

Richiesta di Offerta (RdO) aperta tramite MePA, ai sensi dell'art. 50, comma 1, lett. ed e), del D. Lgs. n. 36/2023, per l'affidamento dei servizi per la Governance in ambito Cybersecurity per la Cassa per i Servizi Energetici e Ambientale – CSEA – CIG BAAB8EB21A

FAQ

Domanda n. 1

Con la presente siamo a richiedere conferma di compilazione e trasmissione dell'EDGUE tramite piattaforma, come indicato nella Richiesta di Offerta art.10, l,2).

All'interno della piattaforma, però, l'apposita sezione risulta chiusa con il messaggio alert automatico seguente: *"La compilazione della Response non è richiesta, in quanto la Stazione Appaltante non ha predisposto un DGUE Request."*

Risposta n. 1

Si conferma che, ai sensi dell'art. 10 della RdO, l'EDGUE deve essere compilato tramite Piattaforma MePA, accedendo al seguente link <https://www.acquistinretepa.it/espd-dgue/#!/start>, selezionando l'opzione "sono un operatore economico" e caricando l'EDGUE request prodotto dalla stazione appaltante, all'interno della busta amministrativa tra la documentazione da compilare. Successivamente, dovrà essere firmato digitalmente e caricato nell'apposita sezione della busta amministrativa.

Domanda n. 2

I Lead Auditor devono possedere un'attestazione valida rilasciata da organo accreditato o una vera e propria certificazione?

I termini per la gestione incidenti da quanto dichiarato risultano scaduti. In caso contrario quale sarebbe il termine?

Risposta n. 2

Si conferma che i Lead Auditor devono essere in possesso di una certificazione in corso di validità rilasciata da organismo accreditato, non essendo ritenuta sufficiente una mera attestazione.

Con riferimento alla procedura per la gestione degli incidenti, sebbene i termini originariamente previsti risultino già scaduti, permane la necessità di procedere alla revisione, integrazione e aggiornamento della procedura esistente, al fine di garantirne la piena coerenza con il complessivo sistema di governance e con il corpus documentale di riferimento, attività che rientra tra le prestazioni richieste all'affidatario.

Domanda n. 3

Con riferimento a quanto indicato nella Determina n. 27 – Avvio RdO aperta per l'affidamento dei servizi per la governance in ambito cyber security, e in particolare ai Requisiti di ordine speciale – Capacità tecniche e professionali, si chiede di confermare quanto segue: in relazione al requisito

inerente il possesso di n. 10 servizi di gestione e coordinamento di progetti di implementazione, mantenimento o rinnovo di certificazioni, si chiede se possano essere ritenute valide, ai fini della copertura del requisito, anche referenze maturate in ambiti differenti da quello energetico e ambientale, purché caratterizzate da analoga complessità (a titolo esemplificativo: telco, tech, banking, Pubblica Amministrazione). Tale richiesta è motivata dal fatto che, considerato l'arco temporale di riferimento previsto per la valutazione (ultimi 10 anni), i settori sopra richiamati risultano essere tra quelli che hanno maggiormente adottato sistemi di gestione in ragione del quadro normativo vigente in materia di sicurezza informatica.

Con riferimento a quanto indicato al paragrafo 2 del Capitolato, ove si specifica che la CSEA risulta certificata ISO/IEC 27001:2022 e ISO 22301:2019, si chiede cortesemente di precisare il perimetro di servizi e sistemi informativi inclusi nel perimetro di certificazione.

Risposta n. 3

Con riferimento al quesito 3.1, si segnala che il requisito di capacità tecniche e professionali è stato modificato con determina n. 29 del 17.03.2026 Prot. CSEA - Reg.Int: 0000261-17-03-2026-I, ed in pari data è stata pubblicata la RdO rettificata, con contestuale proroga dei termini di gara.

