Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber degli Organi Costituzionali e di rilievo Costituzionale, delle Agenzie Fiscali e delle Amministrazioni facenti parte del Nucleo per la cybersicurezza a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity"

M1C1I1.5

ALLEGATO B - PIANO DI PROGETTO

Sezione 1 – ANAGRAFICA

Titolo del progetto	Maturità e Resilienza cyber dell'Agenzia del Demanio
Progetto già avviato o in corso di attivazione ***(in conformità a quanto previsto al par. 4 dell'Avviso, purché avviato a decorrere dal 1° febbraio 2020)***	SI ☐ indicare data di stipula_____ e CIG del/dei contratto/i _____ *Oppure* indicare riferimenti (es. determina di aggiudicazione, prot. invio Piano dei Fabbisogni) _____ NO☒
(in caso di progetto da avviare ex novo) **Tempistiche previste per l'avvio del progetto**	10 gg. lavorativi
Data di ultimazione dell'intervento prevista, nel rispetto del target M1C1-9 o M1C1-19 ***(indicare in GG dalla data di sottoscrizione dell'Atto d'Obbligo)***	Entro il 30/11/2022 L'esecuzione delle attività progettuali sarà perfezionata entro il termine di 180 gg solari. Nel termine indicato sono comprese anche le attività di gestione amministrativa funzionali al quietanziamento delle spese e di rendicontazione

1A. Dati identificativi del Soggetto proponente	
Denominazione	Agenzia del Demanio
CF/P.IVA	06340981007
sede legale (*indicare Via/Piazza, n civico e cap.)*	Via Barberini, 38 00187
posta elettronica certificata (PEC)	AgenziaDemanio@pce.agenziademanio.it

1B. Dati identificativi del titolare del potere di impegnare il Soggetto/legale rappresentante	
Nome e Cognome	Alessandra Dal Verme
CF	[redacted]
Nato a	[redacted]
Residente in (*indicare Via/Piazza, n civico e cap.)*	Via Barberini, 38 00187

1C. Dati identificativi del Responsabile del Progetto	
Nome e Cognome	Massimo Bollati
CF	[redacted]
Nato a	[redacted]

Residente in (*indicare Via/Piazza, n civico e cap.)*	Uff. Via Barberini 38, 00187 Roma
Indirizzo e-mail	massimo.bollati@agenziademanio.it
Numero di telefono	0642367243

Sezione 2 – ORGANIZZAZIONE E CAPACITA' AMMINISTRATIVA DEL SOGGETTO ATTUATORE

2A. Descrizione e dimensionamento delle strutture coinvolte nella gestione, attuazione e controllo dell'intervento, facendo eventualmente riferimento anche alle attività affidate in outsourcing
Max 150 parole

Il progetto sarà gestito da una struttura appositamente costituita all'interno della Direzione Trasformazione Digitale, che avrà il compito di coordinare le attività interne ed esterne e monitorare l'avanzamento.
Le attività in outsourcing saranno affidate a Sogei SPA, società in house del MEF che metterà in campo oltre alle competenze specifiche anche figure di supporto direzionale con esperienze pregresse nell'ambito di progetti finanziati dalla EU.

2B. Descrizione degli elementi utili a garantire la capacità amministrativa del soggetto attuatore
Max 150 parole

L'Agenzia del Demanio, sia avvalendosi delle strutture interne deputate alla gestione dei contratti, sia in virtù della partnership vigente con la Sogei SpA (anche ai sensi di quanto previsto dalla convenzione tra MEF e Agenzia del Demanio 2020-2022), è in grado di avviare le attività operative del progetto entro 15 giorni dalla comunicazione dell'ammissione a finanziamento del piano di progetto in questione.

