispetto all’anno precedente. Al secondo posto troviamo il *settore informatico* (14% dei casi, +3,3% rispetto al 2020) e, a seguire, la sanità e gli obiettivi multipli che, insieme, costituiscono il 13% del totale degli obiettivi colpiti (rispettivamente +24,8% e -8% rispetto al 2020).

Il panorama italiano è parte integrante di questo trend “negativo” di crescita: a livello nazionale i settori più colpiti risultano essere quelli della *Pubblica Amministrazione* e del *Finance/Insurance*.

In questo perimetro si innesta l’iniziativa per la stipula di un Accordo Quadro avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (d’ora in avanti, ***AQ Cybersecurity***), anche con il duplice scopo 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;
* 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.

Più in dettaglio, essa si articola in due Lotti, di cui si riporta di seguito una breve descrizione:

* ***Lotto 1:*** il *Lotto di servizi di Sicurezza da remoto* 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;
* ***Lotto 2:*** il *Lotto di servizi di Compliance e controllo* 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 nonchè sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

*Il presente Piano dei Fabbisogni è rivolto alle Pubbliche Amministrazioni Centrali che intendono usufruire dei servizi offerti nell’ambito del Lotto 2 dell’AQ Cybersecurity.*

* 1. Scopo del documento

Il presente documento ha lo scopo di illustrare e definire l’intervento e gli obiettivi che l’Amministrazione, nell’ambito del presente Accordo Quadro, si prefigge di raggiungere, delineando inoltre le caratteristiche quali-quantitative dei servizi richiesti e le modalità operative da prevedere per la loro erogazione.

* 1. Campo di applicazione

Questo documento è rivolto alle *Pubbliche Amministrazioni Centrali* che intendono usufruire dei servizi offerti nell’ambito del Lotto 2 dell’Accordo Quadro avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni.

* 1. Acronimi

|  |  |
| --- | --- |
| Acronimo | Descrizione |
| *Consip* | Consip S.p.a. |
| *AQ* | Accordo Quadro |
| *RTI* | Raggruppamento Temporaneo d’Impresa |
| *AgID* | Agenzia per l’Italia Digitale |
| *PA* | Pubblica Amministrazione |
| *PAC* | Pubblica Amministrazione Centrale |
| *CE* | Contratto Esecutivo |
| *PNC* | Piano Nazionale Complementare |
| *ABSC* | Agid Basic Security Control |

* 1. Definizioni

|  |  |
| --- | --- |
| Oggetto | Definizione |
| Accordo Quadro/AQ | L’Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A., per ciascun Lotto, all’esito della procedura di gara di prima fase. |
| Aggiudicatario/Fornitore | Se non diversamente indicato va inteso ciascuno degli aggiudicatari, per ciascuno dei Lotti della fornitura. |
| 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 | Il documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa |
| Capitolato Tecnico Speciale | Il Capitolato Tecnico che integra il Capitolato Tecnico Generale e relativo al Lotto avente ad oggetto i servizi di compliance e controllo del presente AQ (Lotto 2). |
| Contratto Esecutivo | Il Contratto stipulato tra Amministrazione Contraente e Fornitore ed avente ad oggetto i servizi professionali di compliance e controllo del presente AQ (Lotto 2). |
| Piano dei fabbisogni | Il documento inviato dall’Amministrazione al Fornitore al quale la medesima affida il singolo Contratto Esecutivo. |
| Piano Operativo | Il documento, inviato dal Fornitore all’Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall’Amministrazione. |

1. ANAGRAFICA DELL’AMMINISTRAZIONE

|  |  |
| --- | --- |
| Dati anagrafici dell’Amministrazione | |
| *Ragione Sociale* |  |
| *Indirizzo* |  |
| *CAP* |  |
| *Comune* |  |
| *Provincia* |  |
| *Regione* |  |
| *Codice Fiscale* |  |
| *Indirizzo Mail* |  |
| *PEC* |  |
| *Codice PA* |  |
| *Comparto di appartenenza* | PAC |

|  |  |
| --- | --- |
| Dati anagrafici del referente dell’Amministrazione | |
| *Nome* |  |
| *Cognome* |  |
| *Telefono* |  |
| *Indirizzo Mail* |  |