Con riferimento a quanto richiesto con riferimento alle certificazioni ISO/IEC 27001:2022 e ISO 22301:2019, il cui patrimonio informativo sarà condiviso con l'aggiudicatario, la CSEA ha individuato i confini e l'applicabilità del Sistema di Gestione Integrato descrivendo il perimetro dal punto di vista logico (servizi e processi), tecnologico (sistemi ICT), fisico (sedi) ed organizzativo (unità organizzative), in particolare:

- Sicurezza delle Informazioni: progettazione, sviluppo e gestione dell'infrastruttura ICT a supporto dei servizi IT;
- Continuità Operativa: continuità operativa della infrastruttura ICT a supporto dei Servizi IT.

Si precisa che potrebbe essere necessaria una gap analysis tra quanto già considerato dalle citate certificazioni e quanto invece richiesto dalla NIS2, e conseguenti azioni.

Domanda n. 4

Con riferimento agli interventi richiesti nell'ambito della formazione Cyber, si chiede di confermare se per l'anno in corso sia già stato predisposto dalle strutture competenti dell'Ente (es. ufficio formazione) un Piano annuale della formazione.

Risposta n. 4

Con riferimento agli interventi richiesti nell'ambito della formazione Cyber, per l'anno in corso, la CSEA ha redatto un Piano annuale della formazione.

Domanda n. 5

Con riferimento alla figura di "Responsabile di Progetto", si chiede di confermare se il possesso della certificazione "PRINCE2 Foundation" - o di altre certificazioni equivalenti in ambito Project

Management - unitamente alle certificazioni Lead Auditor ISO/IEC 27001 e Lead Auditor ISO 22301, sia da considerarsi requisito obbligatorio.

Risposta n. 5

Si conferma che, con riferimento alla figura di Responsabile di Progetto, il possesso della certificazione PRINCE2 Foundation, o di certificazioni equivalenti in ambito Project Management, unitamente alle certificazioni Lead Auditor ISO/IEC 27001 e Lead Auditor ISO 22301, è da considerarsi requisito obbligatorio.

Domanda n. 6

Con riferimento al requisito relativo al possesso delle certificazioni "Lead Auditor ISO/IEC 27001" e "Lead Auditor ISO 22301", si chiede di confermare se tale requisito debba ritenersi obbligatorio sia per la figura di "Esperto/a di conformità" che per la figura di "Esperto/a di processi di cybersecurity", oltre che per la figura di "Responsabile di Progetto".

Risposta n. 6

Si conferma che il requisito relativo al possesso delle certificazioni Lead Auditor ISO/IEC 27001 e Lead Auditor ISO 22301 deve intendersi obbligatorio per tutte le figure indicate, ivi incluse la figura di Esperto/a di conformità, la figura di Esperto/a di processi di cybersecurity e la figura di Responsabile di Progetto.

Domanda n. 7

Con riferimento al requisito relativo al possesso delle certificazioni "Lead Auditor ISO/IEC 27001" e "Lead Auditor ISO 22301", si chiede di confermare se tale requisito debba intendersi applicabile esclusivamente alle figure professionali espressamente richieste dal capitolato, oppure anche ad eventuali ulteriori risorse aggiuntive che il Fornitore intenda proporre nell'ambito dell'offerta tecnica.

Risposta n. 7

Si conferma che il requisito relativo al possesso delle certificazioni Lead Auditor ISO/IEC 27001 e Lead Auditor ISO 22301 deve intendersi applicabile solamente a tutte le figure professionali espressamente richieste dal capitolato ed impiegate nell'esecuzione del servizio.

Domanda n. 8

In riferimento alla procedura di gara in oggetto,

- considerata l'attuale scadenza che ricade immediatamente dopo le festività pasquali, riducendo significativamente i giorni lavorativi disponibili per la predisposizione dell'offerta;
- considerato che la procedura richiede un impegno tecnico-organizzativo rilevante, con particolare riguardo alla Relazione Tecnica, alla Matrice delle competenze e alla raccolta delle certificazioni del team di progetto richieste dal Capitolato;
- tenendo anche conto dei tempi tecnici per predisporre ed ottenere un livello di approvazione funzionale alla possibile migliore offerta da presentarVi.

