Funded by the European Union
NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

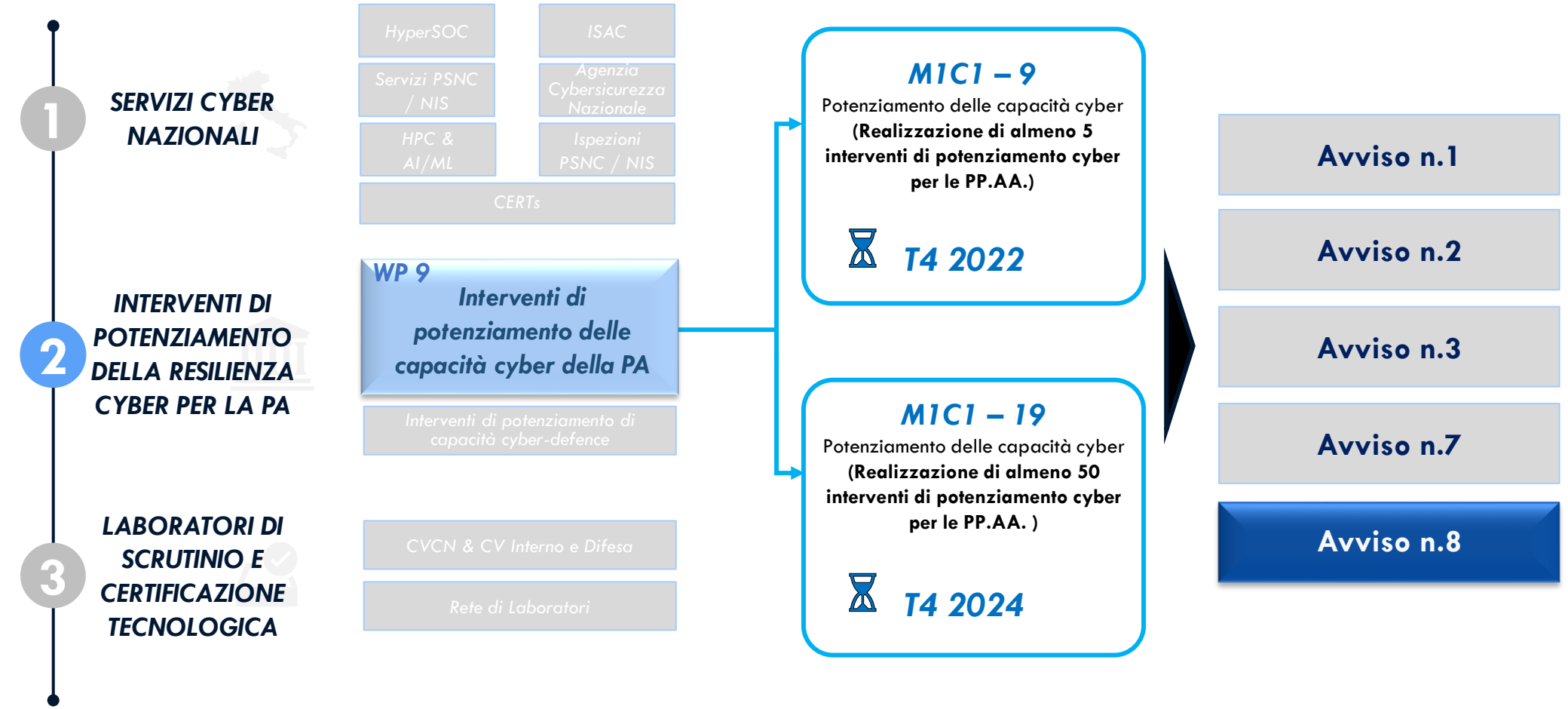
PNRR – M1C1 – Investimento 1.5 "Cybersecurity"