1. DESCRIZIONE DELL’INTERVENTO

*Inserire una breve descrizione dell’Amministrazione contraente e del suo compito istituzionale. Indicare brevemente una descrizione dell’intervento che l’Amministrazione intende mettere in campo nell’ambito del Lotto 2 dell’AQ Cybersecurity.*

3. 1. Scopo e obiettivi dell’intervento

*Dettagliare, per quanto possibile, l’intervento richiesto dall’Amministrazione in termini di scopo e obiettivi che si vogliono raggiungere. Si consiglia di descrivere e declinare opportunamente le attività richieste, anche in funzione dei servizi offerti nell’ambito dell’Accordo Quadro.*

* 1. Benefici attesi

*Delineare i benefici attesi che l’intervento richiesto si prefigge di raggiungere.*

* 1. Categorizzazione dell’intervento

*Specificare la categorizzazione dell’intervento secondo quanto previsto all’interno del Capitolato Tecnico Generale della gara: in particolare, vanno individuati e censiti l’ambito del Piano Triennale AgID di riferimento per la specifica acquisizione, definendo dove possibile:*

* *L’ambito di primo livello;*
* *Uno o più ambiti di II livello, indicando come primo il prevalente.*

*Utilizzare la seguente tabella.*

|  |  |
| --- | --- |
| **Ambito (layer)** | **Obiettivi PT** |
| Servizi | * Servizi al cittadino * Servizi a imprese e professionisti * Servizi interni alla propria PA * Servizi verso altre PA |
|
| Dati | * Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese * Aumentare la qualità dei dati e dei metadati * Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati |
|
| Piattaforme | * Favorire l’evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l’azione amministrativa * Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA * Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini |
|
| Infrastrutture | * Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l’aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio) * Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l’aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud) * Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA |
|
| Interoperabilità | * Favorire l’applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API * Adottare API conformi al Modello di Interoperabilità |
|
| Sicurezza Informatica | * Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA * Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione |

* 1. Organizzazione e figure di riferimento dell’Amministrazione

*Indicare le persone incaricate dall’Amministrazione per la conduzione del progetto e i relativi ruoli/responsabilità.*

|  |  |
| --- | --- |
| Nome e Cognome | Ruolo/responsabilità |
|  |  |
|  |  |

* 1. Organizzazione e figure di riferimento del fornitore

*Indicare le persone incaricate dal Fornitore per la conduzione del progetto e i relativi ruoli/responsabilità.*

|  |  |
| --- | --- |
| Nome e Cognome | Ruolo/responsabilità |
|  |  |
|  |  |

1. SERVIZI OGGETTO DI FORNITURA

In questo paragrafo vengono esplicitati i servizi richiesti nell’ambito del Lotto 2 dell’Accordo Quadro Cybersecurity, in considerazione delle esigenze e degli obiettivi espressi dall’Amministrazione.

A puro scopo informativo, si propone di seguito una breve descrizione dei servizi richiesti, a partire da quanto indicato nel Capitolato Generale del presente Accordo Quadro. Si rimanda alla consultazione del Capitolato Tecnico Speciale Lotto 2 per una descrizione dettagliata dei servizi elencati.

*Eliminare i servizi non di interesse del Piano dei Fabbisogni dell’Amministrazione.*