Sezione 3 – DESCRIZIONE DELL'INTERVENTO

3A. Descrizione dell'ambito di esecuzione dell'intervento (es. descrizione del sistema informatico di riferimento e della struttura organizzativa)
Max 150 parole

L'Agenzia del Demanio ha come mission la gestione, razionalizzazione/valorizzazione del patrimonio immobiliare dello Stato, amministrando un portafoglio di circa 43.000 beni. L'Agenzia sta portando avanti un percorso di trasformazione digitale, attraverso l'adozione di un modello organizzativo orientato a una forte trasversalità e integrazione tra diverse unità organizzative, mirato allo sviluppo di soluzioni e servizi digitali smart e innovativi in una logica di security-by-design. Si è dotata nel tempo di elevate competenze interne in ambito tecnologico, sviluppando ed eroga in autonomia servizi applicativi, anche rivolti alle PPAA, che digitalizzano, in tutto o in parte, alcuni processi di business legati al mondo degli interventi di valorizzazione, razionalizzazione degli spazi e ristrutturazione/ricostruzione degli immobili pubblici. Su tale perimetro si propone l'intervento in oggetto, avente lo scopo di migliorare le metodologie di sviluppo e migliorare la prevenzione e le risposte ad attacchi e/o incidenti cyber al fine di proteggere i dati, vero asset strategico del Paese.

3B. Descrizione delle criticità della postura di sicurezza indirizzate
Max 150 parole

Le scoperture di sicurezza che si intende risolvere con l'esecuzione del progetto proposto riguardano:

L'assenza di

a. un approccio sistematico all'analisi/miglioramento/potenziamento dei processi di gestione del rischio cyber;
b. un sistema organico (ruoli/policy/processi) che, partendo dalla data classification, permetta di valutare il livello di rischio dell'informazione e adottare le conseguenti misure di protezione;
c. processi/metodologie di security-by-design e sviluppo sicuro che consentano ai team di sviluppo interni dell'Agenzia e ai Fornitori, la realizzazione di applicativi con un livello di sicurezza adeguato al rischio assegnato;

Il miglioramento

d. dei processi di gestione delle vulnerabilità e degli incidenti cyber al fine di potenziare la capacità preventiva di protezione e la capacità reattiva in caso di attacchi cyber;
e. della consapevolezza del personale rispetto al rischio cyber.

Tali elementi rivestono una elevata criticità e urgenza stante il percorso di transizione al digitale intrapreso dall'Agenzia caratterizzato dall'esposizione di servizi ai diversi stakeholder (cittadini/imprese/altre amministrazioni).

3C. Descrizione degli obiettivi dell'intervento e dell'impatto in termini di potenziamento della resilienza cyber, ed in particolare in riferimento:

- adozione di misure e controlli di sicurezza
- supportare il processo di transizione digitale

Max 250 parole

Il progetto si pone l'obiettivo di migliorare il livello di maturità e di resilienza cyber dell'Agenzia attraverso la definizione di un sistema organico di gestione della sicurezza che consenta la valutazione e protezione dei propri asset informativi.

In pratica si intende sviluppare un sistema organico (ruoli/policy/processi) che consenta di:

- Definire ruoli/responsabilità in tema di gestione della sicurezza, nonché identificare gli owner degli asset informativi;
- Identificare/classificare i propri asset informativi, sulla base di una condivisa data classification;
- Realizzare un approccio integrato all'analisi del rischio finalizzata a gestire i rischi di violazione della Riservatezza, Integrità e Disponibilità (RID) dei dati anche in vista di una migrazione al cloud degli applicativi dell'Agenzia;
- Adottare/implementare metodologie di Security & Privacy by design per uno sviluppo sicuro finalizzato a incrementare l'affidabilità e solidità dei sistemi applicativi;
- Migliorare l'individuazione/protezione delle vulnerabilità dei sistemi e la capacità di prevenire e rispondere tempestivamente ad eventuali attacchi e/o incidenti cyber;
- Aumentare la consapevolezza al rischio cyber per il personale dell'Agenzia.

Gli interventi previsti nel progetto saranno realizzati in conformità con la normativa di settore e in particolare facendo riferimento al "Framework Nazionale per la cyber security e la data protection", alla norma ISO 27001 in vigore e agli altri standard europei e internazionali applicabili.

L'intervento progettuale di cybersecurity si pone alla base del processo di transizione al digitale intrapreso dall'Agenzia che, in linea con il piano triennale per l'informatica nella PA, sta ridisegnando il proprio sistema informativo in termini di architetture applicative/tecnologiche/riscrittura degli applicativi nell'ottica della migrazione in cloud.