Interventi di potenziamento cyber per la PA:
Avviso Pubblico n. 08/2024

Roma, 11/03/2024

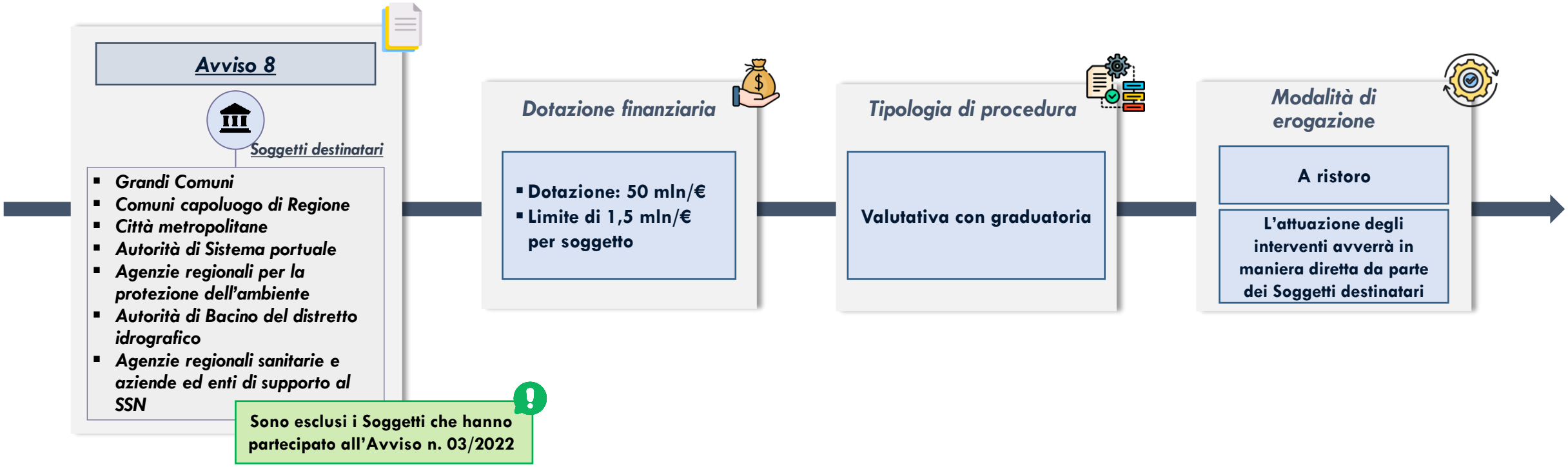
Contesto di riferimento

Per l'attuazione degli **interventi di potenziamento delle capacità cyber della PA** e il perseguimento dei relativi Target previsti dal PNRR, la strategia adottata dall'Agenzia per la Cybersicurezza Nazionale ha previsto l'individuazione e la selezione di progetti da finanziare mediante procedure ad evidenza pubblica rivolte alle Pubbliche Amministrazioni:



Avviso pubblico n. 08/2024

Al fine di concorrere all'obiettivo di **irrobustire le infrastrutture e i servizi digitali del Sistema Paese nonché migliorare le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza,** l'Agenzia per la Cybersicurezza Nazionale intende pubblicare **una procedura ad evidenza pubblica** rivolta alle Pubbliche Amministrazioni.



Soggetti destinatari e obiettivi

L'Agenzia ha individuato quali Soggetti destinatari dell'Avviso **105 PA**, appartenenti alle categorie sotto elencate, con l'obiettivo di incrementare la **sicurezza e l'efficienza dei servizi erogati dalle Pubbliche Amministrazioni** nei relativi ambiti territoriali, nonchè al fine di contribuire alla realizzazione degli **obiettivi descritti dal PNRR** di **sostenibilità ambientale** e di **transizione verso la cosiddetta "sanità digitale"**.

