

GARA A PROCEDURA APERTA AI SENSI DEL D.LGS. 36/2013 E S.M.I, PER L’AFFIDAMENTO DI UN ACCORDO QUADRO PER I SERVIZI DI CONNETTIVITÀ DELLA RETE INTERNAZIONALE DELLA PUBBLICA AMMINISTRAZIONE (S-RIPA) – LOTTO UNICO – ID 2834

RISPOSTE ALLE RICHIESTE DI CHIARIMENTI (I TRANCHE)

I chiarimenti della gara sono visibili sui siti: www.consip.it, e www.acquistinretepa.it.

1) DOMANDA

Con riferimento alla gara ID 2834, e in particolare all’Allegato 3 al Capitolato Tecnico – “Richiesta informazioni e impegno di riservatezza”, considerato che l’Allegato 3 prevede che “in caso di RTI, la presente richiesta dovrà essere necessariamente presentata congiuntamente da tutte le imprese in promessa di RTI”, considerato altresì che entro il termine per la presentazione della suddetta richiesta (13 marzo p.v.) alcuni operatori economici potrebbero non aver ancora definito se parteciperanno in forma singola o in raggruppamento temporaneo di imprese, si chiede di confermare che qualora dopo tale termine l’operatore economico, che ha presentato tempestivamente la dichiarazione, dovesse decidere di partecipare in costituendo RTI, possa lo stesso condividere con i partner le informazioni ricevute da Consip acquisendo analogo impegno alla riservatezza oppure se sia anche necessario inviare a Consip l’allegato 3 debitamente firmato da parte degli altri membri del costituendo RTI prima del termine per la presentazione delle offerte (23 aprile 2026).

Risposta

Si conferma quanto riportato nell’Allegato 3 al Capitolato Tecnico “(in caso di RTI, la presente richiesta dovrà essere necessariamente presentata congiuntamente da tutte le imprese in promessa di RTI)”. Si conferma anche che, come indicato nel Capitolato d’Oneri al paragrafo 12 “È facoltà di Consip riscontrare richieste pervenute oltre tale termine; in tale ipotesi non potrà essere eccepita la mancata contemporaneità dell’invio a tutti i Soggetti titolati.”

2) DOMANDA

DOCUMENTO1: Capitolato d’oneri, Par. 17.1, Pag. 54, Criterio ID 38

TESTO1: “Premialità per la tutela della sicurezza nazionale - Messa a disposizione, ai sensi dell’articolo 4, primo periodo, del DPCM del 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025, di tecnologie di cybersicurezza italiane, o di Paesi appartenenti all’Unione europea, o di Paesi aderenti all’Alleanza atlantica (NATO), o di Paesi terzi di cui all’Allegato 3 del citato DPCM e specificatamente, rispetto all’Allegato 2 del DPCM:

- i. software di VPN di cui alla categoria 3 per la realizzazione del servizio di connettività Best Effort;
- ii. piattaforma software SIEM di cui alla categoria 5;
- iii. firewall di cui alla categoria 11;
- iv. servizio di installazione, configurazione e manutenzione dei prodotti sopra elencati di cui alla categoria 18;
- v. servizio gestito dei prodotti i), ii) e iii), servizio di gestione degli incidenti di sicurezza, servizio professionale di supporto sistemistico e/o operativo in ambito sicurezza di cui alla categoria 20...”

DOCUMENTO2: DPCM 30 Aprile 2025, Allegato 2, Categoria 18

TESTO2: “Categoria 18: Servizi di consulenza, sviluppo e manutenzione di piattaforme software afferenti alle categorie 1, 2, 3, 4, 5, 6, 11, 15, 16 e 17”

DOMANDA 1.1: con riferimento al punto elenco iv. del TESTO 1 sopra riportato e in considerazione del fatto che la categoria 18 è riferita a piattaforme software, (vedi TESTO 2), si chiede di confermare che le attività di “installazione”, “configurazione” e “manutenzione” (in questo specifico ambito della BOM) devono intendersi riconducibili alle sole componenti software.

DOMANDA 1.2: con riferimento ai punti elenco iv. e v. del TESTO 1 sopra riportato e in considerazione del fatto che i servizi potrebbero essere oggetto di subappalto, con subappaltatori definiti in fase di autorizzazione da parte delle Amministrazioni Contraenti, si chiede di confermare che nella BOM nulla dovrà essere riportato con riferimento ai subappaltatori e che pertanto per i servizi ai punti elenco iv. e v. il campo provider della BOM possa essere popolato solo con la ragione sociale del concorrente.

Nel caso non si confermi, si chiede di precisare la corretta modalità di compilazione della BOM nel caso debba essere recepito il riferimento a Subappaltatori.

Risposta

In merito alla domanda 1.1, si conferma.

In merito alla domanda 1.2, si conferma. Resta fermo che il luogo indicato nella BOM, in cui risiede l'infrastruttura attraverso la quale viene erogato il servizio, dovrà essere comunque garantito in fase di esecuzione.

3) DOMANDA

DOCUMENTO1: Capitolato d'oneri, Par. 17.1, Pag. 54, Criterio ID 38

TESTO1: “Premialità per la tutela della sicurezza nazionale - Messa a disposizione, ai sensi dell'articolo 4, primo periodo, del DPCM del 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025, di tecnologie di cybersicurezza italiane, o di Paesi appartenenti all'Unione europea, o di Paesi aderenti all'Alleanza atlantica (NATO), o di Paesi terzi di cui all'Allegato 3 del citato DPCM e specificatamente, rispetto all'Allegato 2 del DPCM:

- 1) software di VPN di cui alla categoria 3 per la realizzazione del servizio di connettività Best Effort;
- 2) piattaforma software SIEM di cui alla categoria 5;
- 3) firewall di cui alla categoria 11;
- 4) servizio di installazione, configurazione e manutenzione dei prodotti sopra elencati di cui alla categoria 18;
- 5) servizio gestito dei prodotti i), ii) e iii), servizio di gestione degli incidenti di sicurezza, servizio professionale di supporto sistemistico e/o operativo in ambito sicurezza di cui alla categoria 20...”

DOCUMENTO2: Linee guida per l'applicazione dei criteri di premialità di cui all'articolo 14 della legge n. 90/2024, Appendice Tecnica BOM, Par. 2.1, pag 22.

TESTO2: “bom.services[].version”

DOMANDA: Poiché il version risulta essere un campo minimo obbligatorio della BOM e poiché i servizi ai punti elenco iv. e v. del TESTO1 sopra riportato, non hanno una versione, si chiede di confermare che tale campo possa essere valorizzato con il valore “1”

Nel caso non si confermi, si chiede di precisare la corretta modalità di compilazione del campo indicato.