3D. Descrizione dei contenuti operativi e delle attività previste
Max 150 parole

L'attività è finalizzata alla definizione dell'organizzazione, dei processi/procedure per una gestione sistematica delle tematiche afferenti la sicurezza informatica; sono previste le seguenti attività:

1. Pianificazione e controllo del progetto: Definizione del piano di progetti e dei relativi SAL.
2. Definizione ambito del progetto: consolidamento obiettivi/finalità/perimetro dell'intervento.
3. Realizzazione Assessment As-Is: l'assessment verrà effettuato utilizzando come quadro di riferimento il "Framework Nazionale di Cybersecurity e Data Protection", la norma ISO 27001 ed eventuali standard internazionali.
4. Gap analysis: definizione livello di maturità e livello di conformità rispetto alla norma ISO 27001. Saranno evidenziati i punti di forza e di debolezza, aree di intervento e relativo piano di lavoro.

5. Sviluppo processi/procedure: progettazione/documentazione di processi, procedure/politiche secondo quanto previsto nel piano di lavoro operativo. Rilascio progressivo dei prodotti alle diverse milestone per consentire verifica/consolidamento degli stessi.
6. Formazione del personale: pianificazione ed erogazione della formazione al personale dell'Agenzia.
7. Preparazione per avvio in esercizio.
8. Rendicontazione spese/milestone/target/intervento.

3E. Descrizione delle modalità attuative ovvero delle modalità amministrative per la realizzazione delle attività

Max 150 parole

Il cronoprogramma del progetto è stato organizzato in termini di contenuti/timing/organizzazione per garantire il termine delle attività entro il 30/11/2022.

A tal proposito, in forza di un contratto esistente, verrà impiegato un fornitore esperto nelle tematiche della cybersecurity e ciò consentirà di ridurre drasticamente i tempi di selezione dei fornitori.

Le attività operative sono state ipotizzate in modo da rafforzare la condivisione delle informazioni per ridurre i tempi di rework e massimizzare l'efficacia dei prodotti rilasciati.

Sono stati ipotizzati SAL periodici (di norma quindicinali, ma potrebbero essere anche settimanali nel caso di eventuali issues) al fine di prevenire e gestire tempestivamente gli eventuali impatti negativi sul progetto.

E' stata definita una governance del progetto che vede il coinvolgimento delle strutture apicali della Direzione transizione al digitale per intervenire con tempestività nella pianificazione, controllo e implementazione del progetto e delle eventuali azioni correttive.

Le attività di Formazione/Avvio/Rendicontazioni sono programmate in parallelo per consentire il termine del progetto entro il 30/11/2022.

Sezione 4 – QUADRO FINANZIARIO

In riferimento al paragrafo n. 5.2 "Spese ammissibili" dell'Avviso pubblico recante "Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber degli Organi Costituzionali e di rilievo Costituzionale, delle Agenzie Fiscali e delle Amministrazioni facenti parte del Nucleo per la cybersicurezza a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5", nella presente sezione, devono essere riportate le spese ammissibili.

Si precisa che le spese, per risultare comprovate ed ammissibili, devono:

- essere comprovate da fatture interamente quietanzate emesse, per il tramite di bonifico bancario o postale ovvero con altri strumenti di incasso o di pagamento idonei a consentire la piena tracciabilità delle operazioni (L. 136/2010, art. 3, comma 1 e 3 e successive modificazioni);
- essere coerenti e pertinenti con le finalità dell'intervento 1.5, Missione M1C1
- essere ammissibile ai sensi della normativa nazionale e europea di riferimento vigente: Reg. (UE) 2021/241, Circolari RSG, Reg. (UE) 2021/1060, DPR nr. 22 del 5 febbraio 2018.

Il finanziamento concesso con il presente Avviso è cumulabile con altri finanziamenti a valere su programmi e strumenti dell'Unione europea, a condizione che gli stessi non interessino i medesimi costi in applicazione del principio di addizionalità di cui all'art.9 del Regolamento (UE) 2021/241. Nel caso in cui l'intervento sia stato avviato con una diversa copertura finanziaria, all'atto della sottoscrizione della Convenzione di finanziamento il Soggetto attuatore dovrà formalmente dimostrare di aver rinunciato al precedente finanziamento, ove questo sia riferito ai medesimi costi per cui si chiede il contributo a valere sul PNRR.