Grandi Comuni*, Comuni capoluogo di Regione e Città metropolitane

Incrementare la **sicurezza e l'efficacia dei nuovi servizi digitali** offerti dalle PA, promuovendone l'utilizzo sulla base di una rinnovata **fiducia da parte dei cittadini**

Autorità di Bacino del distretto idrografico

Favorire la **sostenibilità ambientale**, ivi incluso il **miglioramento dell'efficienza dell'infrastruttura idrica**

Autorità di Sistema portuale

Incrementare **sicurezza ed efficacia** del **servizio reso** negli ambiti territoriali di competenza, mediante un processo di efficientamento dei sistemi informatici

Agenzie regionali per la protezione dell'ambiente

Favorire la **sostenibilità ambientale** e l'aumento dei livelli di **tutela dell'ambiente**, al fine di raggiungere una **transizione ecologica** che è alla base del nuovo modello di sviluppo italiano ed europeo

Agenzie regionali sanitarie e aziende ed enti di supporto al SSN

Promuovere la transizione verso la "**sanità digitale**", garantendo la conservazione e l'accesso sicuro ai dati clinici, nonchè disponibilità e resilienza dei servizi offerti, per **offrire in maniera sicura assistenza sanitaria ai cittadini**

*Comuni italiani con una popolazione residente superiore a 100.000 abitanti, così come individuati dal censimento ISTAT della popolazione residente al 1° gennaio 2023, non già beneficiari di finanziamento relativamente all'Avviso n. 03/2022

Caratteristiche del progetto da presentare – (1/6)

I Soggetti destinatari possono presentare **una sola proposta progettuale** – in caso di proposte multiple sarà considerata ammissibile l'ultima proposta pervenuta in ordine cronologico. I progetti dovranno concludersi entro il **31 dicembre 2025**.

Interventi

I progetti potranno prevedere uno o più dei seguenti interventi:

1. *Governance e programmazione cyber*
2. *Gestione del rischio cyber e della continuità operativa*
3. *Gestione e risposta agli incidenti di sicurezza*
4. *Gestione delle identità digitali e degli accessi logici*
5. *Sicurezza delle applicazioni, dei dati e delle reti*

Tipologie di intervento

Per ciascun possono essere presentate attività riconducibili a una o più delle seguenti tipologie di intervento:

a. *Analisi della postura di sicurezza e definizione di un piano di potenziamento*
b. *Miglioramento dei processi e dell'organizzazione*
c. *Formazione e miglioramento della consapevolezza delle persone*
d. *Progettazione e sviluppo di nuovi sistemi e tecnologie*

Caratteristiche del progetto da presentare – (2/6)

A titolo meramente esemplificativo, si rappresentano, nell'ambito di ciascun intervento, alcune delle attività che possono essere realizzate per ogni tipologia di intervento.

INTERVENTO 1 - Governance e programmazione cyber

Coordinamento, supervisione e gestione olistica e integrata della cybersecurity attraverso la programmazione strategica di investimenti e iniziative

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

- Analisi di dettaglio e definizione di un programma evolutivo in termini di processi, organizzazione e tecnologie cyber

B. Miglioramento dei processi e dell'organizzazione

- Definizione modello organizzativo struttura cyber

C. Formazione e miglioramento della consapevolezza delle persone

- Formazione e certificazioni specialistiche
- Promozione ed esecuzione di iniziative di *cyber culture*
- Svolgimento di simulazioni e campagne di *awareness* a tema *cyber* (es. simulazione attacco di *phishing*)

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

- Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. GRC, asset inventory, piattaforma e-learning)

Caratteristiche del progetto da presentare – (3/6)

A titolo meramente esemplificativo, si rappresentano, nell'ambito di ciascun intervento, alcune delle attività che possono essere realizzate per ogni tipologia di intervento.

INTERVENTO 2 - *Gestione del rischio cyber e della continuità operativa*

Individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito cyber, e implementazione di un piano volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

- Valutazione del rischio su *asset* in perimetro
- *Business Impact Analysis* su servizi in perimetro

B. Miglioramento dei processi e dell'organizzazione

- Definizione metodologia di valutazione del rischio
- Definizione processo *backup & restore*

C. Formazione e miglioramento della consapevolezza delle persone

- Formazione e certificazioni specialistiche e di prodotto

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

- Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. strumenti di *backup, security ratings, cyber threat intelligence*)

Caratteristiche del progetto da presentare – (4/6)

A titolo meramente esemplificativo, si rappresentano, nell'ambito di ciascun intervento, alcune delle attività che possono essere realizzate per ogni tipologia di intervento.