Risposta

Si conferma.

4) DOMANDA

DOCUMENTO: All.6-Modello di offerta tecnica_v1.0

Domanda: Si fa presente che, per tutte le sedi per le quali la “colonna U” è valorizzata con “RU migliorativo”, la colonna AJ non consente di selezionare la tecnologia trasmissiva in quanto propone un menù a tendina con i soli valori SI e NO. Si chiede di rettificare il modello in questione.

Risposta

Si invita sul punto a prendere visione della relativa Errata corrige.

5) DOMANDA

DOCUMENTO: Capitolato tecnico, Par. 10.2.4, Pag. 95, Tabella 17 - SLA e Penali Progetto dei Fabbisogni, Reportistica, Collaudo

TESTO: vedi dettaglio sotto riportato relativo alla tabella 17:

SLA_FR1: Tempo di consegna del progetto dei fabbisogni (primo Progetto, o aggiornamento a seguito di variazione/aggiornamento del Piano dei Fabbisogni) SLA Target: entro 45 giorni lavorativi o migliorativo laddove offerto

SLA_FR2 Tempo di consegna del progetto dei fabbisogni modificato (Progetto dei Fabbisogni che recepisce le modifiche richieste dall'Amministrazione) SLA Target: entro 15 giorni lavorativi o migliorativo laddove offerto

DOMANDA: con riferimento a quanto scritto nella definizione di parametro SLA_FR1, si chiede di confermare che il *Tempo di consegna del progetto dei fabbisogni* è relativo solo al primo progetto e che il resto della frase “...o aggiornamento a seguito di variazione/aggiornamento del Piano dei Fabbisogni” è un refuso in quanto oggetto dello SLA_FR2.

Risposta

Non si conferma. Lo SLA_FR1 è relativo al caso del primo Progetto e al caso in cui l'Amministrazione invii il Piano dei Fabbisogni e successivamente invii una variazione/aggiornamento dello stesso nelle seguenti casistiche:

1. prima che il Fornitore abbia emesso il Progetto dei Fabbisogni
2. a seguito dell'invio da parte dell'Amministrazione dell'Ordinativo di Fornitura quindi a seguito dell'accettazione del Progetto dei Fabbisogni.

Lo SLA_FR2 è, invece, relativo al caso in cui il Fornitore abbia emesso il Progetto dei Fabbisogni e l'Amministrazione, nel rispetto del Piano dei Fabbisogni, chiede una modifica e/o integrazione del Progetto.

6) DOMANDA

DOCUMENTO: Capitolato tecnico, Par. 7.2.1, Pag. 58

TESTO: [R.185] Il sistema di fatturazione deve fornire tutte le informazioni di dettaglio in merito alle sessioni tariffate, nel rispetto delle norme della privacy in vigore.

DOMANDA: si chiede di confermare che il requisito [R.185] è un refuso poiché la presente gara non prevede servizi, quali ad esempio il VoIP, che giustificerebbe la richiesta; diversamente si chiede di specificare a cosa si fa riferimento con la frase “sessioni tariffate” da rendicontare nel rispetto delle norme sulla privacy.

CLASSIFICAZIONE CONSIP: CONSIP PUBLIC

Risposta

Si conferma che il sistema di fatturazione deve fornire tutte le informazioni di dettaglio in merito all'erogazione e fruizione dei servizi nel rispetto delle norme della privacy in vigore senza alcun riferimento alle "sessioni tariffate" in quanto non previste.

7) DOMANDA

Con riferimento al criterio n. 38 a pagina 54 laddove si evidenzia che:

"il coefficiente sarà pari a uno (1) quando la BOM (tutte le BOM qualora siano più di una) dei prodotti/servizi offerti e appartenenti **alle categorie sopra censite** rientri/ino"

posto che Tra le categorie "sopra censite" (sempre nel criterio 38) sono riportate:

iv. servizio di installazione, configurazione e manutenzione dei prodotti sopra elencati di cui alla categoria 18;

v. servizio gestito dei prodotti i), ii) e iii), servizio di gestione degli incidenti di sicurezza, servizio professionale di supporto sistemistico e/o operativo in ambito sicurezza di cui alla categoria 20"

Si chiede di chiarire come compilare le BOM (in formato CycloneDX versione 1.6.) per le sopra citate categorie iv e v (installazione, configurazione, servizi gestiti ...ecc) tenuto conto che la modalità di compilazione non è specificata neanche nelle linee guida ACN (Linee guida per l'applicazione dei criteri di premialità - ACN); infatti il paragrafo "1.3.2. BOM applicata ai servizi" delle linee guida ACN è chiaramente riferito ai servizi erogati da un cloud **provider** e non ai servizi professionali erogati attraverso personale impiegato presso la sede del cliente (o in altri casi da remoto).

Risposta

Si precisa che il paragrafo "1.3.2 BOM applicata ai servizi" si riferisce a tutti i servizi informatici di cui al DPCM del 30 aprile 2025 e nello specifico all'allegato 2 dello stesso, inclusi i servizi cloud (e quindi non esclusivamente a questi ultimi).

Inoltre premesso che ai fini della compilazione della BOM, occorre fare riferimento alla lista 1 di cui al par. 2.1 dell'Appendice BOM delle citate Linee guida, si precisa quanto segue.

Il campo bom.metadata.component deve essere sempre compilato, sia nel caso di prodotti, sia nel caso di servizi.

Con riferimento al campo bom.services[].provider.name, lo stesso andrà compilato indicando il nome dell'impresa che effettivamente erogherà il servizio per cui è richiesta la SBOM.

Con riferimento al campo bom.services[].provider.address.country, occorre inserire il country code della nazione, in formato ISO 3166-1, in cui risiede l'infrastruttura attraverso la quale viene erogato il servizio.

Con riferimento al campo bom.services[].provider.url, si rappresenta che è sufficiente indicare il sito internet ufficiale dell'impresa che eroga il servizio.

Con riferimento al campo bom.services[].name, l'operatore economico dovrà fornire, per ogni servizio presente all'interno della BOM, l'informazione associata al nome dello specifico servizio.

Con riferimento al campo bom.services[].version, l'operatore economico deve fornire, per ogni servizio presente all'interno della BOM, l'informazione associata alla versione del servizio considerato.

8) DOMANDA

Con l'obiettivo di garantire la massima partecipazione alla procedura in oggetto, si chiede di confermare che per l'esecuzione dell'appalto possano essere inserite, senza necessità di avvalimento o subappalto, figure

professionali apicali o operative aventi un rapporto di dipendenza con altre società appartenenti al medesimo Gruppo societario del concorrente, in virtù di accordi infragruppo.