Si chiede che codesta Stazione appaltante voglia concedere una proroga del termine per la presentazione dell'Offerta almeno al prossimo 23 aprile 2026

Risposta n. 8

Considerato il congruo termine già concesso per la presentazione delle offerte, tenuto conto, altresì, della necessità di avviare il servizio tempestivamente, e del bilanciamento dei diversi interessi coinvolti, non si ritengono sussistenti i presupposti per concedere la proroga richiesta del termine di presentazione delle offerte.

Domanda n. 9

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.12; Argomento: f) Gestione degli asset. Definizione e prima redazione dell'inventario degli apparati fisici, dei software, dei sistemi e dei servizi che compongono i sistemi informativi e di rete, inclusi i servizi erogati da terze parti, ivi inclusi i servizi cloud;

Domanda: Si chiede di confermare che per la redazione dell'inventario sia possibile utilizzare un soluzione software a servizio del fornitore che possa effettuare tramite scan la rilevazione e la categorizzazione degli asset IT. In caso contrario, si chiede di fornire maggiori informazioni relative alle attività previste dal punto f).

Risposta n. 9

Si conferma che, ai fini della redazione dell'inventario, è ammesso l'utilizzo di soluzioni software nella disponibilità del Fornitore, ivi incluse quelle basate su attività di scansione automatizzata per la rilevazione e la categorizzazione degli asset IT.

Resta inteso che le risultanze dovranno essere rese disponibili in formati aperti e non proprietari, al fine di garantirne la piena fruibilità e riutilizzabilità da parte della Stazione Appaltante.

Si precisa, altresì, che l'attività di inventariazione non si esaurisce nella sola rilevazione degli apparati fisici, ma deve ricomprendere, come indicato nel Capitolato, anche software, sistemi, servizi e componenti erogati da terze parti, inclusi i servizi cloud, la cui corretta identificazione e classificazione costituisce parte integrante e non trascurabile della prestazione richiesta.

Domanda n. 10

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.12; Argomento: h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi. Definizione e redazione del piano di continuità operativa, del piano di ripristino in caso di disastro e del piano per la gestione delle crisi informatiche per almeno i sistemi informativi e di rete rilevanti. Definizione e redazione delle politiche e procedure di revisione ed aggiornamento dei piani di cui al punto precedente.

Domanda: Si chiede di specificare se siano già state effettuate delle analisi e delle procedure di Disaster Recovery e Business Continuity.

Risposta n. 10

Si precisa che risultano già svolte attività in materia di continuità operativa e disaster recovery nell'ambito dei processi connessi alle certificazioni ISO/IEC 27001:2022 e ISO 22301:2019 di cui la CSEA è in possesso.

Tuttavia, tali attività costituiscono la base di partenza per tutto quanto richiesto dal Capitolato, che prevede la revisione, l'integrazione e l'aggiornamento dei piani e delle procedure esistenti, nonché il loro eventuale ampliamento in coerenza con il perimetro dei sistemi informativi e di rete rilevanti.

Domanda n. 11

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.15; Argomento: 1. Assetto procedurale e organizzativo; Prima esecuzione delle attività periodiche previste (ad esempio: redazione di elenchi ed inventari, valutazione del rischio, individuazione delle forniture critiche, etc.).

Domanda: Si chiede di fornire maggiore dettaglio sulle attività periodiche previste e sul perimetro oggetto di tali attività.

Risposta n. 11

Si precisa che le attività periodiche previste, nonché il loro perimetro di applicabilità, sono tutte e sole quelle richieste dalla normativa NIS2.

Domanda n. 12

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.15; Argomento: 2. Formazione Domanda: Si chiede di fornire il numero di discenti che saranno oggetto di formazione dell'attività.

Risposta n. 12

Si precisa che il numero di discenti è variabile in funzione delle specifiche attività formative che si intende erogare.

A titolo indicativo, la platea della CSEA è, alla data di redazione del presente documento, composta da meno di 150 persone, di cui meno di 20 appartenenti al personale informatico.

Per ulteriori informazioni di dettaglio si rimanda ai dati pubblicamente disponibili sul sito istituzionale della CSEA.

Domanda n. 13

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.16; Argomento: 3. Applicazione operativa diretta sui sistemi Interventi consistenti nell'implementazione di configurazioni, controlli e misure di sicurezza applicabili in modo immediato ai sistemi informativi esistenti, senza necessità di acquisizione di nuovi prodotti software né di competenze aggiuntive rispetto a quelle già disponibili presso l'Ente. Deliverable previsti: Supporto alla definizione e alla redazione di manuali operativi, linee guida e playbook tecnici, coerenti con la specifica azione considerata.

Domanda: Per indirizzare con precisione le professionalità richieste, si chiede di fornire maggiore dettaglio sul perimetro oggetto di tali attività con, possibilmente, le numeriche ed il dettaglio degli asset.

Risposta n. 13

Si rappresenta che, allo stato attuale e in via meramente indicativa e non vincolante, la CSEA dispone complessivamente di un'infrastruttura di produzione composta da circa 120 server, sia in ambiente Linux sia Windows, destinati all'erogazione dei servizi istituzionali e di funzionamento interno.

Tale infrastruttura risiede principalmente su servizi IaaS del Polo Strategico Nazionale.

Le informazioni sopra riportate sono da intendersi non esaustive, non vincolanti e soggette a possibili variazioni nel corso dell'esecuzione contrattuale, senza che ciò comporti il riconoscimento di corrispettivi aggiuntivi rispetto a quanto offerto in sede di gara.

Domanda n. 14

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.16; Argomento: 4. Applicazione operativa sui sistemi con acquisizione di software Supporto alla redazione di capitolati tecnici per la pubblicazione di procedure di gara o per l'adesione a convenzioni Consip, con particolare riferimento alla definizione delle metriche per la quantificazione economica, dei livelli di servizio (SLA), delle penali e di ogni ulteriore elemento tecnico-economico utile allo scopo. 5. Applicazione operativa sui sistemi con competenze specialistiche Supporto alla redazione di capitolati tecnici per la pubblicazione di procedure di gara o per l'adesione a convenzioni Consip, con particolare riferimento alla definizione delle metriche per la quantificazione economica, dei livelli di servizio (SLA), delle penali e di ogni ulteriore elemento tecnico utile alla corretta esecuzione degli interventi.

Domanda: Si chiede di confermare che il supporto alla redazione previsto per le attività in oggetto sia inteso come supporto di revisione della documentazione di gara fornita dalla Committente

Risposta n. 14

Non si conferma. Il supporto richiesto non è da intendersi limitato alla sola revisione di documentazione eventualmente predisposta dalla Committente, ma comprende anche attività di supporto alla redazione, integrazione e strutturazione dei contenuti tecnici ed economici necessari attraverso l'utilizzo di best practices, linee guida e quant'altro possa rendersi necessario affinché la procedura di acquisto risulti efficace ed efficiente al rispetto dei requisiti NIS2.

Resta inteso che, qualora la CSEA disponga, al momento dell'esecuzione, di documentazione pertinente, la stessa sarà messa a disposizione del Fornitore quale base informativa di riferimento.