INTERVENTO 3 - *Gestione e risposta agli incidenti di sicurezza*

Monitoraggio, identificazione e gestione degli incidenti cyber, e ripristino dei sistemi impattati

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

- *Red Teaming*

B. Miglioramento dei processi e dell'organizzazione

- Definizione processo di gestione degli incidenti *cyber*
- Definizione processo di gestione dei log
- Definizione di *playbook* per la risposta a incidenti *cyber* noti

C. Formazione e miglioramento della consapevolezza delle persone

- *Table Top Exercise*
- Formazione e certificazioni specialistiche e di prodotto

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

- Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *SIEM*, *SOAR*, *Case Management*)

Caratteristiche del progetto da presentare – (5/6)

A titolo meramente esemplificativo, si rappresentano, nell'ambito di ciascun intervento, alcune delle attività che possono essere realizzate per ogni tipologia di intervento.

INTERVENTO 4 - *Gestione delle identità digitali e degli accessi logici*

Governo delle identità e definizione dei permessi di accesso alle risorse al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di *"need to know"*, *"least privilege"* e *"segregation of duties"*

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

- Valutazione e *hardening* della postura di sicurezza di *Active Directory*

B. Miglioramento dei processi e dell'organizzazione

- Definizione processo di gestione delle identità e degli accessi ai sistemi informativi

C. Formazione e miglioramento della consapevolezza delle persone

- Formazione e certificazioni specialistiche e di prodotto

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

- Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *IAM*, *PAM*, *IGA*, *MFA*)

Caratteristiche del progetto da presentare – (6/6)

A titolo meramente esemplificativo, si rappresentano, nell'ambito di ciascun intervento, alcune delle attività che possono essere realizzate per ogni tipologia di intervento.

INTERVENTO 5 - *Sicurezza delle applicazioni, dei dati e delle reti*

Protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati riservati, al fine di prevenire l'occorrenza di potenziali incidenti cyber e ridurne gli impatti

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

- *VA/PT*
- Verifica e rafforzamento delle configurazioni di sicurezza perimetrale e monitoraggio

B. Miglioramento dei processi e dell'organizzazione

- Analisi e reingegnerizzazione di reti e architetture
- Definizione processo di *security by design*
- Definizione processo di sviluppo sicuro codice
- Definizione processo di gestione delle vulnerabilità

C. Formazione e miglioramento della consapevolezza delle persone

- Formazione e certificazioni specialistiche e di prodotto

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

- Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *firewall*, *WAF*, *anti-DDoS, DLP*)

Focus: Caratteristiche dell'Avviso – (1/3)

Per chiarimenti e/o informazioni : pnrr-cybersecurity@acn.gov.it*

1. Modalità di partecipazione e requisiti

1. I Soggetti sopra individuati potranno **partecipare all'Avviso esclusivamente in forma singola.** Non sono ammesse partecipazione in forma consortile o in associazione
2. Ciascun Soggetto partecipante potrà presentare un solo progetto finalizzato all'**analisi** e al **potenziamento** delle **proprie capacità di resilienza cyber in termini di postura di sicurezza, processi e modello organizzativo, competenze** e, infine, **sistemi e tecnologie abilitanti.**
3. I Soggetti interessati dovranno presentare la Domanda di partecipazione entro le ore 18:00 del 25/03/2024, tramite l'invio di Posta Elettronica Certificata (PEC) all'indirizzo: ***pnrr@pec.acn.gov.it***

2. Criteri di Ammissibilità

1. **possesso delle competenze, risorse e qualifiche professionali,** sia tecniche che amministrative, idonee a garantire la realizzazione del progetto
2. **aver adottato misure volte a garantire il rispetto del principio di sana gestione finanziaria,** come disciplinato nel Regolamento finanziario (UE, Euratom) 2018/1046 e dall'articolo 22 del Regolamento (UE) 2021/241
3. in caso di progetto da avviare ex novo, **aver generato un Codice Unico di Progetto (CUP)** in coerenza con le indicazioni di cui al Template CUP "PNRR M1C1 – 1.5 – Cybersecurity", codice 2204007

*Le richieste di chiarimento dovranno pervenire entro i 10 giorni precedenti la chiusura dei termini di presentazione delle domande di partecipazione.