|  |  |
| --- | --- |
| Codice e Nome del Servizio | Descrizione |
| L2.S16 – Security strategy | Individuazione delle linee strategiche in ambito sicurezza ICT. |
| L2.S17 – Vulnerability Assessment | Identificazione dello stato di esposizione dei servizi erogati, delle applicazioni, dell’architettura e delle componenti tecnologiche della PA. |
| L2.S18 – Testing del codice – Statico | Identificazione delle vulnerabilità software all’interno del codice delle applicazioni nella fase iniziale del ciclo di vita. |
| L2.S19 – Testing del codice – Dinamico | Identificazione delle vulnerabilità all’interno delle applicazioni Web e analisi dell’esposizione al rischio di attacchi informatici ai sistemi informativi. |
| L2.S20 – Testing del codice – Mobile | Esecuzione test per le applicazioni di tipo mobile per la rilevazione delle vulnerabilità di sicurezza. |
| L2.S21 – Supporto all’analisi e gestione degli incidenti | Supporto allo svolgimento delle attività di analisi degli incidenti e di divulgazione delle informazioni in caso di emergenza. |
| L2.S22 – Penetration Testing | Analisi e valutazione dei punti deboli relativi all’infrastruttura IT. |
| L2.S23 – Compliance normativa | Supporto nell’attuazione degli adempimenti del GDPR applicato in ambito IT. |

1. 1. Dimensionamento dei servizi richiesti

*Per ognuno dei servizi richiesti dall’Amministrazione, indicare gli elementi qualitativi utili al dimensionamento dei servizi richiesti (e.g., numero delle applicazioni da sottoporre a test statici/dinamici, etc.). Indicare inoltre le caratteristiche specifiche, ove possibile, dei servizi richiesti (quali attività si prevede di svolgere tra quelle elencate nel Capitolato Tecnico Speciale Lotto 2 si richiedono, e.g., il servizio di Penetration Testing può essere eseguito nelle modalità “White Box”, “Black Box” o “Grey Box” sulla base della scelta dell’Amministrazione, etc.).*

* 1. Pianificazione dei servizi

*Indicazione dei tempi di attivazione dei servizi e rispettiva durata. Esplicitazione eventuale delle principali milestone attese dall’Amministrazione. Eliminare i servizi che non rientrano nel perimetro di azione del presente obiettivo e modificare l’orario di erogazione in base alle richieste dell’Amministrazione. Gli orari ed i giorni indicati sono quelli riportati da Capitolato Tecnico Speciale Lotto 2.*

Nella tabella che segue, per ognuno dei servizi richiesti dall’Amministrazione, si indica la data di attivazione, la durata e l’orario di erogazione degli stessi. Si specifica che la stima della data di avvio dei servizi potrà essere soggetta a revisione in sede di avanzamento del processo di attivazione della fornitura e in seguito alla stipula del Contratto Esecutivo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Codice | Nome del Servizio | Data attivazione del servizio | Durata del servizio | Orario di erogazione |
| L2.S16 | Security strategy |  |  | Lun – Ven:  08:30 – 17:30);  Sab:  08:30 – 14:00 |
| L2.S17 | Vulnerability Assessment |  |  | Lun – Ven:  08:30 – 17:30);  Sab:  08:30 – 14:00 |
| L2.S18 | Testing del codice – Statico |  |  |  |
| L2.S19 | Testing del codice – Dinamico |  |  |  |
| L2.S20 | Testing del codice – Mobile |  |  |  |
| L2.S21 | Supporto all’analisi e gestione degli incidenti |  |  | Lun – Ven:  08:30 – 17:30);  Sab:  08:30 – 14:00 |
| L2.S22 | Penetration Testing |  |  | Lun – Ven:  08:30 – 17:30);  Sab:  08:30 – 14:00 |
| L2.S23 | Compliance normativa |  |  | Lun – Ven:  08:30 – 17:30);  Sab:  08:30 – 14:00 |

* 1. Sintesi dei servizi richiesti

*Riportare in tabella i servizi richiesti e le relative quantità che l’Amministrazione intende utilizzare, indicandone approssimativamente la data di attivazione di ciascun servizio offerto.*

Nella tabella che segue sono indicate le quantità, la metrica di misurazione (come indicata all’interno del Capitolato Tecnico Speciale Lotto 2) e la tariffa per ognuno dei servizi richiesti dall’Amministrazione contraente.

Si precisa che le stime, *relativamente alla sola quantità*, possono essere soggette a revisione in sede di avanzamento del processo di attivazione della fornitura e in seguito alla stipula del Contratto Esecutivo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Codice | Nome del Servizio | Quantità | Metrica di misurazione | Tariffa |
| L2.S16 | Security strategy |  | Giorni/persona | 260,00 €/GP |
| L2.S17 | Vulnerability Assessment |  | Giorni/persona | 235,00 €/GP |
| L2.S18 | Testing del codice – Statico |  | * Numero di applicazioni (se eseguito one time) * Numero di applicazioni/anno (scansioni periodiche) | * 864,50 €/GP per singola esecuzione; * 796,75 €/GP per >50 applicazioni |
| L2.S19 | Testing del codice – Dinamico |  | Numero di Applicazioni per profilo (Bronze, Silver e Gold)/anno | * Gold: da 2.593,50 € / GP fino a 15 applicazioni a 1.478,29 € / GP per >50 applicazioni * Silver: da 1.395,83 € /GP fino a 15 applicazioni a 998,40 € / GP per >50 applicazioni * Bronze: 564,20 € / GP fino a 15 applicazioni a 432,25 € / GP per >50 applicazioni |
| L2.S20 | Testing del codice – Mobile |  | Numero di applicazioni/anno | * 1.797,32 €/GP fino a 15 applicazioni; * 1.490,30 €/GP per >50 applicazioni |
| L2.S21 | Supporto all’analisi e gestione degli incidenti |  | Giorni/persona | 210,00 €/GP |
| L2.S22 | Penetration Testing |  | Giorni/persona | 256,20 €/GP |
| L2.S23 | Compliance normativa |  | Giorni/persona | 200,00 €/GP |

*Per ognuno dei servizi richiesti che richiedano particolare documentazione di contesto/tecnologica, quali ad esempio, L2.S17 – Vulnerability Assessment, questa deve essere esplicitata nel presente Piano dei Fabbisogni (i.e., per il servizio di cui sopra, strumenti utilizzati dal Fornitore per l’espletamento del servizio e che siano compatibili con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport).*

* 1. Importo e durata del contratto

*Sulla base dei servizi richiesti e della loro pianificazione, indicare in quanto segue l’importo contrattuale da attivare e la durata del contratto. Come indicato da Capitolato Generale, va inoltre specificato se il contratto esecutivo scaturente dal presente Piano dei Fabbisogni è finanziato, in tutto o in parte, con le seguenti risorse:*

* *Risorse previste dal Regolamento UE 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021;*
* *Risorse previste dal Regolamento UE 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021;*
* *Risorse previste dal PNC;*
* *Utilizzo di fondi economici ai sensi del D.L. 77/2021.*

Sulla base di quanto stabilito nei paragrafi precedenti, il presente Piano dei Fabbisogni stabilisce quanto segue:

* importo del contratto esecutivo pari a € XXX.XXX,XX, così suddiviso:
  + € XXX.XXX,XX per i servizi con metrica di misurazione Giorni/persona e per un totale di XXX GG/P previsti;
  + € XXX.XXX,XX per i servizi con metrica di misurazione Numero di applicazioni/anno e Numero di applicazioni per profilo/anno.

*Eliminare questa sezione sui fondi se non necessaria. Se necessaria, indicare i soli fondi utilizzati e la loro percentuale di utilizzo.*

Si prevede inoltre di finanziare il Contratto Esecutivo scaturente dal presente Piano dei Fabbisogni e dal Piano Operativo redatto dal RTI con le seguenti risorse:

|  |  |
| --- | --- |
| Fondi o risorse utilizzate | % sul totale del CE |
| Risorse previste dal Regolamento UE 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 |  |
| Risorse previste dal Regolamento UE 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 |  |
| Risorse previste dal PNC |  |
| Fondi economici ai sensi del D.L. 77/2021 |  |

Infine, il Contratto Esecutivo scaturente dal Piano dei Fabbisogni e dal Piano Operativo avrà durata pari a XXX settimane a decorrere dalla data del XX/XX/XXXX. Si precisa che la data di avvio dei servizi è subordinata al perfezionamento del Contratto Esecutivo.