Risposta

Si conferma, fermo restando il rispetto della normativa giuslavoristica in termini di impiego di tali figure sotto il coordinamento dell'appaltatore.

9) DOMANDA

DOCUMENTO: Allegato 1 - Domanda di Partecipazione

TESTO: "DICHARA che, ai sensi del Regolamento UE/2016/679, i dati personali oggetto di trattamento verranno gestiti nell'ambito dell'UE, e non sarà effettuato alcun trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dell'UE o dello Spazio Economico Europeo

Oppure

- DICHARA che, ai sensi del Regolamento UE/2016/679, i dati personali oggetto di trattamento saranno trasferiti verso i paesi/territori/organizzazioni, coperti da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 Regolamento UE/2016/679 o da altre garanzie adeguate ai sensi degli artt. 46 e ss. del Regolamento UE/2016/679 (es. utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR), che di seguito si elencano_____."

DOMANDA: si chiede di confermare che, nel caso in cui il concorrente non preveda per le proprie attività e, per quanto a propria conoscenza per attività di terzi, il trasferimento verso un paese o un'organizzazione internazionale al di fuori dell'UE o dello SEE di dati personali, possa dichiarare la prima delle due scelte proposte nella domanda di partecipazione ma che sia comunque possibile successivamente, a fronte di necessità organizzative o a causa di circostanze delle quali venga a conoscenza solo in seguito che richiedano il trasferimento di dati personali al di fuori dell'UE o dello SEE, di integrare la dichiarazione acquisendo il consenso dalla singola Pubblica Amministrazione contraente.

Risposta

Si conferma e si evidenzia che, in ogni caso, il Fornitore in fase di emissione dell'Ordinativo di Fornitura, potrà avvalersi di soggetti terzi stabiliti al di fuori dello Spazio Economico Europeo (SEE) previa autorizzazione da parte della PA e sempre a condizione che siano rispettate le garanzie previste dal Regolamento UE/2016/679. In merito all'Allegato 1 – Domanda di partecipazione, si invita sul punto a prendere visione della relativa Errata corrige.

10) DOMANDA

DOCUMENTO 1: Capitolato d'oneri, Par. 10, lett. d), Pag. 24 e Allegato 11 (Foglio calcolo).

DOCUMENTO 2: Allegato 1 - Domanda di partecipazione, Par. 8, Pag. 8.

Domanda: Il Capitolato d'oneri e il relativo Allegato 11 stabiliscono una riduzione forfettaria del 20% sulla garanzia provvisoria qualora l'operatore possieda una o più delle certificazioni indicate nella Tabella 3. Di contro, il modello di Domanda di partecipazione (Allegato 1) riporta in tabella percentuali di riduzione analitiche e sensibilmente inferiori, quantificate nel 5% per la norma ISO 9001 e nel 3% per le restanti certificazioni.

Si chiede di confermare che la riduzione spettante ai sensi del Par. 10, lett. d) del Capitolato d'Oneri sia pari al 20% complessivo in caso di possesso di almeno una delle certificazioni citate. Si chiede altresì di chiarire se, in caso di conferma del valore del 20% in caso di possesso di almeno una certificazione, il passaggio citato nel modello di Domanda di partecipazione debba essere considerato un refuso e che pertanto verrà pubblicato una errata corrige della Domanda di partecipazione.

Risposta

CLASSIFICAZIONE CONSIP: CONSIP PUBLIC

Si conferma quanto previsto nel Capitolato d'oneri al capitolo 10 e nell'Allegato "Allegato n.11 - Foglio di calcolo Garanzia Provvisoria e Definitiva". In merito all'Allegato "Allegato n. 1 - Domanda di partecipazione e dichiarazioni", si invita sul punto a prendere visione della relativa Errata corrige.

11) DOMANDA

DOCUMENTO: All.11 Foglio calcolo riduzione cauzioni

DOMANDA: Si chiede di rendere fruibile l'All.11 in quanto quello fornito è protetto da password.

Risposta

Si invita sul punto a prendere visione della relativa Errata corrige.

12) DOMANDA

Si chiede di confermare che, con riguardo all'art. 16 – RECESSO dello Schema di Accordo Quadro, quanto previsto al comma 1. e, cioè, che: Consip e/o le Amministrazioni, per quanto di proprio interesse, hanno diritto di recedere unilateralmente dal presente Accordo Quadro e/o da ciascun singolo Contratto esecutivo, in tutto o in parte, in qualsiasi momento, senza preavviso, nei casi di: a) giusta causa; b) reiterati inadempimenti del Fornitore, anche se non gravi, sia superato e derogato da quanto successivamente previsto al comma 3. dello stesso articolo, in cui è indicato che: Consip e/o l'Amministrazione, ai sensi dell'art. 123, commi 1 e 2 del Codice, potrà recedere dall'Accordo Quadro e/o da ciascun singolo contratto esecutivo, in qualunque momento, con preavviso non inferiore a 20 (venti) giorni solari, previo il pagamento da parte delle Amministrazioni delle prestazioni oggetto del contratto esecutivo eseguite a regola d'arte, nonché del valore dei materiali utili esistenti in magazzino (ove esistenti), oltre al decimo dell'importo delle opere, dei servizi o delle forniture non eseguite, così come determinato ai sensi dell'art. 11 dell'Allegato II.14 del Codice, rinunciando espressamente il Fornitore, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso e/o indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ.”.

Risposta

Non si conferma. Le ipotesi sono distinte e non in alternativa riguardando il comma 2 fattispecie specifiche in cui è previsto il recesso senza preavviso.

13) DOMANDA

Oggetto: Modalità di presentazione della documentazione di comprova dei requisiti tecnici (Rif. Capitolato d'Oneri par. 21 e Allegato 16)

Quesito: Con riferimento a quanto previsto al capitolo 21 del Capitolato d'Oneri e alle istruzioni di compilazione dell'Allegato 16 – Modello di Dichiarazione Tecnica, dove viene richiesto di allegare la documentazione atta a comprovare la sussistenza di tutte le caratteristiche minime e migliorative (es. datasheet, manuali tecnici), si espone quanto segue:

Considerata l'elevata numerosità dei requisiti richiesti e la dimensione dei manuali tecnici completi relativi alle soluzioni di Next Generation Firewall (NGFW), i quali possono superare le migliaia di pagine, si evidenzia che il caricamento integrale di tale documentazione potrebbe comportare il superamento dei limiti dimensionali (MB) previsti dalla piattaforma telematica. Tanto premesso, si chiede se sia possibile assolvere all'obbligo di comprova mediante una delle seguenti modalità alternative:

1. Produzione di estratti mirati dei manuali tecnici, contenenti esclusivamente le copertine (per l'identificazione del documento), l'indice originale e le sole pagine specifiche riportanti le caratteristiche tecniche dichiarate nell'Allegato 16 dove poter reperire le prove;

2. Indicazione del link ipertestuale diretto ai documenti ufficiali pubblicati sui siti web istituzionali dei produttori (es. portali di documentazione tecnica pubblica), fermo restando l'impegno del Concorrente a fornire il file completo su richiesta della Stazione Appaltante in sede di verifica.
3. Produzione, da parte del produttore, di documentazione ad hoc che attesti il rispetto delle caratteristiche minime e migliorative, comprensiva dei riferimenti alle fonti documentali da cui sono tratte le informazioni (es. datasheet e manuali tecnici), nonché dei link ipertestuali diretti ai documenti ufficiali.