Si fornisce di seguito un dettaglio delle tipologie di spese ammissibili, a titolo esemplificativo e non esaustivo:

- spese per servizi di consulenza per l'implementazione degli interventi progettuali ammissibili secondo indicazioni di cui alla circolare RGS n. 4/2021, incluse attività di formazione specifica;
- spese per la progettazione, lo sviluppo e l'implementazione di software specifici;
- spese per l'acquisto di hardware, software;
- spese per l'acquisizione di servizi per l'implementazione degli interventi progettuali (es: sviluppo software; servizi di connettività; analisi, studi, ecc);
- spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale nella misura pari al 7% di costi diretti ammissibili ai sensi dell'art. 54 lett. a del Reg. (UE) 2021/1060.

4A. Indicazione e descrizione delle **risorse finanziarie** necessarie alla realizzazione del progetto_____, per ogni macro-attività

Compilare gli elementi e la tabella sottostante (è possibile aggiungere righe alla tabella)

COSTO COMPLESSIVO DEL PROGETTO_____: _____284.600 €

CONTRIBUTO RICHIESTO (fino a € _____): _____284.600€

DESCRIZIONE DI ALTRE FONTI DI FINANZIAMENTO UTILIZZATE PER LA REALIZZAZIONE DEL PROGETTO (se previste):

Compilare la seguente tabella selezionando le tipologie di investimento previste *(rif. Paragrafo 4.1 dell'avviso)* aggiungendo se necessarie ulteriori righe per le attività, dettagliando il contributo finanziario richiesto:

DESCRIZIONE	€ (netto)	€ (IVA)	Data inizio	Data fine
1.analisi della postura di sicurezza e piano di potenziamento *(max euro 300.000,00)*	37.704,00 €	46.000,00 €	Q2 2022	Q3 2022
1.Pianificazione e controllo del progetto	6.557,00 €	8.000,00 €		
2.Definizione ambito del progetto	4.918,00 €	6.000,00 €		
3.Realizzazione Assessment As IS	16.393,00 €	20.000,00 €		
4.Gap analysis	9.836,00 €	12.000,00 €		
2.miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	93.443,00 €	114.000,00 €	Q3 2022	Q4 2022
5.Sviluppo processi /procedure	93.443,00 €	114.000,00 €		
3. miglioramento della consapevolezza delle persone	9.836,00 €	12.000,00 €	Q4 2022	Q4 2022
7.Formazione del personale	9.836,00 €	12.000,00 €		
4. progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	77.049,00 €	94.000,00 €	Q3 2022	Q4 2022
6.Attivazione strumenti applicativi	65.574,00 €	80.000,00 €		
8.preparazione avvio in esercizio	6.557,00 €	8.000,00 €		
9.Rendicontazione	4.918,00 €	6.000,00 €		

DESCRIZIONE	€ (netto)	€ (IVA)
Spese Generali	15.262,24 €	- €

Sezione 5 – CRONOPROGRAMMA

5A. Indicazione e descrizione del **cronoprogramma delle attività** di implementazione del progetto

Compilare la tabella sottostante (è possibile aggiungere righe alla tabella)

Tipologie di investimento *(rif. Paragrafo 4.1 dell'avviso)*	Attività (breve descrizione)	Data di inizio prevista (es. Q3 2022)	Data di fine prevista (es. Q4 2022)	Durata espressa in gg
2) miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	1. Pianificazione e controllo del progetto	Q3 2022	Q3 2022	10 gg solari
	2. Definizione ambito del progetto	Q2 2022	Q2 2022	10 gg solari
	3. Realizzazione Assessment As-Is	Q2 2022	Q2 2022	30 gg solari
	4. Gap analysis	Q2 2022	Q3 2022	20 gg solari
	5. Sviluppo processi/procedure	Q3 2022	Q4 2022	110 gg solari
	6. Attivazione strumenti applicativi	Q3 2022	Q4 2022	110 gg solari
	7. Formazione del personale	Q4 2022	Q4 2022	20 gg solari
	8. Preparazione avvio in esercizio	Q4 2022	Q4 2022	20 gg solari
	9. Rendicontazione	Q4 2022	Q4 2022	20 gg solari