Domanda n. 15

Si desidera contestare la specifica dei requisiti relativi alla Direttiva NIS2, in quanto il criterio che richiede di aver eseguito attività di adeguamento alla compliance per un importo non inferiore a 50.000 euro per ciascun progetto risulta essere altamente limitante. La previsione appare, inoltre, sproporzionata e restrittiva, in quanto seleziona gli operatori economici non sulla base dell'effettiva

competenza specialistica maturata nell'ambito della compliance NIS2, bensì sulla base di una soglia economica rigida riferita a ciascun singolo incarico, senza che emerga una puntuale giustificazione della necessità di tale parametro rispetto all'oggetto e alla complessità dell'affidamento. Considerando che le Direttive NIS e NIS2 sono relativamente nuove, molte realtà, pur avendo esperienza rilevante nel settore della compliance, potrebbero non aver gestito un numero specifico di progetti di tale importo. L'imposizione di un importo minimo rischia di escludere realtà specializzate nella consulenza per la sicurezza in ambito cybersecurity e la compliance, ma di dimensioni medio-piccole, violando al contempo il principio di "trattamento equo" sancito anche dalle normative di appalto pubblico. Pertanto, si propone di rivedere tale requisito, consentendo di partecipare anche alle aziende che hanno gestito progetti di dimensioni inferiori ma altrettanto significativi, purché dimostrabili in termini di esperienza e qualità dei risultati ottenuti. In particolare, si chiede che la capacità tecnica sia valutata sulla base della pertinenza, complessità ed effettiva qualità dei servizi svolti, e non esclusivamente sul valore economico del singolo contratto.

Motivazioni per la Contestazione del Requisito:

1. Nuova Applicazione della Normativa (NIS e NIS2):

- Le Direttive NIS e NIS2 sono normative relativamente nuove, e molte aziende di consulenza (soprattutto quelle di dimensioni medie) potrebbero non aver ancora avuto l'opportunità di gestire progetti di adeguamento con valori così elevati, pur avendo comunque esperienza nella gestione di progetti di compliance legati alla sicurezza cibernetica. Il requisito dell'importo potrebbe quindi escludere ingiustamente realtà competenti ma che non hanno avuto il volume di progetti richiesto. Con specifico riferimento alla NIS2, la previsione appare ancor più critica, in quanto si tratta di un ambito regolatorio di recente consolidamento; pertanto, la richiesta di almeno 10 servizi da almeno euro 50.000 ciascuno rischia di non essere coerente con l'effettiva maturazione del mercato di riferimento.

2. Esclusione delle PMI e delle Società di Consulenza Specializzate:

- Imporre un importo minimo di 50.000 euro per ciascun progetto potrebbe limitare la partecipazione solo alle grandi società di consulenza, escludendo altre aziende che, pur non avendo gestito progetti così grandi, sono comunque in grado di garantire servizi di alta qualità. Questo tipo di criterio potrebbe violare il principio di non discriminazione, limitando la concorrenza e non consentendo alle realtà più piccole ma altamente qualificate di partecipare.

3. Competenza Comprovata, Indipendentemente dal Budget:

- Anche se una società non ha gestito un progetto di 50.000 euro o più, potrebbe comunque possedere una comprovata esperienza nell'adeguamento alla normativa NIS/NIS2, attraverso contratti con importi inferiori, ma comunque rilevanti e significativi in termini di qualità del servizio. La validità della competenza non dovrebbe dipendere esclusivamente dal valore economico del progetto, ma dalla qualità dell'adeguamento effettuato, dalle soluzioni implementate e dai risultati ottenuti.

4. Equità nella Partecipazione:

- Un requisito troppo stringente in termini di importo potrebbe violare il principio di "trattamento equo", sancito anche dalle normative di appalto pubblico. Le gare devono garantire che tutte le imprese, indipendentemente dalle loro dimensioni, abbiano pari opportunità di partecipare. La specifica di un importo minimo per progetto potrebbe non essere coerente con la finalità di garantire un'ampia e sana concorrenza. Più correttamente, la clausola rischia di porsi in contrasto con i principi sopracitati nella misura in cui seleziona gli operatori in base al valore economico del singolo incarico più che all'effettiva capacità tecnica.

Si chiede pertanto la revisione del requisito, mediante riduzione o eliminazione della soglia minima di euro 50.000 per singolo servizio, ovvero mediante ammissione del cumulo di incarichi di importo inferiore, purché pertinenti, dimostrabili e coerenti con l'oggetto della gara.

Risposta n. 15

Con riferimento alla richiesta di modifica del requisito di capacità tecniche e professionali nella parte in cui è previsto che il valore di ciascun contratto analogo svolto non sia inferiore ad euro 50.000,00 (cinquantamila/00), si rileva quanto segue.

Il suddetto requisito è stato individuato dalla CSEA, nell'ambito della propria discrezionalità amministrativa, al fine di garantire che il servizio oggetto della procedura di gara sia svolto da un operatore economico in possesso delle risorse umane e tecniche, nonché dell'esperienza necessaria per eseguire l'affidamento con un adeguato *standard* di qualità.

Tale requisito risulta attinente e proporzionato all'oggetto dell'appalto che, come dettagliatamente indicato nella documentazione di gara ed in particolare all'interno del "Capitolato speciale e obblighi contrattuali", richiede la gestione integrata e coordinata di un processo di adeguamento alla normativa NIS2 in favore di un soggetto NIS classificato come «importante» ai sensi del D.Lgs. 138/2024, qual è la CSEA, e si sostanzia, quindi, nello svolgimento di attività che, per loro natura, richiedono una gestione progettuale di adeguata ampiezza, con coinvolgimento multidisciplinare di competenze tecniche, giuridiche e organizzative, e con un livello di responsabilità professionale commisurato alla criticità della Stazione Appaltante.

Ne consegue, pertanto, che il valore economico di ciascuno dei contratti analoghi richiesti, pari almeno ad euro 50.000,00 (cinquantamila/00), risulti necessario per garantire che gli operatori economici partecipanti abbiano la capacità di sostenere interventi caratterizzati da un livello di complessità, impiego di risorse, articolazione organizzativa, e profondità di intervento, analoghi a quelli del presente affidamento, a cui corrisponde inevitabilmente una contropartita in termini economici.

In altri e più chiari termini, la CSEA ha valutato che contratti analoghi d'importo inferiore ad euro 50.000,00 (cinquantamila/00) non possano ritenersi strutturalmente idonei a documentare l'esposizione dell'operatore economico ad una complessità progettuale analoga a quella dell'affidamento in oggetto, ciò in quanto il valore economico di un incarico di consulenza regolatoria è, per i servizi intellettuali, il riflesso diretto del volume di attività svolte, del numero e della *seniority* delle risorse impiegate, della durata dell'intervento e dell'ampiezza delle tematiche presidiate.

Sul punto si precisa, inoltre, che la disciplina in materia di sicurezza delle reti e dei sistemi informativi non costituisce un ambito di recente introduzione, essendo stata oggetto di regolazione con la Direttiva (UE) 2016/1148 (c.d. Direttiva NIS) del 6 luglio 2016 e recepita nell'ordinamento italiano con

il decreto legislativo 18 maggio 2018, n. 65. Successivamente, il quadro normativo è stato aggiornato con la Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2), recepita nell'ordinamento nazionale con il decreto legislativo 4 settembre 2024, n. 138.

Pertanto, considerato che il periodo di riferimento per la verifica del requisito di capacità tecniche e professionali richiesto, è di dieci anni antecedenti alla data di pubblicazione della presente procedura, si ritiene che il requisito in parola possa agevolmente essere posseduto da parte di operatori economici dotati di effettiva competenza specialistica nel settore della cybersicurezza e della compliance regolatoria.

Si ricorda, infine, che la vigente disciplina in materia di contratti pubblici prevede, proprio in ottica pro-concorrenziale e di correlato sostegno alle piccole e medie imprese, gli istituti dell'avvalimento, ai sensi dell'art. 104 del D. Lgs. 36/2023, e del Raggruppamento temporaneo d'impresa, ai sensi dell'art. 68 del Codice.

Alla luce di quanto sopra, pertanto, non si ritiene di modificare il requisito di capacità tecniche e professionali previsto dalla *lex specialis* di gara.

Domanda n. 16

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.12; Argomento: f) Gestione degli asset. Definizione e prima redazione dell'inventario degli apparati fisici, dei software, dei sistemi e dei servizi che compongono i sistemi informativi e di rete, inclusi i servizi erogati da terze parti, ivi inclusi i servizi cloud.

Domanda: Si chiede di confermare che il fornitore dovrà occuparsi di compilare l'inventario degli asset del Cliente e in caso affermativo si chiede di specificare il livello di dettaglio atteso per tale inventario.

Risposta n. 16

Si conferma che l'attività di predisposizione dell'inventario degli asset è in capo al Fornitore, ferma restando la disponibilità di CSEA mettere a disposizione la documentazione già disponibile al riguardo.

Il livello di dettaglio richiesto dovrà essere coerente con gli obblighi di compliance applicabili, con particolare riferimento alla normativa NIS2, nonché allineato alle best practice di settore in materia di asset management e sicurezza delle informazioni.

Domanda n. 17

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.12; Argomento: h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi

- Definizione e redazione del piano di continuità operativa, del piano di ripristino in caso di disastro e del piano per la gestione delle crisi informatiche per almeno i sistemi informativi e di rete rilevanti
- Definizione e redazione delle politiche e procedure di revisione ed aggiornamento dei piani di cui al punto precedente;

Domanda: Si richiede se sono già stati definiti i requisiti di continuità e ripristino, redigendo una BIA eventualmente consultabile in fase di definizione dei piani di continuità. Si richiede inoltre se è già disponibile in termini di infrastruttura e servizi una soluzione di DR da descrivere nel piano richiesto.

Risposta n. 17

Si conferma che, nell'ambito delle certificazioni ISO in possesso della CSEA, è già stata condotta una Business Impact Analysis (BIA), che potrà costituire base di riferimento per le attività oggetto dell'appalto, fermo restando che la stessa potrà richiedere attività di revisione e integrazione nell'ambito delle prestazioni richieste.

Con riferimento alla disponibilità di soluzioni infrastrutturali e di servizi di Disaster Recovery, si rappresenta che le informazioni di dettaglio, a tutela della CSEA, saranno rese disponibili esclusivamente all'aggiudicatario, previa sottoscrizione di appositi accordi di riservatezza (NDA).

Domanda n. 18

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.15; Argomento: 1. Assetto procedurale e organizzativo
Prima esecuzione delle attività periodiche previste (ad esempio: redazione di elenchi ed inventari, valutazione del rischio, individuazione delle forniture critiche, etc.).

Domanda: Si chiede di fornire maggiore dettaglio sull'entità dell'attività prevista e sul dettaglio richiesto nell'eventuale compilazione delle attività periodiche previste dalla normativa NIS.

Risposta n. 18

Si precisa che l'entità delle attività previste è quella necessaria a garantire la piena conformità ai requisiti della normativa NIS, sia con riferimento alla prima redazione degli elaborati richiesti, sia con riferimento alla definizione delle procedure per il loro aggiornamento periodico.

Il livello di dettaglio atteso dovrà pertanto risultare adeguato a soddisfare gli obblighi normativi applicabili, nonché coerente con le best practice di settore in materia di gestione della sicurezza delle informazioni e della cybersicurezza.

Domanda n. 19

Documento: CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI; Paragrafo: 3.2 Linee di azione e risultati attesi; PAG.15; Argomento: 2. Formazione; Domanda: Si chiede di fornire il numero di sessioni richiesto.

Risposta n. 19

Si precisa che il numero di sessioni richiesto è da intendersi pari, almeno, a quello necessario a garantire la conformità ai requisiti previsti dalla normativa NIS2.

Resta altresì inteso che dovrà essere assicurato un livello di formazione adeguato e coerente con le best practice di settore, anche sulla base delle evidenze e dei fabbisogni che emergeranno nel corso dell'esecuzione delle attività.