Si chiede conferma che la produzione di estratti mirati (punto 1) sia considerata prova documentale sufficiente e idonea per la Commissione Giudicatrice, o che in alternativa venga accettato il puntamento esterno (punto 2) alla documentazione completa, oppure che sia ritenuta ammissibile la documentazione ad hoc (punto 3) atta a consentire la puntuale e precisa verifica dei requisiti dichiarati.

Risposta

Come indicato nel Capitolato d'Oneri al paragrafo 21, si conferma che “[..] documentazione denominata “Documenti a comprova” [...] dovrà contenere: [...] la documentazione atta a comprovare la sussistenza di tutte le caratteristiche minime e, ove offerte, migliorative, relativamente al servizio di Next Generation Firewall, alla data della sottoscrizione dell’offerta.”. Come indicato nell’ Allegato n. 16 – Modello di Dichiarazione Tecnica “è richiesto che le tabelle 2 e 3 della sezione 2 vengano compilate inserendo il nome del documento e il puntamento nel quale rinvenire il possesso del requisito specifico.”

In merito alla modalità numero 1 (produzione di estratti mirati dei manuali tecnici), si precisa che tali estratti costituiscono una documentazione atta a comprovare la sussistenza di tutte le caratteristiche minime e, ove offerte, migliorative per il servizio di Next Generation Firewall. Si ribadisce, inoltre, quanto precisato nel Capitolato d'Oneri, paragrafo 21, rispetto al caso in cui le caratteristiche tecniche vengono dichiarate dal concorrente tramite allegazione di documentazione tecnica ufficiale del produttore (quali ad esempio datasheet, brochure, manuali o schede tecniche ufficiali del produttore), “- le dichiarazioni devono essere sottoscritte digitalmente dal concorrente (in caso di concorrenti associati con le modalità indicate al punto 14.1. del presente Capitolato d'Oneri); - ogni documentazione tecnica del produttore deve essere corredata da apposita dichiarazione di conformità all’originale ex d.P.R. 445/2000, sottoscritta digitalmente dal concorrente secondo le modalità indicate al punto 14.1. del presente Capitolato d'Oneri”.

In merito alla modalità numero 2 (indicazione dei link ipertestuali), si precisa che la stessa non costituisce una documentazione atta a comprovare la sussistenza delle suddette caratteristiche ma può essere utilizzata come una informazione di supporto e integrazione della “documentazione atta a comprovare la sussistenza” di cui al Capitolato d'Oneri.

In merito alla modalità numero 3 (produzione, da parte del produttore, di documentazione ad hoc) si conferma e si ribadisce quanto precisato nel Capitolato d'Oneri, paragrafo 21, “i documenti che possono essere sottoscritti in alternativa:

- digitalmente dal produttore medesimo;
- tramite firma olografa del produttore, in tal caso i documenti devono essere corredata da apposita dichiarazione di conformità all’originale ex d.P.R. 445/2000 sottoscritta digitalmente dal concorrente secondo le modalità indicate al punto 14.1. del presente Capitolato d'oneri.”

14) DOMANDA

Si chiede di confermare che l'affidamento ad un operatore terzo della fornitura degli accessi e degli apparati comprensiva delle attività di installazione, configurazione e manutenzione - necessarie a rendere esercibili i servizi di connettività e a garantirne il corretto mantenimento in esercizio – si configura come subcontratto e non come subappalto qualora l'incidenza del costo della manodopera sia inferiore al 50% del valore del subcontratto, in quanto verrebbe a mancare una delle due condizioni di valore e di incidenza della manodopera

che invece devono sussistere congiuntamente affinché si configuri il subappalto (art. 119, comma 2, secondo capoverso, del Decreto Legislativo n. 36/2023).

Risposta

La qualificazione o meno di una attività quale "subappalto" è determinata dal ricorrere (o meno) delle disposizioni di cui all'art. 119 del Codice, a cui si rimanda. In tale contesto, l'operatore economico procederà a declinare la configurabilità della/e prestazione /i nel quadro normativo citato, tenuto anche conto delle fattispecie escluse dalla disciplina del subappalto ai sensi del medesimo articolo. Segnatamente, ai sensi del comma 2 del citato art. 119, si è in presenza di un subappalto di lavori nel caso in cui il contratto (tra subappaltatore e soggetto terzo) abbia ad oggetto attività che richiedono l'impiego di manodopera, quali le forniture con posa in opera e i noli a caldo, se singolarmente di importo superiore al 2 per cento dell'importo delle prestazioni affidate o di importo superiore a 100.000 euro e qualora l'incidenza del costo della manodopera e del personale sia superiore al 50 per cento dell'importo del contratto da affidare.

15) DOMANDA

Allegato 1 - Domanda di partecipazione - Dichiarazione per riduzione garanzia - riduzione per il possesso di uno o più delle seguenti certificazioni o marchi:

- UNI EN ISO 9001 Sistemi di gestione per la qualità 5%
- ISO/IEC 27001:2022 Sistemi di gestione della sicurezza delle Informazioni 3%
- EN ISO/IEC 27001:2023 Sistemi di gestione della sicurezza delle Informazioni 3%
- UNI CEI EN ISO/IEC 27001:2024 Sistemi di gestione della sicurezza delle Informazioni 3%
- UNI EN ISO 14001 Sistemi di gestione ambientale 3%
- UNI ISO 45001 Sistemi di gestione per la salute e sicurezza sul lavoro 3%

Si chiede conferma che l'operatore in possesso della ISO/IEC 27001:2022 - UNI CEI EN ISO/IEC 27001:2024 possa usufruire della riduzione del 3% per la 27001:2022, del 3% della 27001:2024 e anche del 3% della 27007:2023, in quanto la versione 2024 recepisce anche la precedente versione 2023.

Inoltre, nell'Allegato 11 – Foglio di calcolo Riduzioni Cauzioni, è indicato che si applica il 20% di riduzione se in possesso di almeno una tra le certificazioni indicate sopra. Pertanto, si chiede conferma che si possa applicare il 20% di riduzione anche se in possesso di una sola tra le certificazioni indicate sopra.

Risposta

In merito alla prima domanda, si veda la risposta al quesito numero 10.

In merito alla seconda domanda, si invita sul punto a prendere visione della relativa Errata corrige e la risposta al quesito numero 10.

16) DOMANDA

Capitolato d'Oneri e Schema di Accordo Quadro - nello Schema di Accordo Quadro (punto 12, pag. 36) è riportato:

<<nel caso in cui il Fornitore abbia notificato/dichiarato sovvenzioni estere ai sensi del Regolamento UE n. 2560/2022 e, al momento della stipula, sono spirati i termini previsti dell'art. 30 dello stesso Regolamento anche in relazione ad eventuali procedure d'ufficio avviate dalla Commissione UE ai sensi dell'art.29, par. 8 del Regolamento senza che sia intervenuta una decisione ai sensi dell'art. 31, par. 2 del Regolamento UE n. 2560/2022, e si sia quindi proceduto all'aggiudicazione condizionata:

Nel Capitolato d'Oneri manca il paragrafo sulle Sovvenzioni estere e la richiesta della relativa dichiarazione, a cui fa, però, riferimento l'Accordo Quadro. Si chiede, pertanto, se la dichiarazione vada prodotta o se quanto indicato nello Schema di Accordo Quadro si tratti di un refuso.

Risposta

Si conferma che quanto indicato nello Schema di Accordo Quadro è un refuso.

17) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi di Sicurezza - paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che la funzionalità di trasmissione di eventi e log al SIEM o XDR afferente al servizio SOC possa essere realizzata tramite protocolli standard di log forwarding (ad esempio Syslog o API) verso la piattaforma SIEM utilizzata dal Fornitore?

Risposta

Si conferma fermo restando quanto stabilito al requisito [R.126] del Capitolato Tecnico: “Il trasferimento di dati sensibili, quali ad esempio configurazioni di sicurezza, tra apparati gestiti e sistema di gestione del Fornitore, deve essere criptato e adeguatamente protetto con opportuni meccanismi di sicurezza volti a preservare la confidenzialità delle informazioni (a titolo esemplificativo e non esaustivo: SSH, VPN- IPsec, VPN - TLS).”

18) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi di Sicurezza - paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che la retention minima dei log pari ad almeno 12 mesi debba essere garantita dal sistema SOC del Fornitore e che tale requisito sia riferito alla conservazione dei log necessari alle attività di monitoraggio e analisi di sicurezza?

Risposta

Si conferma e si ribadisce che dovranno essere prese in considerazione tutte le varie tipologie di log acquisiti dai sistemi di sicurezza oggetto di fornitura.

19) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che l'integrazione con feed di Threat Intelligence provenienti da fonti istituzionali (ACN, CSIRT Italia, ecc.) possa avvenire tramite piattaforme di gestione delle minacce e sistemi SIEM/SOC del Fornitore, purché compatibili con protocolli standard (ad es. MISP, API, OCSF)?

Risposta

Non si conferma e si ribadisce quanto previsto al requisito [R.136] del Capitolato Tecnico: “Il SOC deve essere in grado di ricevere informazioni di security threat intelligence attraverso feed di terze parti, aggiornamento costante dei propri sistemi con gli IoC (indicatori di compromissione) e IoA (Indicatori di Attacco)” e [R.138]: “Il SOC deve recepire ed aggiornare costantemente i propri sistemi con gli IoC predisposti da fonti istituzionali o inviati dall'Amministrazione stessa.”.

20) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che i requisiti relativi alla protezione dei file di log da modifiche o cancellazioni non autorizzate possano essere soddisfatti mediante l'adozione di meccanismi di immutabilità dei log, firma digitale o sistemi di storage sicuro?

Risposta

Premesso che il requisito citato è presente a Capitolo 3 – Servizio di sicurezza, [R.90], non viene fornita alcuna prescrizione tecnica sui meccanismi da utilizzare, ciò che rileva è che il requisito sia soddisfatto.

21) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali -paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che il servizio SOC possa essere erogato tramite una piattaforma multi-tenant, garantendo la segregazione logica dei dati e degli eventi relativi alle singole Amministrazioni?

Risposta

Si conferma. Si ribadisce quanto indicato nel Capitolato tecnico al paragrafo 5.2, requisito [R.122], “Tutti i sistemi ICT funzionali all'erogazione del servizio di sicurezza, inclusi quelli centrali di gestione e di accesso per gli operatori SOC del Fornitore, devono essere esclusivamente dedicati alla S-RIPA e non possono essere contemporaneamente utilizzati in altri contesti. L'accesso da parte degli operatori del Fornitore deve avvenire da privileged access workstations (PAWs) tramite un sistema di privileged access management (PAM). Ad esclusione di quelli installati presso le Sedi estere, è consentito ospitare i suddetti sistemi su infrastrutture fisiche condivise, purché sia adottata un'opportuna segmentazione logica tramite virtualizzazione o meccanismo analogo.[...]”.

22) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC)
Si chiede di confermare che l'infrastruttura tecnologica utilizzata per l'erogazione del servizio SOC e SIEM possa essere ospitata presso data center del Fornitore ubicati nell'Unione Europea?

Risposta

Si conferma.

23) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC)
Si chiede di confermare che, su richiesta dell'Amministrazione, il Fornitore possa configurare l'invio dei log verso sistemi di monitoraggio o SIEM dell'Amministrazione stessa?

Risposta

In merito alla possibilità del Fornitore di configurare l'invio dei log verso sistemi di monitoraggio o SIEM dell'Amministrazione, si conferma e si ribadisce quanto previsto al requisito [R.83] “[...] Sempre su richiesta dell'Amministrazione, che potrebbe avvenire generalmente a seguito di un evento di sicurezza ad elevata gravità ma anche di livello inferiore, il Fornitore deve fornire i log di sistema generati dai dispositivi di sicurezza utilizzati, predisposti almeno in formato CSV o TXT. Tali log devono essere inviati all'Amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta pena l'applicazione delle penali di cui al Cap. 10” e quanto previsto al requisito [R.94] nella tabella dei “Requisiti funzionali minimi” in merito alla seguente richiesta “Trasmissione di eventi e log al SIEM o XDR afferente al servizio trasversale SOC o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione”.

24) DOMANDA

Capitolato Tecnico - Capitolo 3 – Servizi di Sicurezza - paragrafo 3.1 relativo a NGFW
Si chiede di confermare che la funzionalità di sandboxing possa essere erogata anche tramite infrastruttura cloud del Produttore e che non sia richiesta l'installazione di appliance di sandboxing on premise presso le sedi delle Amministrazioni?

Risposta

In merito alla possibilità di erogare la funzionalità di sandboxing tramite infrastruttura cloud del Produttore, non si conferma e si veda la risposta al quesito numero 29.

In merito alla possibilità di installare appliance di sandboxing on premise presso le sedi delle Amministrazioni, si conferma che è facoltà del Fornitore integrarla o meno nell'apparato Next Generation Firewall presente presso la sede così come indicato nel requisito [R.94] nella tabella dei “Requisiti funzionali minimi” in merito

alla seguente richiesta “La funzionalità di sandboxing può essere integrata oppure può essere su infrastruttura remota del Produttore, ubicata in UE”.

25) DOMANDA

Capitolato Tecnico - Capitolo 3 – Servizi di Sicurezza - paragrafo 3.1 relativo a NGFW

Si chiede di confermare che le interfacce 10Gigabit Ethernet siano richieste esclusivamente per le appliance NGFW di Fascia 3 mentre per le Fasce 1 e 2 siano sufficienti interfacce 10/100/1000 Ethernet Autosensing?

Risposta

Non si conferma in quanto è responsabilità del Fornitore scegliere l'adeguato dimensionamento del servizio NGFW nel rispetto dei requisiti minimi e migliorativi dichiarati dal Fornitore stesso.

26) DOMANDA

Capitolato Tecnico - Capitolo 3 – Servizi di Sicurezza - paragrafo 3.1 relativo a NGFW

Si chiede di confermare che per 'interconnessione con Public Cloud' si intenda la capacità dell'NGFW di integrarsi nativamente con i servizi dei cloud provider indicati tramite API o connettori dedicati e non semplicemente tramite tunnel VPN?

Risposta

Si conferma.

27) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che i sistemi ICT funzionali all'erogazione del servizio di sicurezza debbano essere dedicati alla S-RIPA e che tale segregazione possa essere garantita tramite virtualizzazione su infrastrutture fisiche condivise con adeguata segmentazione logica?

Risposta

Si conferma. Si veda anche la risposta al quesito numero 21.

28) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC)

Si chiede di confermare che i log forniti all'Amministrazione debbano includere almeno gli eventi di sicurezza e gli accessi amministrativi e che possano essere forniti in un formato standard leggibile e interoperabile?

Risposta

Si precisa che i log forniti all'Amministrazione, sono i log generati dai dispositivi di sicurezza utilizzati, come indicato al requisito [R.83], e sono i log relativi alle attività di gestione, manutenzione e amministrazione, come indicato al requisito [R.88]. In merito al formato, si ribadisce quanto indicato al requisito [R. 83] “[..] predisposti almeno in formato CSV o TXT”.

29) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC)

Con riferimento alla piattaforma SIEM e SOAR richiesta nell'ambito dei servizi di Security Operation Center (SOC), si chiede di chiarire quanto segue.

Nel caso in cui tali piattaforme siano erogate in modalità SaaS (Software as a Service), si richiede di confermare:

1. se tali soluzioni debbano essere qualificate secondo il processo di qualificazione dei servizi cloud per la Pubblica Amministrazione previsto dall'Agenzia per la Cybersicurezza Nazionale (ACN);
2. in caso affermativo, quale sia il livello minimo di qualificazione richiesto (es. qualificazione ACN per servizi cloud per la PA, eventuale classificazione del servizio o ulteriori requisiti specifici);

3. se la qualificazione debba riguardare la piattaforma SIEM/SOAR in quanto servizio SaaS oppure l'infrastruttura cloud sottostante utilizzata per l'erogazione del servizio SOC da Centro Servizi del Fornitore.
4. in caso di richiesta di qualificazione ACN si chiede inoltre di confermare che la verifica del possesso di qualificazione avverrà in fase di stipula dell'AQ.

Risposta

Le piattaforme SIEM e SOAR non possono essere erogate in modalità SaaS. Si ribadisce quanto riportato nel Capitolato Tecnico al requisito [R.123] "Il Fornitore è tenuto ad erogare il servizio SOC avvalendosi di un'infrastruttura hardware/software installata presso il centro servizi del Fornitore."

30) DOMANDA

Capitolato Tecnico - Capitolo 5 – Servizi trasversali - paragrafo 5.2 relativo al Security Operation Center (SOC) Con riferimento alla piattaforma SIEM/SOAR utilizzata per l'erogazione dei servizi di Security Operation Center (SOC), si richiede di chiarire i requisiti relativi alla localizzazione e al trattamento dei dati di sicurezza (log, eventi, telemetrie e informazioni correlate). In particolare, si chiede di confermare:

1. se i dati raccolti e analizzati dalla piattaforma SIEM/SOAR debbano essere conservati ed elaborati esclusivamente all'interno del territorio dell'Unione Europea oppure se sia ammesso l'utilizzo di infrastrutture cloud localizzate in Paesi extra-UE purché conformi alla normativa vigente (es. Paesi NATO);
2. se siano previsti vincoli specifici di sovranità del dato o requisiti di data residency in relazione alla natura dei dati trattati nell'ambito dei servizi SOC;
3. se eventuali servizi SaaS di analisi, correlazione o threat intelligence integrati nella piattaforma SIEM/SOAR possano prevedere il trasferimento di metadati o eventi di sicurezza verso infrastrutture situate al di fuori dell'Unione Europea e/o paesi amici.

Risposta

In merito al punto 1, se i dati raccolti e analizzati dalla piattaforma SIEM/SOAR contengono anche dati personali, il trasferimento di tali Dati al di fuori dell'Unione europea per l'erogazione di servizi connessi al Contratto di fornitura – da intendersi anche come mero accesso ai dati da un paese terzo – potrà avvenire, previa autorizzazione dell'Amministrazione, da o verso un paese terzo o un'organizzazione internazionale coperta da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 del Regolamento o da altre garanzie adeguate di cui agli artt. 46 e ss. del Regolamento stesso (es. utilizzo delle clausole contrattuali tipo adottate dalla Commissione europea ai sensi dell'art. 46, par. 2, lett. c) del Regolamento, utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR), fatta salva la necessità valutata preventivamente tra le Parti di adottare eventuali misure supplementari per garantire l'efficacia di tali garanzie. In merito all'utilizzo di infrastrutture cloud, si ribadisce quanto indicato nella risposta al quesito numero 29.

In merito al punto 2, non si conferma, la decisione è rimessa all'Amministrazione.

In merito al punto 3, vale quanto indicato al punto 1 con riferimento ai dati personali e all'utilizzo di infrastrutture cloud.

31) DOMANDA

Capitolato d'Oneri - 17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA - Criterio 38

Con riferimento alla categoria 18 dell'Allegato 2 del DPCM, relativa ai servizi di installazione, configurazione e manutenzione dei prodotti, di cui criterio di valutazione 38, ai punti i), ii) e iii), si richiede di chiarire le modalità di applicazione del requisito relativo alla presentazione della BOM in formato CycloneDX v1.6. In particolare, considerato che le Linee Guida ACN del 24 ottobre 2025 prevedono che la BOM rappresenti, a livello 1, i componenti e/o servizi costituenti le tecnologie di cybersicurezza, si chiede di confermare che:

- con riferimento alla categoria 18 (servizi di installazione, configurazione e manutenzione), la BOM/SBOM in formato CycloneDX non debba includere componenti hardware (es. appliance fisiche), ma debba essere riferita all'installazione, configurazione e manutenzione delle componenti software/firmware delle tecnologie di cybersicurezza di cui ai punti i), ii) e iii) esclusa la manutenzione hardware.

Risposta

Si veda la risposta al quesito numero 2.

32) DOMANDA

Capitolato d'Oneri - 17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA - Criterio 38

Con riferimento alla categoria 18 dell'Allegato 2 del DPCM, di cui al criterio prerelativa ai servizi di installazione, configurazione e manutenzione dei prodotti, di cui criterio di valutazione 38, ai punti i), ii) e iii), si richiede di chiarire le modalità di applicazione del requisito relativo alla presentazione della BOM in formato CycloneDX v1.6. In particolare, considerato che le Linee Guida ACN del 24 ottobre 2025 prevedono che la BOM rappresenti, a livello 1, i componenti e/o servizi costituenti le tecnologie di cybersicurezza, si chiede di confermare che:

- nell'ambito dei servizi di cui alla categoria 18, la SBOM debba essere riferita esclusivamente ai software/Firmware riferiti ai punti i) ii) iii) che implementano le funzionalità di cybersicurezza che concorrono al punteggio premiale, ovvero: software di VPN, software di firewall e software di piattaforme SIEM, escludendo le componenti infrastrutturali fisiche e virtuali.

Risposta

Si veda la risposta al quesito numero 2. Si precisa che la categoria 18, come indicato al Capitolato d'Oneri - criterio premiale numero 38, lettera iv (categoria 18) – si riferisce al servizio di installazione, configurazione e manutenzione riferiti ai prodotti: software di VPN per la realizzazione del servizio di connettività Best Effort, piattaforma software SIEM, firewall rispettivamente lettera i., ii. e iii. del suddetto criterio. Si rimanda alle “Linee Guida per l'applicazione dei criteri di premialità” del 24 Ottobre 2025 di ACN, paragrafo 1.3 “Formato di presentazione della BOM” per la distinzione tra “BOM applicata ai prodotti” e “BOM applicata ai servizi”.

33) DOMANDA

Capitolato d'Oneri - 17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA - Criterio 38

Con riferimento alla categoria 18 dell'Allegato 2 del DPCM, relativa ai servizi di installazione, configurazione e manutenzione dei prodotti, di cui criterio di valutazione 38, ai punti i), ii) e iii), si richiede di chiarire le modalità di applicazione del requisito relativo alla presentazione della BOM in formato CycloneDX v1.6. In particolare, nel caso in cui i servizi di installazione, configurazione e manutenzione siano associati a componenti software erogati tramite infrastrutture (anche centralizzate o cloud), si chiede di confermare che, ai fini della verifica dei requisiti di provenienza geografica previsti dal DPCM, si debba fare riferimento:

1. al Paese di appartenenza del/i siti dove operano le figure che si occupano dell'erogazione del servizio oppure
2. al Paese in cui è localizzata l'infrastruttura che ospita il software oggetto del servizio.

Risposta

Si veda preliminarmente la risposta al quesito numero 7.

Come riportato nelle “Linee Guida per l'applicazione dei criteri di premialità” del 24 Ottobre 2025 di ACN, nel campo “bom.services[].provider.address.country” è esplicitato il country code della nazione, in formato ISO 3166-1, in cui risiede l'infrastruttura attraverso la quale viene erogato il servizio.

Si ribadisce, inoltre, quanto indicato alla risposta del quesito numero 2 e nel Capitolato Tecnico al requisito [R. 123] “Il Fornitore è tenuto ad erogare il servizio SOC avvalendosi di un'infrastruttura hardware/software installata presso il centro servizi del Fornitore.” e al requisito [R.128] “Il SOC deve essere realizzato attraverso

infrastrutture che rispettino le normative vigenti in tema di sicurezza fisica e logica, oltre alla sicurezza di connessione in rete.”.

34) DOMANDA

Capitolato d'Oneri - 17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA - Criterio 38

Con riferimento alla categoria 18 dell'Allegato 2 del DPCM, relativa ai servizi di installazione, configurazione e manutenzione dei prodotti, di cui criterio di valutazione 38, ai punti i), ii) e iii), si richiede di chiarire le modalità di applicazione del requisito relativo alla presentazione della BOM in formato CycloneDX v1.6. In particolare, si chiede di confermare che, per i servizi di cui alla categoria 18, sia possibile produrre un'unica SBOM che includa tutti le tre componenti di attività di installazione, configurazione e manutenzione, relative ai prodotti ai punti i), ii) e iii).

Risposta

In merito alla struttura della BOM, si rimanda al paragrafo 1.1 dell'appendice delle “Linee Guida per l'applicazione dei criteri di premialità” del 24 Ottobre 2025 di ACN “Essa deve contenere, pertanto: [...] un elenco di elementi, indicati in bom.components (per prodotti) o bom.services (per servizi), per ciascun bene o servizio costituente l'oggetto della fornitura (Livello 1).”, oltre al campo bom.metadata.component, che deve essere compilato sia in caso di prodotti sia in caso di servizi. Pertanto, posto che i dati devono essere inseriti per ciascuno dei servizi indicati nel quesito, si conferma.

35) DOMANDA

Capitolato d'Oneri - 17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA - Criterio 38

Relativamente alla parte di Next Generation Firewall e console di management, ai fini del criterio di premialità, si chiede di confermare che la SBOM da produrre deve contenere solo gli 8 campi obbligatori come riportato nel documento Linee guida per l'applicazione dei criteri di premialità di cui all'articolo 14 della legge n. 90/2024 Capitolo 2.1. Campi minimi per componenti/servizi di ACN. Di seguito gli 8 campi: 1. Bom.metadata.component, 2. Bom.components[].manufacturer, 3. Bom.components[].type, 4. Bom.components[].name, 5. Bom.components[].version, 6. Bom.services[].provider, 7. Bom.services[].name, 8. Bom.services[].version.

Risposta

Come da “Linee Guida per l'applicazione dei criteri di premialità” del 24 Ottobre 2025 di ACN, al paragrafo 1.6 dell'appendice delle suddette linee guida, i campi minimi riportano la seguente descrizione “Per poter ottenere il punteggio premiale, l'operatore economico deve fornire una BOM compilata con i campi minimi riportati nella lista tabellare 1 all'interno dell'Appendice Tecnica, potendo far riferimento alla colonna ‘Interpretazione del Campo’ al fine di fornire un dato coerente con le specificità dei vari elementi.” Si precisa altresì quanto segue: con riferimento a tutte le categorie deve essere compilato il campo iniziale bom.metadata.component di cui al paragrafo 2.1 e in aggiunta

- con riferimento alle categorie di cui ai punti i), ii), iii), dovranno essere compilati i campi relativi “components”;
- con riferimento alle categorie di cui ai punti iv) e v), dovranno essere compilati i campi relativi “services”.

Si veda altresì la risposta al quesito numero 7.

36) DOMANDA

Capitolato d'Oneri - 17.1 CRITERI DI VALUTAZIONE DELL'OFFERTA TECNICA - Criterio 38

Si richiede di confermare che, per le soluzioni SaaS, tenuto conto delle peculiarità dei servizi cloud e considerato quanto indicato nell'art 4 del DPCM DEL 30/04/2025 che fa esplicito riferimento alle "infrastrutture impiegate per erogare un servizio", ai fini dell'attribuzione del punteggio premiale valga la sola indicazione del

Paese ove risiede l'infrastruttura, ossia il Data Center o la Region, impiegata dal cloud service provider che eroga il servizio in modalità cloud/SaaS.

Risposta

Si veda la risposta al quesito numero 29 e numero 33.

37) DOMANDA

DOCUMENTO1: ID 2834 - AQ SRIPA - All. 6 - Modello di offerta tecnica_v1.0.xlsx

DOCUMENTO2: ID 2834 - AQ SRIPA - All. 1 al CT - Vista complessiva servizi di connettività delle PA_v1.0.xlsx

DOMANDA:

Nell' All.6 per la sede nel Regno Unito del Maeci Id. 232 sono richieste delle bande pari a 10Gbps e 2Gbps rispettivamente per SC1 e SC2, tali bande non sembrano coerenti con le bande di 1Gbps richieste per le linee SC1 e SC2 delle sedi italiane che si ipotizza siano gli HQ del cliente (vedi All. 1. vista complessiva rete attuale). Si chiede di confermare se le bande richieste siano effettivamente quelle presenti in allegato 6 o se i valori indicati siano un refuso ed in tal caso indicare quali quelli corretti, anche in riferimento al requisito RU migliorativo richiesto che non sembra coerente con quanto presente come affidabilità attuale standard indicata nell'All.1. sempre per la sede id.232

Risposta

Si conferma quanto indicato all'Allegato numero 6 del Capitolato d'Oneri per la sede ID 232. In merito all'Allegato 1 del Capitolato tecnico, si ribadisce quanto indicato "L'Allegato "ID 2834 - SRIPA - All. 1 - Vista complessiva servizi di connettività delle PA" al presente Capitolato Tecnico contiene un quadro sintetico delle consistenze dei servizi di connettività fruiti dalle Amministrazioni aderenti alla precedente iniziativa aggiornato ad Agosto 2025 integrato con le informazioni sui servizi di connettività attivati in autonomia dalle Amministrazioni al di fuori dell'iniziativa di gara S-RIPA."

38) DOMANDA

DOCUMENTO: Capitolato tecnico, Cap. 2 SERVIZI DI CONNETTIVITA, pg.16 e pg.17

TESTO:

[R.19] I servizi di connettività devono permettere la trasmissione di pacchetti IP nei seguenti ambiti (o sottoinsieme di essi indicato dall'Amministrazione):

Ambito di trasferimento privato

- Intranet: componente di trasferimento con indirizzamento privato costituita dal dominio interno alla singola Amministrazione che connette tutte le sedi della stessa (o un loro sottoinsieme), distribuite sul territorio nazionale e internazionale. La singola Amministrazione contraente deve poter raggiungere in modalità Intranet anche i servizi erogati tramite soggetti titolari quali Poli Strategici Nazionali e/o Centri Servizi del Fornitore, che rappresenteranno, in tal caso, le ulteriori sedi di erogazione dei servizi dell'Amministrazione;

Ambiti di trasferimento pubblico

- Infranet: componente di trasferimento con indirizzamento pubblico che connette tra loro le singole Amministrazioni attestata sul medesimo ISP o su ISP differenti attraverso la QXN (Qualified eXchange Network);
- Internet: componente di trasferimento con indirizzamento pubblico costituita dall'interconnessione di una specifica Amministrazione con la rete Internet pubblica.

[R.20] Le diverse modalità di erogazione dei servizi di connettività devono consentire all'Amministrazione la trasmissione/ricezione di pacchetti IPv4 e IPv6 negli ambiti configurati.

Sui servizi di connettività, oltre l'ambito di trasferimento privato (componente di trasferimento Intranet), incluso di default e disattivabile su richiesta, il Fornitore deve permettere, su richiesta dell'Amministrazione, l'abilitazione del traffico dati multiambito, cioè anche dell'ambito di trasferimento pubblico (componente di

trasferimento Infranet e/o componente di trasferimento Internet). Ognuna delle componenti di trasferimento, su richiesta dell'Amministrazione, deve poter essere disabilitata separatamente.

[R.21] Il Fornitore deve garantire, su accessi configurati per gestire più componenti di trasferimento, la segregazione del traffico appartenente a ciascuna componente di trasferimento ed è compito dell'apparato di accesso eseguire l'instradamento del traffico sulla componente di trasferimento corretta.

DOMANDA:

In riferimento ai requisiti [R.19], [R.20] e [R.21] del Capitolato Tecnico, relativi alla gestione degli ambiti di trasferimento Intranet, Infranet e Internet, al traffico dati multiambito e alla segregazione del traffico, inclusa la possibilità di abilitare/disabilitare separatamente le singole componenti di trasferimento, si chiede di confermare se tali requisiti debbano essere garantiti solo su accessi di tipo MPLS escludendo quindi accessi basati su Internet e/o su connettività satellitare (Geo/Leo).

Risposta

Non si conferma.

Divisione Sourcing Infrastrutture, TLC e Cybersecurity

Il Responsabile

(Dott. Olindo Rencricca)