* 1. Modalità di consuntivazione dei servizi

*Eliminare dalla tabella che segue i servizi non richiesti dall’Amministrazione nell’ambito della presente fornitura.*

Nella tabella che segue, per ognuno dei servizi richiesti, si indicano le modalità di consuntivazione previste nel Capitolato Tecnico Speciale Lotto 2.

|  |  |  |
| --- | --- | --- |
| Codice | Nome del Servizio | Modalità di consuntivazione |
| L2.S16 | Security strategy | Progettuale (a corpo) |
| L2.S17 | Vulnerability Assessment | Progettuale (a corpo) |
| L2.S18 | Testing del codice – Statico | Singola esecuzione (one time);  oppure, Canone annuale (scansioni periodiche) |
| L2.S19 | Testing del codice – Dinamico | Canone annuale |
| L2.S20 | Testing del codice – Mobile | Canone annuale |
| L2.S21 | Supporto all’analisi e gestione degli incidenti | Progettuale (a corpo) |
| L2.S22 | Penetration Testing | Progettuale (a corpo) |
| L2.S23 | Compliance normativa | Progettuale (a corpo) |

Come indicato nel documento di gara di cui sopra, sarà cura del Fornitore predisporre mensilmente, nell’ambito del documento relativo allo Stato di Avanzamento Lavori, la consuntivazione delle attività previste per ognuno dei servizi elencati nella tabella precedente, evidenziando le fasi chiuse e riportando gli eventuali scostamenti rispetto alla pianificazione concordata tra le Parti contraenti.

* 1. Luogo di esecuzione dei servizi

*Indicare il luogo di esecuzione dei servizi richiesti dall’Amministrazione, previo accordo con la stessa. Come stabilisce il Capitolato Tecnico Speciale Lotto 2, le prestazioni contrattuali saranno di tipo on-site, i.e., svolte primariamente presso le sedi dell’Amministrazione; in alternativa, presso la sede del Fornitore.*

* 1. Indicazione della quota e della prestazione da subappaltare

Laddove il Fornitore si fosse riservato la possibilità di ricorrere al subappalto si fa richiesta di indicare nel Piano Operativo, per ogni servizio attivato, la quota ed il tipo di prestazione che sarà ceduta in subappalto.

1. INDICATORI DI DIGITALIZZAZIONE E PROGRESSO

Nell’ambito delle attività di governance ed in particolare della valutazione del livello di efficacia degli interventi operati dalle Amministrazioni attraverso l’utilizzo di contratti esecutivi afferenti alle Gare Strategiche in ambito Sicurezza ICT, si intendono definite due tipologie di indicatori:

* *Indicatori Generali*, che mappano il macro-obiettivo dell’intervento rispetto ai principali obiettivi strategici del Piano Triennale;
* *Indicatori Specifici*, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti. In tale contesto, è definito un indicatore (cd. “indicatore di progresso” in seguito descritto) che indica il livello di maturità della infrastruttura di sicurezza ICT delle Amministrazioni, sulla base del grado di mappatura degli interventi effettuati con le misure minime di sicurezza AGID (Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»).

5. 1. Indicatori di digitalizzazione

*Sulla base di quanto stabilito nelle Gare Strategiche ICT, vanno scelti dalla tabella a pag. 16 del Capitolato Tecnico Generale almeno 3 indicatori suddivisi per i seguenti cluster: indicatori quantitativi, indicatori quantitativi e indicatori di collaborazione e riuso, quantificando, per ognuno di essi il valore ex ante ed ex post.*

|  |  |  |  |
| --- | --- | --- | --- |
| Indicatore | Tipologia | Valore ex ante | Valore ex post |
|  | Quantitativo |  |  |
|  | Qualitativo |  |  |
|  | Collaborazione e riuso |  |  |

* 1. Indicatore di progresso

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 l’acquisto dei servizi previsti nel Lotto 2 del presente Accordo Quadro, che sarà determinato come da schema seguente:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicatore | 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 = (N1 – N0)/NT | | |
| Regole di arrotondamento | Nessuna | | |
| Valore soglia | N0: numero di controlli relativi alla specifica classe soddisfatti prima dell’intervento | | |
| Applicazione | Amministrazione Contraente | | |