Focus: Caratteristiche dell'Avviso – (2/3)

Per chiarimenti e/o informazioni : pnrr-cybersecurity@acn.gov.it

3. Requisiti minimi di progetto

1. **essere coerente e pertinente con le finalità individuate dal presente Avviso** e, in particolare, in linea con gli obiettivi di cui al target M1C1-19 (target finale UE) "*Supporto all'aggiornamento delle misure di sicurezza T2 - 50 strutture di sicurezza adeguate entro dicembre 2024*";
2. **avere ad oggetto investimenti per il potenziamento (e non la conduzione) delle capacità cyber** del Soggetto attuatore dell'intervento e la cui stima economica sia proporzionale agli obiettivi e ai target della milestone intercettata;
3. **riguardare interventi da realizzare ex novo** oppure il **completamento di progettualità avviate dal 1° febbraio 2021** e non concluse alla data di presentazione della candidatura;
4. **non aver beneficiato di altre forme di finanziamento pubblico** da parte del Dispositivo RRF e/o di altri Programmi dell'Unione;
5. **avere ad oggetto informazioni a cui non sono attribuite classifiche di segretezza,** ai sensi della legge 124/2007.

Focus: Caratteristiche dell'Avviso – (3/3)

Per chiarimenti e/o informazioni : pnrr-cybersecurity@acn.gov.it

4. Documentazione componente l'Avviso

1. **Allegato A** – Domanda di ammissione corredata dall'Autodichiarazione relativa al rispetto dei principi previsti per gli interventi del PNRR (**sezione 1**) e dall'Autodichiarazione sul "Titolare effettivo" nell'ambito degli stessi (**sezione 2**)*
2. **Allegato B1** – Scheda di Progetto comprensiva del Quadro finanziario e del Cronoprogramma (**Allegato B2**)
3. **Allegato C** – Schema di Atto d'obbligo
4. **Allegato D** – Istruzioni operative per la generazione del CUP tramite Template Codice 2204007 PNRR M1C1 - 1.5 – Cybersecurity
5. **Allegato E** – Elenco dei Soggetti Attuatori ammessi

*La domanda di partecipazione, sottoscritta con firma digitale dal Legale rappresentante o da Soggetto delegato (con copia di atto di delega), da inviare alla casella PEC **pnrr@pec.acn.gov.it**, dovrà contenere, pena l'esclusione, l'Allegato A e gli Allegati B1 e B2 debitamente compilati.

Focus: Compilazione Quadro finanziario e Cronoprogramma

L'**Allegato B2** consiste in un file Excel composto da due fogli: il primo relativo al **Quadro finanziario** e il secondo relativo al **Cronoprogramma.** Una volta compilato, dovrà essere trasmesso **sia in formato Excel sia in formato PDF.**

1. Quadro finanziario

- **Tabella 1**: il Soggetto dovrà indicare il dettaglio preventivato dei costi per le attività progettuali, indicando per ciascuna di esse intervento e tipologia di intervento, categoria di costo e importo contributo richiesto.
- **Tabella 2:** si compilerà automaticamente sulla base delle informazioni inserite nella Tabella 1, fornendo una vista di sintesi dei contributi richiesti per ciascun intervento indicato.

2. Cronoprogramma

Dovranno essere indicate le attività progettuali previste, identificate ciascuna in relazione all'intervento e alla tipologia di intervento di riferimento, con l'indicazione, per ciascuna di esse, dei trimestri ("*quarter*") pianificati di inizio e fine.

Grazie

Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT