AVVISO PUBBLICO 7/2023

a sportello per l'erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa a valere sul

PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"

M1C1I1.5

INDICE

1 PREMESSA E OBIETTIVI DELL'AVVISO

L'Agenzia per la Cybersicurezza Nazionale (di seguito anche "*Agenzia*" o "*ACN*"), in qualità di Soggetto attuatore dell'Investimento 1.5 "Cybersecurity" – Missione 1 Componente 1 del PNRR, a titolarità della Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale (di seguito anche "DTD"), promuove il presente Avviso, finanziato dall'Unione Europea – Next Generation EU, per l'**erogazione di interventi di potenziamento e miglioramento delle capacità cyber della Pubblica Amministrazione.**

L'Avviso ha lo scopo di individuare, mediante **procedura a sportello,** i Soggetti destinatari di interventi volti a **irrobustire le infrastrutture e i servizi digitali del Sistema Paese nonché a migliorare le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza**, quale elemento fondante per la transizione digitale sicura della Pubblica Amministrazione.

Nello specifico, il presente dispositivo intercetta la **Misura #14** della Strategia Nazionale di Cybersicurezza, volta a **coordinare interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini**. Nel perseguimento dei suddetti obiettivi, in accordo alle regole ed ai principi trasversali individuati dal *framework* normativo di riferimento del PNRR, il presente Avviso costituisce una delle iniziative che l'Agenzia intende attuare per la selezione di **interventi cd. a titolarità**. L'attuazione degli interventi finanziati, difatti, avverrà in modalità diretta da parte dell'Agenzia a favore delle Pubbliche Amministrazioni Centrali individuate quali Soggetti destinatari.

In continuità con le azioni poste in essere dall'Agenzia e in linea con quanto previsto nel documento di indirizzo strategico - predisposto dall'Agenzia, sentito il DTD della Presidenza del Consiglio del ministri – recante la "*Strategia di finanziamento mediante Avvisi Pubblici*", il presente Avviso è finalizzato ad ampliare la platea di Soggetti destinatari ad un perimetro più ampio di Pubbliche Amministrazioni Centrali, come nel prosieguo individuate, rispetto a precedenti analoghe iniziative.

Il presente Avviso contribuisce al raggiungimento del traguardo e obiettivo dell'Investimento 1.5 relativo alla ***milestone* M1C1-19 (target finale UE) *"Supporto all'aggiornamento delle misure di sicurezza T2 - 50 strutture di sicurezza adeguate entro dicembre 2024"***

Il codice di investimento connesso all'intervento oggetto del presente Avviso è **M1C1 I1.5**.

1.1 Normativa di riferimento

La procedura di selezione e la realizzazione degli interventi finanziati a valere sul presente Avviso avverranno nel rispetto della seguente normativa:

- la legge 7 agosto 1990, n. 241, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*", e, in particolare, l'art. 12, secondo cui la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari e l'attribuzione di vantaggi economici di qualunque genere a persone ed Enti pubblici e privati sono subordinate alla predeterminazione da parte delle Amministrazioni procedenti, nelle forme previste dai rispettivi ordinamenti, dei criteri e delle modalità cui le amministrazioni stesse devono attenersi;
- il Regolamento di esecuzione (UE) n. 821/2014 della Commissione del 28 luglio 2014, recante modalità di applicazione del regolamento (UE) n. 1303/2013 del Parlamento europeo e del

Consiglio per quanto riguarda le modalità dettagliate per il trasferimento e la gestione dei contributi dei programmi, le relazioni sugli strumenti finanziari, le caratteristiche tecniche delle misure di informazione e di comunicazione per le operazioni e il sistema di registrazione e memorizzazione dei dati;

- il decreto legislativo 31 marzo 2023, n. 36, "*Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici*";
- il decreto del Presidente della Repubblica 5 febbraio 2018, n. 22, "*Regolamento recante i criteri sull'ammissibilità delle spese per i programmi cofinanziati dai Fondi strutturali di investimento europei (SIE) per il periodo di programmazione 2014/2020*";
- il Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i Regolamenti (UE) n. 1296/2013, n. 1301/2013, n. 1303/2013, n. 1304/2013, n. 1309/2013, n. 1316/2013, n. 223/2014, n. 283/2014 e la decisione n. 541/2014/UE e abroga il Regolamento (UE, Euratom) n. 966/2012;
- il decreto legislativo 18 maggio 2018, n. 65, "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*";
- il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, "*relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)"*;
- il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*";
- la Delibera del Comitato per la programmazione economica (CIPE) del 26 novembre 2020, n. 63, che introduce la normativa attuativa della riforma CUP;
- la legge 30 dicembre 2020, n. 178, recante *"Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023"* e, in particolare, l'articolo 1, comma 1042, ai sensi del quale con uno o più decreti da parte del Ministero dell'economia e delle finanze sono stabilite le procedure amministrativo-contabili per la gestione delle risorse di cui ai commi da 1037 a 1050, nonché le modalità di rendicontazione della gestione del Fondo di cui al comma 1037; il comma 1043 del medesimo articolo 1, ai sensi del quale al fine di supportare le attività di gestione monitoraggio, rendicontazione e controllo delle componenti del NGEU, il Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato sviluppa e rende disponibile un apposito sistema informatico;
- il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133"*;
- il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021 che istituisce il Dispositivo per la ripresa e la resilienza, come modificato dal Regolamento (UE) 435/23

rispetto all'inserimento di capitoli dedicati al piano REPowerEU nei Piani per la Ripresa e la Resilienza;

- il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*";
- il decreto-legge del 6 maggio 2021, n. 59, convertito, con modificazioni, dalla legge 1° luglio 2021, n. 101, recante "*Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti*";
- il decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, recante "*Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*" e, in particolare, l'articolo 8, ai sensi del quale ciascuna Amministrazione centrale titolare di interventi previsti nel PNRR provvede al coordinamento delle relative attività di gestione, nonché al loro monitoraggio, rendicontazione e controllo;
- il decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113, recante "*Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia*", che definisce percorsi veloci, trasparenti e rigorosi per il reclutamento di profili tecnici e gestionali necessari alle finalità del PNRR, tra cui la cybersicurezza;
- il Piano Nazionale di Ripresa e Resilienza (di seguito anche "PNRR") - presentato alla Commissione in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021 - e, in particolare, le indicazioni contenute relativamente al raggiungimento di Milestone e Target;
- il decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, recante "*Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale*";
- la Missione 1 "*Digitalizzazione, Innovazione, Competitività, Cultura e Turismo*", Componente 1 "*Digitalizzazione, Innovazione e Sicurezza della P.A.*", Investimento 1.5 "*Cybersicurezza*" del PNRR che prevede interventi per la digitalizzazione delle infrastrutture tecnologiche e dei servizi della P.A., rafforzando le difese cyber nazionali, mediante lo stanziamento complessivo di € 623.000.000,00 (seicentoventitrémilioni/00);
- gli ulteriori principi trasversali previsti dal paragrafo 5.2.1 del PNRR, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (c.d. tagging), il principio di parità di genere, l'obbligo di protezione e valorizzazione dei giovani e del superamento dei divari territoriali;
- il decreto del Ministro dell'economia e delle finanze del 6 agosto 2021, recante "*Assegnazione delle risorse finanziarie previste per l'attuazione degli interventi del Piano nazionale di ripresa e resilienza (PNRR) e ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione*", che individua il DTD della Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante *"Cybersicurezza"*;
- il Regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio del 18 giugno 2020, relativo all'istituzione di un quadro che favorisce gli investimenti sostenibili e recante modifica del

regolamento (UE) 2019/2088, e in particolare l'articolo 17, che definisce gli obiettivi ambientali, tra cui il principio del *"non arrecare un danno significativo"* (DNSH, "*Do no significant harm*"), e la Comunicazione della Commissione UE 2021/C 58/01, recante "*Orientamenti tecnici sull'applicazione del principio non arrecare danno significativo a norma del regolamento sul dispositivo per la ripresa e la resilienza*";

- il decreto del Presidente del Consiglio dei ministri del 15 settembre 2021, con il quale sono stati individuati gli strumenti per il monitoraggio del PNRR;
- il decreto ministeriale dell'11 ottobre 2021, recante "*Procedure relative alla gestione finanziaria delle risorse previste nell'ambito del PNRR di cui all'articolo 1, comma 1042, della legge 30 dicembre 2020, n. 178*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 14 ottobre 2021, n. 21, recante "*Piano Nazionale di Ripresa e Resilienza - Trasmissione delle Istruzioni tecniche per la selezione dei progetti PNRR*";
- il decreto-legge 6 novembre 2021, n. 152, convertito, con modificazioni, dalla legge 29 dicembre 2021, n. 233, recante "*Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, 30 dicembre 2021, n. 32, recante "*Piano Nazionale di Ripresa e Resilienza – Guida operativa per il rispetto del principio di non arrecare danno significativo all'ambiente (DNSH)*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 31 dicembre 2021, n. 33, recante "*Piano Nazionale di Ripresa e Resilienza (PNRR) - Nota di chiarimento sulla Circolare del 14 ottobre 2021, n. 21 - Trasmissione delle Istruzioni Tecniche per la selezione dei progetti PNRR - Addizionalità, finanziamento complementare e obbligo di assenza del c.d. doppio finanziamento*";
- il decreto del Presidente del Consiglio dei ministri 15 giugno 2021, recante "*Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 21 giugno 2022, n. 27, recante "*Piano Nazionale di Ripresa e Resilienza (PNRR) - Monitoraggio delle misure PNRR*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, del 18 gennaio 2022, n. 4, recante "*Piano Nazionale di Ripresa e Resilienza (PNRR) - articolo 1, comma 1, del decreto-legge n. 80 del 2021 - Indicazioni attuative*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 24 gennaio 2022, n. 6, recante "*Piano Nazionale di Ripresa e Resilienza (PNRR) – Servizi di assistenza tecnica per le Amministrazioni titolari di interventi e soggetti attuatori del PNRR*";

- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 10 febbraio 2022, n. 9, recante "*Piano Nazionale di Ripresa e Resilienza (PNRR) - Trasmissione delle Istruzioni tecniche per la redazione dei sistemi di gestione e controllo delle amministrazioni centrali titolari di interventi del PNRR*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 29 aprile 2022, n. 21, recante "*Piano nazionale di ripresa e resilienza (PNRR) e Piano nazionale per gli investimenti complementari - Chiarimenti in relazione al riferimento alla disciplina nazionale in materia di contratti pubblici richiamata nei dispositivi attuativi relativi agli interventi PNRR e PNC*";
- il decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79, recante "*Ulteriori modifiche urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, del 4 luglio 2022, n. 28, recante "*Controllo di regolarità amministrativa e contabile dei rendiconti di contabilità ordinaria e di contabilità speciale. Controllo di regolarità amministrativa e contabile sugli atti di gestione delle risorse del PNRR - prime indicazioni operative*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 26 luglio 2022, n. 29, recante "*Circolare delle procedure finanziarie PNRR*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, dell'11 agosto 2022, n. 30, recante "*Circolare sulle procedure di controllo e rendicontazione delle misure PNRR*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 2 gennaio 2023, n. 1, recante "*Controllo preventivo di regolarità amministrativa e contabile di cui al decreto legislativo 30 giugno 2011, n. 123. Precisazioni relative anche al controllo degli atti di gestione delle risorse del Piano Nazionale di Ripresa e Resilienza*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 13 marzo 2023, n. 10, recante "*Interventi PNRR. Ulteriori indicazioni operative per il controllo preventivo ed il controllo dei rendiconti delle Contabilità Speciali PNRR aperte presso la Tesoreria dello Stato*";
- la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 22 marzo 2023, n. 11, recante "*Registro Integrato dei Controlli PNRR – Sezione controlli milestone e target*";
- la Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di Implementazione (di seguito anche "Piano") che definiscono come pianificare, coordinare e attuare misure tese al potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente*;*
- l'Accordo tra l'Agenzia e il DTD del 14 dicembre 2021, di cui al prot. ACN n. 896 del 15 dicembre 2021, stipulato ai sensi dell'art. 15 della legge n. 241 del 1990 che, ai sensi dell'articolo 5, comma

6, del d.lgs. n. 50/2016, è escluso dall'ambito di applicazione del citato decreto legislativo n. 50, disciplinante lo svolgimento in collaborazione delle attività di realizzazione dell'"*Investimento 1.5*", registrato dalla Corte dei Conti il 18 gennaio 2022 al n. 95, così come modificato dall'atto aggiuntivo del 13 dicembre 2021, registrato dalla Corte dei Conti il 5 settembre 2023 al n. 2425.

1.2 Definizioni

Ai fini del presente Avviso, si intende per:

- **"Amministrazioni centrali titolari di interventi PNRR"**: Ministeri e strutture della Presidenza del Consiglio dei ministri responsabili dell'attuazione delle riforme e degli investimenti (ossia delle Misure) previsti nel PNRR che possono individuare Soggetti delegati per l'attuazione degli interventi;
- **"Avviso pubblico a sportello"**: Procedura prevista per la selezione dei Soggetti attuatori, che rispondono ai requisiti minimi di partecipazione, secondo l'ordine cronologico di presentazione delle Istanze di partecipazione, fino a concorrenza delle risorse disponibili;
- **"Cabina di regia del PNRR"**: Organo con poteri di indirizzo politico, impulso e coordinamento generale sull'attuazione degli interventi del PNRR;
- **"Componente"**: Elemento costitutivo o parte del PNRR che riflette riforme e priorità di investimento correlate ad un'area di intervento, ad un settore, ad un ambito, ad un'attività, allo scopo di affrontare sfide specifiche e si articola in una o più misure;
- **"CUP"**: Codice Unico di Progetto, vale a dire il codice che identifica un progetto d'investimento pubblico e strumento cardine per il funzionamento del Sistema di Monitoraggio degli Investimenti Pubblici;
- **"Milestone"**: Traguardo qualitativo da raggiungere tramite una determinata misura del PNRR (riforma e/o investimento), che rappresenta un impegno concordato con l'Unione europea o a livello nazionale (es. legislazione adottata, piena operatività dei sistemi IT, ecc.);
- **"Missione"**: Risposta, organizzata secondo macro-obiettivi generali e aree di intervento, rispetto alle sfide economiche-sociali che si intendono affrontare con il PNRR e articolata in Componenti. Le sei Missioni del Piano rappresentano aree "tematiche" strutturali di intervento (Digitalizzazione, innovazione, competitività e cultura; Rivoluzione verde e transizione ecologica; Infrastrutture per una mobilità sostenibile; Istruzione e ricerca; Inclusione e coesione; Salute);
- **"Investimento"**: Spesa per un'attività, un progetto o altre azioni utili all'ottenimento di risultati benefici per la società, l'economia e/o l'ambiente. Gli investimenti possono essere intesi come misure che portano ad un cambiamento strutturale e hanno un impatto duraturo sulla resilienza economica e sociale, sulla sostenibilità, sulla competitività a lungo termine (transizioni verdi e digitali) e sull'occupazione;
- **"Misura del PNRR"**: Specifici investimenti e/o riforme previste dal Piano Nazionale di Ripresa e Resilienza realizzati attraverso l'attuazione di interventi/progetti ivi finanziati;
- **"PNRR" o "Piano"**: Piano Nazionale di Ripresa e Resilienza presentato alla Commissione europea ai sensi dell'articolo 18 e seguenti del Regolamento (UE) 2021/241;

- **"Principio di non arrecare un danno significativo" o "DNSH"**: Principio definito all'articolo 17 Regolamento (UE) 2020/852;
- **"Progetto" o "Intervento"**: Specifico progetto/intervento (anche inteso come insieme di attività e/o procedure) selezionato e finanziato nell'ambito di una Misura del Piano e identificato attraverso un Codice Unico di Progetto. Il progetto contribuisce alla realizzazione degli obiettivi della Missione e rappresenta la principale entità del monitoraggio quale unità minima di rilevazione delle informazioni di natura anagrafica, finanziaria, procedurale e fisica;
- **"Progetti a titolarità"**: Progetti attuati direttamente dall'Amministrazione centrale titolare di interventi previsti nel PNRR, che pertanto assume in questo caso anche il ruolo di Soggetto attuatore del progetto incluso all'interno dell'intervento (investimento o riforma) di competenza;
- **"Rendicontazione delle spese"**: Attività necessaria a comprovare la corretta esecuzione finanziaria del progetto;
- **"Rendicontazione di milestone e target"**: Attività finalizzata a fornire elementi comprovanti il raggiungimento degli obiettivi del Piano (milestone e target, UE e nazionali). Non è necessariamente legata all'avanzamento finanziario del progetto;
- **"Rendicontazione dell'intervento"**: Rendicontazione bimestrale all'Ispettorato Generale per il PNRR da parte dell'Amministrazione centrale titolare di intervento. Tale attività può ricomprendere la rendicontazione delle spese sostenute dai soggetti attuatori e/o la rendicontazione del conseguimento dei milestone e target associati agli interventi di competenza;
- **"Referente dell'Amministrazione centrale titolare di interventi"**: Soggetto incardinato nella Struttura di coordinamento individuata o istituita dall'Amministrazione centrale titolare di interventi PNRR che rappresenta il punto di contatto diretto (Single Contact Point) con l'Ispettorato Generale per il PNRR e che supervisiona l'attuazione di tutti gli interventi/progetti che compongono la misura PNRR di competenza dell'Amministrazione;
- **"Sistema ReGiS"**: Sistema informatico di cui all'articolo 1, comma 1043, della legge n.178 del 2020 (legge di bilancio 2021), sviluppato per supportare le attività di gestione, di monitoraggio, di rendicontazione e di controllo del PNRR e atto a garantire lo scambio elettronico dei dati tra i diversi soggetti coinvolti nella Governance del Piano;
- **"Ispettorato Generale per il PNRR (IGPNRR"):** Struttura dirigenziale di livello generale istituita presso il Ministero dell'economia e delle finanze, Dipartimento della Ragioneria Generale dello Stato, con compiti di coordinamento delle fasi di programmazione, gestione, monitoraggio, rendicontazione e controllo del PNRR;
- **"Soggetto attuatore"**: l'Agenzia, che agisce in qualità di Soggetto delegato dalle Amministrazioni centrali titolari di interventi PNRR per l'attuazione degli interventi previsti nell'Investimento 1.5, assumendo la responsabilità dell'avvio, dell'attuazione e della funzionalità dell'intervento/progetto finanziato dal PNRR;
- "**Soggetto realizzatore**": L'Agenzia che erogherà i servizi oggetto del presente Avviso a favore dei Soggetti destinatari individuati all'esito della procedura selettiva. Ove l'Agenzia dovesse ricorrere anche a Fornitori propri, questi ultimi assumeranno il ruolo di Soggetti realizzatori;

- **"Soggetto destinatario"**: Pubblica Amministrazione che sarà individuata quale destinatario finale dell'erogazione dei servizi in oggetto, a seguito della presentazione di un'Istanza di partecipazione al presente Avviso;
- **"Target"**: Traguardo quantitativo da raggiungere tramite una determinata misura del PNRR (riforma e/o investimento), che rappresenta un impegno concordato con l'Unione europea o a livello nazionale, misurato tramite un indicatore ben specificato (es. numero di chilometri di rotaia costruiti, numero di metri quadrati di edificio ristrutturato, ecc.).

Per quanto non espressamente previsto, si rimanda alle definizioni fissate dal PNRR.

2 OGGETTO DELL'AVVISO

Il presente Avviso è volto all'individuazione dei Soggetti destinatari dei servizi che l'Agenzia intende erogare per **il potenziamento e il miglioramento delle capacità cyber delle Pubbliche Amministrazioni Centrali**, finanziati nell'ambito dell'Investimento 1.5 – Cybersecurity del PNRR, Missione M1C1 "Digitalizzazione, innovazione e sicurezza nella P.A.".

L'Avviso si rivolge ai Soggetti destinatari, individuati al successivo paragrafo 3, con l'obiettivo di supportare gli stessi nella realizzazione di un percorso virtuoso di gestione del rischio cyber. In particolare, l'Avviso concerne:

- il finanziamento per la realizzazione di un censimento dei livelli di maturità della postura di sicurezza delle PA;
- il finanziamento per la realizzazione di interventi di potenziamento dell'organizzazione, dei processi e delle procedure per la gestione del rischio cyber nella PA;
- il finanziamento per la realizzazione di un piano programmatico di potenziamento delle capacità cyber a favore del personale in modo da rafforzare il percorso di trasformazione digitale sicura della PA.

In tale ottica, il presente dispositivo ha l'obiettivo di dotare le Pubbliche Amministrazioni dei necessari strumenti e processi per una gestione del rischio cyber in linea con le migliori prassi nazionali e internazionali.

2.1 Dotazione finanziaria dell'Avviso

La dotazione finanziaria dell'Avviso ammonta complessivamente ad **€ 15.000.000,00 (quindicimilioni/00),** a valore sull'Investimento 1.5 "Cybersecurity", Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", Componente 1 – "Digitalizzazione, Innovazione e Sicurezza nella P.A.", Misura 1 – "Digitalizzazione P.A." del PNRR, da destinare alla realizzazione degli interventi, come descritti nel successivo paragrafo 4, a favore dei Soggetti destinatari individuati.

L'Agenzia si riserva la facoltà di incrementare la dotazione finanziaria del presente Avviso.

3 SOGGETTI DESTINATARI AMMESSI

Ai fini del riconoscimento e dell' erogazione del contributo per il potenziamento e il miglioramento delle capacità cyber, sono ammessi alla partecipazione gli **Organi costituzionali e a rilevanza**

costituzionale, i **Ministeri,** le **Agenzie fiscali** di cui al Titolo II e al Titolo V, Capo II, del decreto legislativo 30 luglio 1999, n. 300, gli **Enti di regolazione dell'attività economica**, le **Autorità amministrative indipendenti** e gli **Enti a struttura associativa**, come individuate da ISTAT nel settore delle Amministrazioni Pubbliche Centrali (Settore S.13)[1]. **Nel rispetto del divieto del "doppio finanziamento", non è ammessa la partecipazione dei Soggetti che abbiano già beneficiato, per la realizzazione delle medesime attività, di altre forme di finanziamento pubblico da parte del Dispositivo RRF e/o altri Programmi.** In particolare, non è ammessa la partecipazione dei Soggetti che abbiano beneficiato del finanziamento concesso, con Determina dell'Agenzia prot. n. 04136 del 20.04.2022, relativamente all'Avviso n. 2/2022 recante "*Avviso pubblico a sportello per l'erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi Costituzionali e di rilievo Costituzionale, delle Agenzia Fiscali e delle Amministrazioni facenti parte del Nucleo per la cybersicurezza a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1 I1.5*".

Conseguentemente, possono partecipare al presente Avviso esclusivamente i seguenti Soggetti:

- Consiglio di Stato;
- Consiglio nazionale dell'economia e del lavoro;
- Consiglio superiore della magistratura;
- Corte Costituzionale;
- Corte dei conti;
- Segretariato Generale della Presidenza della Repubblica;
- Ufficio parlamentare di bilancio;
- Agenzia delle dogane e dei monopoli;
- Agenzia delle entrate;
- Ministero del lavoro e politiche sociali;
- Ministero dell'interno;
- Ministero della giustizia;
- Ministero delle politiche agricole alimentari e forestali;
- Ministero per la transizione ecologica;
- Ministero dell'istruzione;
- Ministero dell'università e della ricerca;
- Ministero della cultura;
- Ministero del turismo;
- Agenzia italiana del farmaco - AIFA;
- Agenzia nazionale per i servizi sanitari regionali - AGE.NA.S.;
- Agenzia nazionale per la sicurezza del volo - ANSV;
- Agenzia nazionale per la sicurezza delle ferrovie e delle infrastrutture stradali e autostradali – ANSFISA;
- Agenzia nazionale per le politiche attive del lavoro - ANPAL;

[1] *Cfr. Classificazione ISTAT delle unità istituzionali che fanno parte del settore delle Amministrazioni Pubbliche (Settore S.13) di cui all'"Elenco delle amministrazioni pubbliche inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm. (Legge di contabilità e di finanza pubblica)" – Elenco analitico 2022*

- Agenzia per i controlli e le azioni comunitarie - AGE.CONTROL S.p.a.;
- Agenzia per l'Italia digitale - AGID;
- Agenzia per la coesione territoriale;
- Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni - ARAN;
- Agenzia per le erogazioni in agricoltura - AGEA;
- Cassa per i servizi energetici e ambientali - CSEA;
- Ente nazionale per il microcredito;
- Gestore dei servizi energetici - GSE S.p.a.;
- Ispettorato nazionale del lavoro;
- Ispettorato nazionale per la sicurezza nucleare e la radioprotezione - ISIN;
- Agenzia nazionale di valutazione del sistema universitario e della ricerca - ANVUR;
- Autorità di regolazione dei trasporti - ART;
- Autorità di regolazione per energia reti e ambiente - ARERA;
- Autorità garante della concorrenza e del mercato - AGCM;
- Autorità garante per l'infanzia e l'adolescenza - AGIA;
- Autorità nazionale anticorruzione - ANAC;
- Autorità per le garanzie nelle comunicazioni - AGCOM;
- Commissione di garanzia dell'attuazione della legge sullo sciopero nei servizi pubblici essenziali;
- Garante per la protezione dei dati personali - GPDP;
- Associazione nazionale comuni italiani - ANCI;
- Associazione nazionale degli enti di governo d'ambito per l'idrico e i rifiuti - ANEA;
- Centro Interregionale per i Sistemi Informatici Geografici e Statistici - CISIS;
- Federazione nazionale dei consorzi di bacino imbrifero montano - FEDERBIM;
- Unione delle province d'Italia - UPI;
- Unione italiana delle camere di commercio, industria, artigianato e agricoltura - UNIONCAMERE;
- Unione nazionale comuni, comunità, enti montani – UNCEM.

La partecipazione al presente Avviso è ammessa esclusivamente in forma singola e, pertanto, non sono ammesse partecipazioni in forma consortile o in associazione.

4 INTERVENTI FINANZIABILI

Con il presente Avviso, l'Agenzia intende finanziare **interventi di analisi e potenziamento della postura di sicurezza delle Pubbliche Amministrazioni centrali**, al fine di migliorare le relative capacità di prevenire e identificare le minacce cyber in continua evoluzione e rispondere in modo tempestivo a potenziali attacchi informatici. Gli interventi finanziabili a valere sul presente Avviso sono, infatti, mirati alla risoluzione di criticità delle capacità di gestione del rischio cyber nei sistemi informativi del Soggetto destinatario.

In particolare, i Soggetti partecipanti possono chiedere l'attivazione di uno o più servizi selezionati tra quelli presenti nel catalogo strutturato secondo tre specifiche tipologie di intervento di seguito descritte:

1. ***Analisi della postura di sicurezza e piano di potenziamento***: identificazione e analisi della postura di sicurezza del Soggetto destinatario, con conseguentemente definizione di un piano

strategico di potenziamento, al fine di migliorare la postura di sicurezza cyber e supportare il processo di evoluzione del livello di maturità riscontrato verso il livello target auspicato dall'Agenzia. Il modello di *analisi della postura di sicurezza* sul quale l'Agenzia eroga i servizi oggetto del presente Avviso è definito in linea con il *"Framework nazionale per la Cybersecurity e la Data Protection"* ed ha l'obiettivo di uniformare i risultati del censimento dei livelli di resilienza cyber della PA, introducendo concetti quali la rilevanza e i livelli di maturità su controlli e prassi di sicurezza; l'analisi ha, infatti, l'obiettivo di individuare i livelli di maturità dei sistemi informativi ed eventuali rischi e criticità annesse. Il modello di *piano di potenziamento strategico* ha l'obiettivo di tracciare le attività di adeguamento rispetto a carenze eventualmente identificare in fase di analisi nonché rappresentare una vista organica degli investimenti a breve e a medio-lungo termine da realizzare in ambito cyber per il Soggetto destinatario.

2. ***Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity***: valutazione - a partire dalle risultanze dei sotto-interventi di analisi e sulla base di ulteriori approfondimenti - dei processi di cybersecurity (ad es. backup & restore, gestione delle vulnerabilità, delle identità digitali, sicurezza della rete e revisione del framework documentale) attualmente utilizzati al fine di migliorarli, potenziarli e definirne di ulteriori.
3. ***Miglioramento della consapevolezza delle persone***: realizzazione di interventi formativi su tematiche di cybersecurity a favore del personale dei Soggetti destinatari, per rafforzarne la consapevolezza e le competenze, mediante la divulgazione di buone pratiche per la gestione di potenziali attacchi aventi come target gli utenti dei Soggetti destinatari.

Ogni intervento è articolato in più sotto interventi. Per ciascuno di essi, al fine di valutare il possibile valore aggiunto connesso alla relativa erogazione, si riporta, a titolo esemplificativo, una descrizione dei possibili output e dei benefici ottenibili.

Intervento 1 - Analisi della postura di sicurezza e piano di potenziamento

Sotto intervento 1.1 - Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber

Descrizione	Possibili output	Possibili benefici
Valutazione dal punto di vista organizzativo e dei processi della maturità cyber del Soggetto destinatario, identificando i punti di miglioramento e definendo una strategia evolutiva volta a incrementare il relativo livello di maturità	• Rapporto delle risultanze di analisi • Piano strategico degli interventi di potenziamento • Strumento operativo di analisi	Incremento della consapevolezza sulla postura di sicurezza corrente e rilevamento delle aree di miglioramento, al fine di orientare adeguatamente le scelte strategiche in ambito cyber per il potenziamento del livello di maturità cyber

Sotto intervento 1.2 **- Analisi delle capacità dei sistemi e strumenti di sicurezza in essere**

Descrizione	Possibili output	Possibili benefici
Valutazione tecnologica della maturità cyber del Soggetto destinatario, identificando i punti di miglioramento e definendo una strategia evolutiva volta a incrementare il relativo livello di maturità	• Rapporto delle risultanze di analisi • Piano strategico degli interventi di potenziamento • Strumento operativo di analisi	Ottimizzazione dell'ecosistema tecnologico di sicurezza cyber e identificazione di potenziali nuove soluzioni abilitanti le capacità di governo, protezione, rilevazione e risposta in ambito, al fine di incrementare la postura di sicurezza complessiva

Sotto intervento 1.3 **- Analisi di valutazione del rischio eseguita sui principali asset del Soggetto destinatario**

Descrizione	Possibili output	Possibili benefici
Valutazione del rischio cyber sui principali asset IT critici del Soggetto destinatario *(qualora non sia disponibile un catalogo di servizi consolidato presso il Soggetto Destinatario, tali asset IT saranno individuati tramite il sotto-intervento #1.1)*	• Rapporto delle risultanze di analisi • Documento descrittivo azioni di trattamento selezionate • Strumento operativo di analisi	Rilevamento del livello di esposizione al rischio cyber degli asset critici, al fine di prioritizzare i propri processi e attività in funzione dei potenziali impatti sul business, anche a supporto della continuità operativa

A prescindere dalla tipologia di servizi presenti nel catalogo di cui i Soggetti partecipanti possono chiedere l'attivazione, nel caso di ammissione a selezione quali Soggetti destinatari, gli stessi beneficeranno obbligatoriamente dell'erogazione del sotto-intervento 1.1 al fine di consentire una corretta analisi della maturità cyber dell'Amministrazione. Resta fermo che l'attivazione di tale sotto-intervento concorre alla determinazione del numero massimo di interventi erogabili e dell'importo massimo finanziabile per Soggetto.

***

Intervento 2 – Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity

Sotto intervento 2.1 **- Definizione e/o potenziamento dei processi di *gestione degli incidenti* di natura *cyber* e di *backup e restore***

Descrizione	Possibili output	Possibili benefici
Valutazione dei processi di gestione degli incidenti di natura *cyber* e di *backup e restore* eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o	• Rapporto di analisi del processo di gestione degli incidenti di natura *cyber* • Piano strategico degli interventi di potenziamento	Standardizzazione e incremento del livello di maturità delle attività di gestione e risposta agli incidenti di sicurezza, al fine di contenerne gli impatti - minimizzando la perdita di

ottimizzazione delle relative procedure a supporto	• Valutazione tecnologica e piano strategico degli interventi - *backup e restore* • Procedura aggiornata di gestione degli incidenti di natura *cyber* • Procedura aggiornata di *backup e restore*	informazioni - e ridurre il rischio di future occorrenze

Sotto intervento 2.2 **- Definizione e/o potenziamento del processo di *security by design***

Descrizione	Possibili output	Possibili benefici
Valutazione del processo e della metodologia di *security by design* eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o ottimizzazione della relativa procedura a supporto	• Procedura di *security by design* • Catalogo dei controlli di *security by design*	Definizione e ottimizzazione di un approccio standard volto a integrare gli aspetti di sicurezza durante l'intero ciclo di vita di un progetto o servizio, al fine di mitigare i rischi di sicurezza in modo proattivo

Sotto intervento 2.3 **- Definizione e/o potenziamento del processo a supporto della continuità operativa**

Descrizione	Possibili output	Possibili benefici
Valutazione del processo a supporto della continuità operativa in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o ottimizzazione della relativa politica a supporto. Conduzione di attività di *Business Impact Analysis (BIA)* su un sotto-insieme di servizi critici e definizione di strategie di continuità operativa da implementare al fine di garantire la continuità di tali servizi. *(Qualora il Soggetto destinatario non abbia definito un catalogo servizi, il sotto-insieme di servizi critici oggetto di BIA è individuato tramite sotto-intervento #1)*	• Rapporto di analisi del processo di gestione della continuità operativa • Piano strategico degli interventi di potenziamento • Politica di gestione della continuità operativa • Documento descrittivo dei risultati del *Business Impact Analysis (BIA)* svolto su un sotto-insieme di servizi in perimetro • Documento descrittivo delle strategie di continuità operativa del sotto-insieme di servizi in perimetro	Incremento del livello di comprensione delle minacce correlate alla continuità operativa di asset e servizi, e preparazione al ripristino da eventi di indisponibilità al fine di ridurre i potenziali impatti sul business

Sotto intervento 2.4 **– Definizione e/o potenziamento del processo di gestione delle vulnerabilità e di sviluppo sicuro del codice**

Descrizione	Possibili output	Possibili benefici
Valutazione dei processi di gestione delle vulnerabilità e di sviluppo sicuro del codice eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o ottimizzazione dei relativi manuali operativi/procedure a supporto	• Rapporto di analisi dei processi di gestione delle vulnerabilità e sviluppo sicuro del codice • Piano strategico degli interventi di potenziamento • Procedura di gestione delle vulnerabilità • Procedura di sviluppo sicuro del codice • Manuali operativi per lo sviluppo sicuro del codice (linguaggi applicabili: es. Java, Python, php, ecc.)	Standardizzazione e incremento del livello di maturità delle attività *end-to-end* di gestione delle vulnerabilità e sviluppo sicuro, al fine di ridurre la superficie d'attacco e mitigare il rischio di incidenti correlati allo sfruttamento di tali carenze

Sotto intervento 2.5 **– Definizione e/o potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi**

Descrizione	Possibili output	Possibili benefici
Valutazione del processo di gestione delle identità digitali e degli accessi ai sistemi informativi eventualmente in essere presso il contesto di riferimento, definizione di un piano di potenziamento strategico e conseguente elaborazione e/o ottimizzazione delle relative politiche/procedure a supporto	• Rapporto di analisi del processo di gestione delle identità digitali e degli accessi • Piano strategico degli interventi di potenziamento • Documento illustrativo dell'architettura di alto livello dell'*AS-IS* e della proposta di architettura di alto livello del *TO-BE* • Politica di gestione delle identità digitali e degli accessi logici ai sistemi • Procedura di monitoraggio e controllo delle utenze autorizzate e dei relativi accessi ai sistemi informativi	Regolamentazione delle attività di gestione delle identità digitali, dei processi di autenticazione e autorizzazione, e ottimizzazione del governo centralizzato del ciclo di vita di tali identità, al fine di mitigare i rischi connessi allo sfruttamento di utenze legittime (es. compromissione delle credenziali di accesso di un utente)

Sotto intervento 2.6 **– Supporto in ambito Network Security: analisi della rete e piano di reingegnerizzazione**

Descrizione	Possibili output	Possibili benefici
Valutazione dello stato di sicurezza della rete del Soggetto destinatario approfondendo a titolo esemplificativo i seguenti aspetti: la segregazione all'interno dell'infrastruttura di riferimento, le logiche e i presidi tecnologici di sicurezza perimetrale. Definizione di elementi adeguativi/migliorativi e conseguente elaborazione di un piano di alto livello di reingegnerizzazione dell'architettura di riferimento	• Rapporto di analisi dello stato di sicurezza della rete • Piano degli interventi migliorativi ed evolutivi • Piano di alto livello di reingegnerizzazione della rete	Incremento della consapevolezza sullo stato di sicurezza delle reti e identificazione di interventi evolutivi *ad-hoc*, al fine di migliorare la postura di sicurezza e ridurre la superficie d'attacco

Sotto intervento 2.7 **– Revisione e potenziamento del framework documentale (politiche/procedure) di sicurezza sulla base delle esigenze emerse dalle attività di analisi**

Descrizione	Possibili output	Possibili benefici
Revisione del framework documentale di sicurezza attualmente definito presso il contesto di riferimento, identificazione ed elaborazione – anche in base alle risultanze emerse dal sotto-intervento *1.1 "Analisi delle maturità di sicurezza"* – delle politiche/procedure rilevanti per incrementare la postura di sicurezza del Soggetto destinatario	• Rapporto di analisi dello stato del framework documentale presente • Politiche/procedure di sicurezza (max 15 in totale tra politiche e procedure)	Formalizzazione di politiche e procedure di sicurezza, al fine di incrementare il livello di maturità dei processi in essere, standardizzarne l'esecuzione e favorire la condivisione di conoscenze

Sotto intervento 2.8 **– Definizione di un modello di CSIRT/SOC**

Descrizione	Possibili output	Possibili benefici
Identificazione dell'attuale organizzazione preposta al controllo e al governo della sicurezza (dalla prevenzione delle minacce cyber fino alla gestione degli incidenti di sicurezza) e predisposizione di un modello CSIRT/SOC (es. constituency di riferimento, servizi da erogare, ecc.) a partire dal contesto in essere e sulla base delle buone pratiche di settore	• Rapporto di analisi che delinei l'attuale organizzazione preposta al controllo e governo della sicurezza • Documento che illustri il modello CSIRT/SOC predisposto, con evidenza dei driver a supporto della relativa strategia	Supporto all'istituzione di un centro volto a salvaguardare gli asset digitali e il proprio patrimonio informativo dalle minacce cyber, attraverso la gestione centralizzata degli eventi di sicurezza

Sotto intervento 2.9 **– Revisione e potenziamento dell'organizzazione della cybersicurezza e disegno dei relativi processi**

Descrizione	Possibili output	Possibili benefici
Revisione e potenziamento dell'attuale organizzazione di cybersecurity del Soggetto destinatario, identificando ruoli, responsabilità e processi a supporto della sicurezza informatica al fine di individuare potenziali punti evolutivi e definire/potenziare il modello di Information Security Governance	• Rapporto delle risultanze di analisi • Piano strategico degli interventi evolutivi • Modello di Information Security Governance con identificazione dei principali ruoli • Disegno dei Processi di Information Security con definizione dei workflow e delle RACI	Supporto all'identificazione di un modello organizzativo di gestione della governance della cybersicurezza, favorendo la standardizzazione dei processi in essere e la definizione di eventuali nuovi processi e ruoli, questo anche al fine di orientare adeguatamente le scelte strategiche in ambito cyber per il potenziamento del livello di maturità cyber

***

Intervento 3 **- Miglioramento della consapevolezza delle persone**

Sotto intervento 3.1 **– Servizi di *cybersecurity awareness***

Descrizione	Possibili output	Possibili benefici
Erogazione di sessioni informative su tematiche di cybersecurity a beneficio del personale dei Soggetti destinatari, attraverso lo sviluppo e la condivisione di materiale interattivo	• Materiale a supporto del corso • Pillole formative (Locandine)	Incremento della consapevolezza dei dipendenti relativamente ai rischi di cybersecurity utile per minimizzare l'occorrenza di attacchi informatici aventi come vettore l'utente finale

4.1 Dimensione finanziaria, durata e termini di realizzazione degli interventi

L'importo massimo ammissibile per ciascun finanziamento, indipendentemente dal numero degli interventi e/o dei sotto-interventi erogati, è pari a **€ 800.000,00** (ottocentomila/00) per ciascun Soggetto destinatario.

Sono previsti, altresì, dei massimali per numero e tipologia di intervento e/o sotto-intervento, che saranno quantificabili in relazione ai driver dimensionali di ciascuna Amministrazione, calcolati sulla base di quanto dichiarato da ciascun Soggetto in sede di compilazione della Scheda Fabbisogno (Allegato B) di cui al paragrafo 6.

Il Soggetto richiedente potrà attivare al massimo quattro sotto-interventi ulteriori rispetto a quello obbligatorio relativo all' "*Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber*" (#1.1). Nell'ipotesi in cui il Soggetto richiedente dovesse selezionare un numero di sotto-interventi superiore rispetto al massimale di cui sopra, verranno presi in considerazione esclusivamente i primi quattro sotto-interventi richiesti, seguendo l'ordine indicato nel precedente paragrafo 4.

1. Analisi della postura di sicurezza e definizione del piano di potenziamento

ID	Sotto-intervento	Driver dimensionale	Dettaglio per quantificazione attività	Importo massimo per Attività
1.1	**Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di politiche/procedure presenti • Numero di applicazioni gestite	• Numero di Dipartimenti coinvolti: >= 3 • Numero di politiche/procedure presenti: > 10 • Numero di applicazioni gestite: > 30	180.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di politiche/procedure presenti: da 5 a 10 • Numero di applicazioni gestite: da 10 a 30	140.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di politiche/procedure presenti: < 5 • Numero di applicazioni gestite: < 10	100.000 €
1.2	**Analisi delle capacità dei sistemi e strumenti di sicurezza in essere**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di soluzioni di sicurezza (es. SIEM, Identity & Access Management) • Numero di asset (server + workstation)	• Numero di Dipartimenti coinvolti: >= 3 • Numero di soluzioni di sicurezza: > 15 • Numero di asset: > 30	150.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di soluzioni di sicurezza: da 5 a 15 • Numero di asset: da 20 a 30	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di soluzioni di sicurezza: < 5 • Numero di asset: < 20	50.000 €
1.3	**Analisi di valutazione del rischio eseguita sui principali asset del Soggetto destinatario**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di Applicazioni critiche da analizzare • Numero di responsabili degli applicativi	• Numero di Dipartimenti coinvolti: >= 3 • Numero di applicazioni critiche da analizzare: > 10 • Numero di responsabili degli applicativi: > 3	150.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di applicazioni critiche da analizzare: da 5 a 10 • Numero di responsabili degli applicativi: da 2 a 3	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di applicazioni critiche da analizzare: < 5 • Numero di responsabili degli applicativi: < 2	50.000 €

2. Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity

ID	Sotto-intervento	Driver dimensionale	Dettaglio per quantificazione attività	Importo massimo per Attività
2.1	**Definizione e/o potenziamento dei processi di gestione degli incidenti di natura *cyber* e di *backup e restore***	• Numero di Dipartimenti coinvolti nell'analisi • Numero di Server • Numero di Client	• Numero di Dipartimenti coinvolti: >= 3 • Numero di Server: > 500 • Numero di Client: > 10.000	200.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di Server: da 100 a 500 • Numero di Client: da 1.000 a 10.000	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di Server: < 100 • Numero di Client: < 1.000	50.000 €
2.2	**Definizione e/o potenziamento del processo di security by design**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di Tecnologie	• Numero di Dipartimenti coinvolti: >= 3 • Numero di Tecnologie: > 20	80.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di Tecnologie: da 10 a 20	60.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di Tecnologie: < 10	35.000 €
2.3	**Definizione e/o potenziamento del processo a supporto della continuità operativa**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di Processi/Servizi critici • Numero di Applicazioni critiche da analizzare	• Numero di Dipartimenti coinvolti: >= 3 • Numero di applicazioni critiche da analizzare: > 10 • Numero di processi/servizi critici: > 15	180.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di applicazioni critiche da analizzare: da 10 a 5 • Numero di processi/servizi critici: da 15 a 10	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di applicazioni critiche da analizzare: < 5 • Numero di processi/servizi critici: < 10	50.000 €
2.4	**Definizione e/o potenziamento del processo di gestione delle vulnerabilità e di sviluppo sicuro del codice**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di Linguaggi di programmazione usati • Numero di applicazioni gestite	• Numero di Dipartimenti coinvolti: >= 3 • Numero di Linguaggi di programmazione usati: > 5 • Numero di applicazioni gestite: > 30	200.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di Linguaggi di programmazione usati: da 3 a 5 • Numero di applicazioni gestite: da 10 a 30	150.000 €

ID	Sotto-intervento	Driver dimensionale	Dettaglio per quantificazione attività	Importo massimo per Attività
			• Numero di Dipartimenti coinvolti: 1 • Numero di Linguaggi di programmazione usati: < 3 • Numero di applicazioni gestite: < 10	75.000 €
2.5	**Definizione e/o potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di Identità gestite • Numero di policy implementate	• Numero di Dipartimenti coinvolti: >= 3 • Numero di Identità gestite: > 300 • Numero di policy implementate: > 10.000	200.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di Identità gestite: da 100 a 300 • Numero di policy implementate: da 5.000 a 10.000	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di Identità gestite: < 100 • Numero di policy implementate: < 5.000	50.000 €
2.6	**Supporto in ambito Network Security: analisi della rete e piano di reingegnerizzazione**	• Numero di Dipartimenti coinvolti nell'analisi • Tipologia di segmenti di rete • Numero di utenti (utilizzatori web proxy) • Numero di Server	• Numero di Dipartimenti coinvolti: >= 3 • Presenza di VPN, MPLS, SD-WAN, Dark Fiber • Numero di utenti (utilizzatori web proxy): > 5.000 • Numero di Server: da 501 a 2.000	180.000 €
			• Numero di Dipartimenti coinvolti: 2 • Presenza di VPN, MPLS, SD-WAN • Numero di utenti (utilizzatori web proxy): da 1.000 a 5.000 • Numero di Server: da 101 a 500	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Presenza di VPN, MPLS • Numero di utenti (utilizzatori web proxy): < 1.000 • Numero di Server: < 101	75.000 €
2.7	**Revisione e potenziamento del framework documentale (politiche/ procedure) di sicurezza sulla base delle esigenze emerse dalle attività di analisi**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di policy/procedure in essere	• Numero di Dipartimenti coinvolti: >= 3 • Numero di Policy/Procedure in essere: > 10	200.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di Policy/Procedure in essere: da 10 a 5	150.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di Policy/Procedure in essere: < 5	100.000 €
2.8	**Definizione di un modello di CSIRT/SOC**	• Numero di Dipartimenti coinvolti nell'analisi • Presenza SOC • Presenza SIEM; se sì, Numero di	• Numero di Dipartimenti coinvolti: >= 3 • Presidio SOC presente: NO • Presenza SIEM: NO • Presenza SIEM: SI Applicazioni agganciate SIEM: > 20	150.000 €

ID	Sotto-intervento	Driver dimensionale	Dettaglio per quantificazione attività	Importo massimo per Attività
		applicazioni agganciate al SIEM	• Numero di Dipartimenti coinvolti: 2 • Presidio SOC presente: NO • Presenza SIEM: NO • Presenza SIEM: SI Applicazioni agganciate SIEM: da 10 a 20	100.000 €
			• Numero di Dipartimenti coinvolti: 1 • Presidio SOC presente: SI • Presenza SIEM: SI Applicazioni agganciate SIEM: < 10	75.000 €
2.9	**Revisione e potenziamento dell'organizzazione della cybersicurezza e disegno dei relativi processi**	• Numero di Dipartimenti coinvolti nell'analisi • Numero di processi definiti • Numero di applicazioni gestite	• Numero di Dipartimenti coinvolti: >= 3 • Numero di processi definiti: > 25 • Numero di applicazioni gestite: > 30	200.000 €
			• Numero di Dipartimenti coinvolti: 2 • Numero di processi definiti: da 15 a 25 • Numero di applicazioni gestite: da 10 a 30	150.000 €
			• Numero di Dipartimenti coinvolti: 1 • Numero di processi definiti: < 15 • Numero di applicazioni gestite: < 10	100.000 €

3. Miglioramento della consapevolezza delle persone

ID	Sotto-intervento	Driver dimensionale	Dettaglio per quantificazione attività	Importo massimo per Attività
3.1	**Servizi di cybersecurity, awareness (ad es. contrasto mail di phishing)**	• Numero di dipendenti (personale a cui è rivolta la formazione)	• Numero di dipendenti: > 500	40.000 €
			• Numero di dipendenti: da 151 a 500	25.000 €
			• Numero di dipendenti: <= 150	7.500 €

In considerazione del fatto che gli interventi dovranno essere erogati e completati, nel rispetto di quanto previsto dalla *milestone* M1C1-19, entro la fine del mese di dicembre 2024, le tempistiche attuative di ciascun intervento saranno individuate direttamente sulla base delle insindacabili valutazioni dell'Agenzia.

A tal fine, i Soggetti destinatari ammessi dovranno fornire all'Agenzia tutta la collaborazione necessaria all'avvio, allo svolgimento e al completamento degli interventi nel rispetto delle tempistiche definite nelle Schede Intervento che saranno allegate alle Convenzioni di cui al successivo paragrafo 5. Nel caso in cui la violazione di tale obbligo rilevi ai fini del mancato raggiungimento della *milestone* di cui sopra, l'Agenzia potrà procedere alla **revoca del finanziamento concesso**.

5 MODALITÀ ATTUATIVE

L'avvio delle progettualità ammesse a finanziamento e la realizzazione degli interventi a favore dei Soggetti destinatari avverrà solo dopo la stipula di specifiche Convenzioni dedicate a regolare i rapporti con l'Agenzia.

In particolare, a seguito della pubblicazione della determina di approvazione della graduatoria, i Soggetti destinatari dovranno collaborare con l'Agenzia per la condivisione di tutta la documentazione e di tutte le informazioni necessarie per individuare puntualmente il perimetro di intervento, le modalità operative e le tempistiche previste per lo svolgimento di ciascun intervento e sotto-intervento. A tal fine, verranno organizzati specifici **incontri operativi di kick-off tra l'Agenzia e ciascun Soggetto destinatario** ai quali potranno partecipare, oltre al Referente di progetto interno all'Amministrazione, anche i Soggetti che a vario titolo potranno essere coinvolti nelle attività operative.

Al termine degli incontri, verrà formalizzato in un'apposita **Scheda di Intervento, parte integrante della Convenzione** da stipulare, il piano operativo condiviso per l'erogazione degli interventi a favore dei Soggetti destinatari.

L'erogazione degli interventi ammessi a finanziamento è subordinata al trasferimento dei fondi all'Agenzia da parte del DTD.

A seguito della condivisione della suddetta Scheda di Intervento, l'Agenzia inoltrerà, ai Soggetti destinatari, apposita comunicazione di nulla osta alla stipula della Convenzione. Tali Soggetti dovranno procedere alla trasmissione della Convenzione, debitamente sottoscritta, **entro 30 (trenta) giorni lavorativi** dalla ricezione del nulla osta alla stipula da parte dell'Agenzia, salvo diverso termine concordato tra le Parti e fatte salve eventuali interruzioni necessarie per il completamento di attività istruttorie da parte dell'Agenzia.

La Convenzione dovrà essere firmata digitalmente dal legale rappresentante del Soggetto destinatario e trasmessa all'indirizzo di posta elettronica certificata (PEC) *pnrr@pec.acn.gov.it*, con l'indicazione, del seguente oggetto *"Avviso 7/2023 – Convenzione – nome Soggetto destinatario"*.

Per l'erogazione dei servizi oggetto del presente Avviso, l'Agenzia potrà avvalersi di figure tecnico/professionali all'uopo individuate, in conformità a quanto previsto dalla Circolare RGS n. 4/2022, e/o propri Fornitori, concordando con il Soggetto destinatario le modalità per l'erogazione degli interventi.

Durante la fase di erogazione degli interventi, potranno essere organizzate **riunioni sullo Stato di avanzamento delle attività** con il/i Referente/i di progetto interno/i all'Amministrazione al fine di monitorare lo stato di attuazione degli interventi e acquisire ogni altra documentazione e/o informazione che si rendesse necessaria. In ogni caso, il Soggetto destinatario è tenuto a fornire la massima collaborazione e a garantire lo scambio di dati, documenti e informazioni al fine di assicurare il corretto svolgimento degli interventi e il buon esito delle progettualità ammesse a finanziamento.

In particolare, a conclusione degli interventi, il Soggetto destinatario dovrà supportare l'Agenzia nell'individuare i **risultati raggiunti nell'ambito del potenziamento delle proprie capacità cyber**, anche nell'ottica di contribuire al raggiungimento della milestone M1C1-19.

In considerazione del fatto che gli importi previsti per l'erogazione degli interventi e riportati nelle determine di ammissione a finanziamento sono da considerarsi quali massimali, l'Agenzia procederà

ad una quantificazione dei costi reali degli interventi conclusi. La ricognizione dei costi sostenuti e la rilevazione di eventuali economie è esclusivo onere dell'Agenzia.

5.1 Modalità e rendicontazione delle spese

La realizzazione degli interventi e il conseguimento degli obiettivi prefissati devono essere puntualmente rendicontati al fine di attestare il raggiungimento delle milestone e dei target associati al presente Avviso. A tal fine, i Soggetti destinatari dovranno collaborare attivamente con l'Agenzia per consentire il monitoraggio delle attività e per garantire il rispetto delle tempistiche di programmazione, secondo tempi e modalità condivise in fase di stipula della Convenzione.

In particolare, il Soggetto destinatario è tenuto collaborare alla compilazione – per quanto di sua specifica competenza e nei tempi, con i format e secondo le modalità successivamente condivisi dall'Agenzia – della seguente documentazione predisposta dall'Agenzia:

- **Scheda di Intervento** con l'indicazione e relativa descrizione di ciascun sotto-intervento;
- **Verbale di avvio degli interventi** individuati nella Scheda di Intervento allegata alla Convenzione, con la definizione della data effettiva di inizio di ciascun sotto-intervento;
- **Relazione sullo stato di avanzamento degli interventi**, contenente tutte le informazioni necessarie per la predisposizione da parte dell'Agenzia delle Relazioni annuali di cui all'articolo 31 del Regolamento (UE) n. 2021/241;
- **Documentazione attestante milestone e target realizzati**, in conformità a quanto previsto dall'articolo 9, comma 4, del decreto-legge n. 77 del 2021
- **Verbale di chiusura degli interventi**, al fine di attestare la conclusione degli interventi erogati nel rispetto delle modalità e delle tempistiche previste dalla Scheda di Intervento nonché procedere alla quantificazione dei costi reali e alla rilevazione dei risultati raggiunti per l'Amministrazione;
- **Eventuale ulteriore documentazione richiesta** dall'Agenzia nell'ambito dei compiti e delle responsabilità attribuite dalla Convenzione stipulata.

6 TERMINI E MODALITÀ DI PARTECIPAZIONE

I Soggetti destinatari interessati dovranno presentare l'istanza di partecipazione **a partire dalle ore 10:00 del 11/10/2023 e fino alle ore 18:00 del 13/11/2023**, tramite l'invio di Posta Elettronica Certificata (PEC) all'indirizzo dedicato **pnrr@pec.acn.gov.it.** Nell'oggetto della PEC di trasmissione, dovrà essere necessariamente indicata, **pena inammissibilità**, la seguente dicitura: *"Istanza di partecipazione Avviso 7/2023 – SOGGETTO"*.

Ai fini del presente Avviso, il rispetto del termine di presentazione e la data e l'ora di ricezione ai fini della definizione dell'ordine cronologico è attestata dalla data e dall'ora indicata nella ricevuta di accettazione inviata dal Sistema di Posta Elettronica Certificata. L' Agenzia non assume responsabilità in ordine a ritardi, disguidi o malfunzionamenti legati all'inoltro/ricezione della PEC essendo la responsabilità del recapito dell'Istanza di partecipazione a carico esclusivo del richiedente.

L'Agenzia si riserva la facoltà di riaprire lo sportello per la presentazione delle istanze, nel caso di risorse residue o rifinanziamento dell'Avviso.

Ogni Soggetto destinatario interessato potrà presentare una sola istanza di partecipazione, avente ad oggetto la richiesta di erogazione di servizi **per la realizzazione di uno o più interventi tra quelli proposti**, fermo restando il limite massimo di 4 sotto-interventi, oltre il sotto-intervento obbligatorio 1.1 "*Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber*".

Nel caso di invio di più istanze di partecipazione da parte del medesimo Soggetto, sarà presa in considerazione l'ultima pervenuta in ordine cronologico, in rettifica e sostituzione alla precedente. Si chiarisce a tal fine che, al verificarsi di tale fattispecie, verranno considerati quali termini di presentazione dell'istanza quelli relativi all'ultima inviata.

L'**istanza di partecipazione,** debitamente compilata in tutte le sue parti, dovrà essere sottoscritta con firma digitale, in corso di validità, dal legale rappresentate del Soggetto richiedente. In alternativa, la stessa potrà essere sottoscritta da un Soggetto delegato, fornendo contestualmente copia del relativo atto di delega.

L'istanza è resa nella forma di dichiarazione sostitutiva di certificazione, ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e con le responsabilità previste dagli artt. 75 e 76 dello stesso decreto, al fine di dichiarare il possesso dei requisiti minimi di partecipazione all'Avviso.

Nella **Scheda Fabbisogno**, redatta secondo il *template* di cui all'**Allegato B** del presente Avviso, il Soggetto richiedente dovrà indicare, per ogni sotto-intervento richiesto, tutte le informazioni necessarie alla definizione ed alla quantificazione del perimetro degli stessi. Per supportare la comprensione dei termini utilizzati, in allegato alla Scheda Fabbisogno, è fornito un **Glossario che non dovrà essere ricompreso** nella documentazione da trasmettere.

Non saranno ammesse alla valutazione istanze di partecipazione incomplete o pervenute fuori termine.

7 ISTRUTTORIA DELLE ISTANZE

La modalità di selezione delle istanze inoltrate nell'ambito del presente Avviso è quella dello **sportello**, che resterà aperto nel rispetto dei termini previsti dal precedente paragrafo 6.

Le istanze presentate saranno istruite e valutate sotto i seguenti profili, sulla base dell'ordine cronologico di ricezione:

a. Ricevibilità formale:

- presentazione dell'istanza di partecipazione nei termini e nelle modalità di trasmissione previsti al precedente paragrafo 6 (PEC, oggetto della PEC, sottoscrizione digitale);
- completezza e regolarità formale dell'istanza, corredata da tutti gli allegati indicati nel precedente paragrafo 6 e formata nel rispetto dei template forniti che devono essere correttamente valorizzati in tutti i loro campi.

b. Ammissibilità del Soggetto. Le sole istanze ritenute ricevibili a seguito dei controlli di cui sopra saranno oggetto di verifiche di ammissibilità così declinate:

- ammissibilità del Soggetto proponente, che deve individuarsi tra i Soggetti individuati nel paragrafo 3 ed essere in possesso dei requisiti minimi previsti.

c. Conformità del progetto:

- rispetto del numero massimo di sotto-interventi previsto al paragrafo 4.1;
- attinenza alle finalità dell'Avviso: gli interventi richiesti dovranno essere coerenti rispetto agli obiettivi di potenziamento e miglioramento delle capacità cyber del Soggetto richiedente e alla capacità degli stessi interventi di contribuire alla risoluzione delle criticità riscontrate nell'attuale postura di sicurezza;
- perimetro degli interventi: gli interventi richiesti non dovranno riguardare attività che hanno ad oggetto informazioni a cui sono attribuite classifiche di segretezza, ai sensi della legge3 agosto 2007, n. 124 , al fine di consentire il rispetto delle disposizioni in materia di pubblicità e trasparenza e la trasmissione della richiesta di trasferimento delle risorse, delle dichiarazioni sul conseguimento delle milestone e dei target e delle relazioni sullo stato di attuazione dei progetti alla Servizio centrale per il PNRR e alla Commissione Europea.

Il Responsabile del procedimento, in virtù dei compiti definiti dall'art. 6 della legge n. del 1990, potrà individuare un gruppo di lavoro a suo supporto per lo svolgimento dell'istruttoria amministrativa per le verifiche di conformità degli interventi rispetto alle tipologie di cui al paragrafo 4.

7.1 Formalizzazione degli esiti dell'istruttoria e concessione del contributo

A conclusione della fase di istruttoria amministrativa, l'Agenzia redigerà gli elenchi delle proposte progettuali pervenute individuando, in particolare, le proposte progettuali:

- ammesse al finanziamento e totalmente finanziabili;
- ammesse al finanziamento e parzialmente finanziabili;
- ammissibili non finanziabili (ad es. per carenza di risorse a disposizione o per superamento del massimale per Soggetto);
- non ammesse al finanziamento, con indicazione della relativa motivazione.

L'Agenzia, in caso di rifinanziamento dell'Avviso, rinunce o revoche o successiva rilevazione di economie a seguito della quantificazione dei costi reali, si riserva la possibilità di utilizzare gli elenchi delle proposte progettuali parzialmente finanziabili e ammissibili ma non finanziabili ai fini dello scorrimento degli stessi elenchi.

L'approvazione degli elenchi e la formalizzazione degli stessi da parte del Direttore Generale dell'Agenzia sarà notificata a tutti Soggetti partecipanti.

8 OBBLIGHI DELLE PARTI

8.1 Obblighi del Soggetto attuatore

Ai fini della realizzazione dell'intervento proposto, il Soggetto attuatore dovrà impegnarsi a:

- sottoscrivere la Convenzione entro i termini previsti dal presente Avviso;

- assicurare il rispetto di tutte le disposizioni previste dalla normativa europea e nazionale, con particolare riferimento al disposto del Regolamento (UE) 2021/241 e del decreto-legge n. 77 del 2021;
- assicurare l'adozione di misure adeguate volte a rispettare il principio di sana gestione finanziaria secondo quanto disciplinato nel Regolamento (UE, Euratom) 2018/1046 , e nell'articolo 22 del Regolamento (UE) 2021/241, in particolare in materia di prevenzione, identificazione e rettifica dei conflitti di interessi, delle frodi, della corruzione e di recupero e restituzione dei fondi che sono stati indebitamente assegnati, nonché di garantire l'assenza del c.d. doppio finanziamento ai sensi dell'articolo 9 del Regolamento (UE) 2021/241;
- rispettare, ove applicabile, il principio di "*non arrecare un danno significativo*" (DNSH) agli obiettivi ambientali, ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 e garantire la coerenza con il PNRR valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021;
- rispettare, ove applicabili, le condizioni prescrittive necessarie all'assolvimento del principio del contributo all'obiettivo climatico e digitale (cd. tagging);
- rispettare la normativa applicabile in tema di trattamento dei dati personali e, in particolare, il Regolamento (UE) 2016/679 (GDPR);
- rispettare, ove applicabili, gli ulteriori principi trasversali previsti per il PNRR dalla normativa nazionale ed europea, con particolare riferimento alla protezione e valorizzazione dei giovani e del superamento dei divari territoriali;
- introdurre nella fase di esecuzione, ove applicabili, misure a sostegno della partecipazione di donne e giovani, anche in coerenza con quanto previsto dall'articolo 47 del decreto-legge n. 77 del 2021;
- rispettare le norme europee e nazionali applicabili in ambito di tutela dei soggetti diversamente abili;
- rispettare i principi di parità di trattamento, non discriminazione, trasparenza, proporzionalità e pubblicità;
- garantire il rispetto del principio di parità di genere in relazione agli articoli 2, 3, paragrafo 3, del TUE, 8, 10, 19 e 157 del TFUE, e 21 e 23 della Carta dei diritti fondamentali dell'Unione europea;
- dare piena attuazione agli interventi così come illustrati nella Scheda Intervento ed avviare tempestivamente le attività al fine di non incorrere in ritardi attuativi;
- garantire la correttezza, l'affidabilità e la congruenza al tracciato del sistema informativo unitario per il PNRR di cui all'articolo 1, comma 1043, della legge n. 178 del 2020 dei dati di monitoraggio finanziario, fisico e procedurale, e di quelli che comprovano il conseguimento degli obiettivi dell'intervento quantificati in base agli stessi indicatori adottati per milestone e target della misura e assicurarne l'inserimento nel sistema informativo e gestionale adottato dalla Amministrazione centrale titolare dell'intervento responsabile nel rispetto delle indicazioni che saranno fornite dalla stessa Amministrazione;
- adottare un'apposita codificazione contabile e informatizzata per tutte le transazioni relative al progetto al fine di assicurare la tracciabilità dell'utilizzo delle risorse del PNRR;

- effettuare i controlli di gestione e amministrativo-contabili previsti dalla legislazione nazionale applicabile per garantire la regolarità delle procedure e delle spese sostenute prima di rendicontarle alla Amministrazione centrale titolare dell'intervento, nonché la riferibilità delle spese al progetto ammesso al finanziamento sul PNRR;
- fornire tutte le informazioni richieste relativamente alle procedure e alle verifiche in relazione alle spese rendicontate conformemente alle procedure e agli strumenti definiti nella manualistica adottata dall'Amministrazione centrale titolare dell'intervento;
- assicurare la completa tracciabilità dei flussi finanziari come previsto dall'articolo 3 della legge 3 agosto 2016, n. 136, e prevedere una modalità di gestione finanziaria che sia conforme alle disposizioni del Regolamento (UE, Euratom) 2018/1046 e dell'articolo 22 del Regolamento (UE) 2021/241, in materia di prevenzione di sana gestione finanziaria, assenza di conflitti di interessi, di frodi e corruzione;
- rilevare e imputare nel sistema informativo i dati di monitoraggio sull'avanzamento procedurale, fisico e finanziario del progetto, *ex* articolo 22, comma 2, lettera d), del Regolamento (UE) 2021/241, nonché le informazioni a comprova del conseguimento delle milestone e dei target associati all'intervento, ivi inclusa la documentazione probatoria;
- garantire la correttezza, l'affidabilità e la congruenza dei dati di monitoraggio di cui sopra;
- rispettare gli adempienti in materia di trasparenza amministrativa *ex* decreto legislativo 25 maggio 2016, n. 97, e gli obblighi in materia di comunicazione e informazione previsti dall'articolo 34 del Regolamento (UE) 2021/241;
- rendere nota l'origine del finanziamento e garantirne visibilità riportando in tutta la documentazione di progetto il logo dell'Unione Europea e utilizzando la dicitura "Finanziato dall'Unione Europea – Next Generation UE – PNRR M1C1 – Investimento 1.5";
- conservare - nel rispetto di quanto previsto dal decreto legislativo 7 marzo 2005, n. 82, e all'articolo 9, comma 4, del decreto-legge n. 77 del 2021 - la documentazione progettuale per assicurare la completa tracciabilità delle operazioni che, nelle diverse fasi di controllo e verifica previste dal sistema di gestione e controllo del PNRR, deve essere messa prontamente a disposizione su richiesta dell'Agenza, dell'Amministrazione centrale titolare dell'intervento, del Servizio centrale per il PNRR del MEF, dell'Unità di Audit, della Commissione europea, dell'Ufficio europeo per la lotta antifrode, della Corte dei conti europea (ECA), della Procura europea (EPPO) e delle competenti Autorità giudiziarie nazionali;
- autorizzare la Commissione, l'Ufficio europeo per la lotta antifrode, la Corte dei conti e l'EPPO a esercitare i diritti di cui all'articolo 129, paragrafo 1, del Regolamento (UE; EURATOM) 1046/2018;
- garantire, anche attraverso la trasmissione di relazioni periodiche sullo stato di avanzamento del progetto, che l'Amministrazione centrale titolare dell'intervento riceva tutte le informazioni necessarie, relative alle linee di attività per l'elaborazione delle relazioni annuali di cui all'articolo 31 del Regolamento (UE) n. 2021/241, nonché qualsiasi altra informazione eventualmente richiesta;
- contribuire al raggiungimento dei milestone e target associati alla Misura e fornire, su richiesta dell'Amministrazione centrale titolare dell'intervento, le informazioni necessarie per la

predisposizione delle dichiarazioni sul conseguimento dei target e milestone e delle relazioni e documenti sull'attuazione dei progetti;

- garantire il rispetto degli obblighi in materia di comunicazione e informazione previsti dall'articolo 34 del Regolamento (UE) 2021/241 indicando nella documentazione progettuale che il progetto è finanziato nell'ambito del PNRR, con esplicito riferimento al finanziamento da parte dell'Unione europea e all'iniziativa Next Generation EU (utilizzando la frase "finanziato dall'Unione europea – Next Generation EU"), riportando nella documentazione progettuale l'emblema dell'Unione europea e fornire un'adeguata diffusione e promozione del progetto, anche online, sia web che social, in linea con quanto previsto dalla Strategia di Comunicazione del PNRR;
- reimpiegare, per finalità sociali, gli eventuali proventi derivanti dalla gestione diretta o indiretta del bene finanziato nell'ambito del presente Avviso e/o da qualunque utilizzo economico e/o commerciale dello stesso;
- garantire una tempestiva, diretta, informazione agli organi preposti, tenendo informata l'Amministrazione centrale titolare dell'intervento sull'eventuale avvio e andamento di procedimenti di carattere giudiziario, civile, penale o amministrativo che dovessero interessare le attività oggetto del progetto finanziato;
- comunicare le irregolarità o le frodi eventualmente riscontrate a seguito delle verifiche di competenza e adottare le misure necessarie, nel rispetto delle procedure adottate dalla Amministrazione centrale titolare dell'intervento, in linea con quanto indicato dall'articolo 22 del Regolamento (EU) 2021/2041;
- garantire la massima collaborazione in occasione di verifiche e controlli richiesti dall'Amministrazione centrale titolare dell'intervento, dal Servizio centrale per il PNRR, dall'Unità di Audit, dalla Commissione europea, dall'Ufficio europeo per la lotta antifrode, dalla Corte dei Conti europea (ECA), della Procura europea (EPPO) e dalle competenti Autorità giudiziarie nazionali, nonché eventualmente delle Forze di polizia nazionali.

8.2 Obblighi dei Soggetti destinatari

Ai fini della realizzazione dell'intervento proposto, il Soggetto destinatario dovrà impegnarsi a:

- sottoscrivere la Convenzione entro i termini di cui al presente Avviso;
- collaborare all'ultimazione degli interventi finanziati e previsti nella Scheda Intervento;
- fornire la necessaria collaborazione per lo svolgimento di tutte le attività previste nella Convenzione, nei termini ivi indicati e con le modalità di cui alla Scheda di Intervento;
- collaborare con il Soggetto attuatore per assicurare il rispetto di tutte le disposizioni previste dalla normativa europea e nazionale, con particolare riferimento a quanto previsto dal Regolamento (UE) 2021/241 e dal decreto-legge n. 77 del 2021;
- collaborare con il Soggetto attuatore per garantire il rispetto del principio di *"non arrecare un danno significativo"* (DNSH) agli obiettivi ambientali ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 e per garantire la coerenza con il PNRR valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021;

- collaborare con il Soggetto attuatore per rispettare le condizioni prescrittive necessarie all'assolvimento del principio del contributo all'obiettivo climatico e digitale (cd. tagging);
- collaborare con il Soggetto attuatore nell'assicurare l'adozione di misure adeguate volte a rispettare il principio di sana gestione finanziaria secondo quanto disciplinato dal Regolamento (UE, Euratom) 2018/1046 e dall'articolo 22 del Regolamento (UE) 2021/241, in particolare in materia di prevenzione, identificazione e rettifica dei conflitti di interessi, delle frodi, della corruzione e di recupero e restituzione dei fondi che sono stati indebitamente assegnati, nonché di garantire l'assenza del c.d. doppio finanziamento ai sensi dell'articolo 9 del Regolamento (UE) 2021/241;
- collaborare con il Soggetto attuatore per rispettare le norme europee e nazionali applicabili in ambito di tutela dei soggetti diversamente abili;
- collaborare con il Soggetto attuatore per rispettare i principi di parità di trattamento, non discriminazione, trasparenza, proporzionalità e pubblicità;
- collaborare con il Soggetto attuatore per garantire il rispetto del principio di parità di genere in relazione agli articoli 2, 3, paragrafo 3, del TUE, 8, 10, 19 e 157 del TFUE, e 21 e 23 della Carta dei diritti fondamentali dell'Unione europea e alla protezione e valorizzazione dei giovani, anche in coerenza con quanto previsto dall'articolo 47 del decreto-legge n. 77 del 2021 e del superamento dei divari territoriali;
- collaborare con il Soggetto attuatore per individuare eventuali fattori che possano determinare ritardi che incidano in maniera considerevole sulla tempistica attuativa e di spesa, definita nel cronoprogramma, relazionando all'Agenzia sugli stessi;
- collaborare con il Soggetto attuatore per mitigare e gestire i rischi connessi al progetto nonché per porre in essere azioni mirate connesse all'andamento gestionale ed alle caratteristiche tecniche;
- fornire supporto per la rendicontazione degli indicatori di realizzazione associati al progetto, in riferimento al contributo al perseguimento dei target e milestone del PNRR;
- collaborare con il Soggetto attuatore per garantire la correttezza, l'affidabilità e la congruenza dei dati di monitoraggio di propria competenza con il tracciato informativo previsto per l'alimentazione del sistema informativo PNRR (ReGiS) dei dati di monitoraggio finanziario, fisico e procedurale, e di quelli che comprovano il conseguimento degli obiettivi dell'intervento quantificati in base agli stessi indicatori adottati per i milestone e i target della misura e assicurarne l'inserimento nel sistema informativo utilizzato dall'Amministrazione responsabile dei dati di monitoraggio sull'avanzamento procedurale, fisico e finanziario del progetto, ex articolo 22, comma 2, lettera d), del Regolamento (UE) 2021/241, nonché le informazioni a comprova del conseguimento delle milestone e dei target associati all'intervento, ivi inclusa la documentazione probatoria e tenendo conto delle indicazioni che verranno fornite dall'Amministrazione responsabile;
- rispettare gli adempienti in materia di trasparenza amministrativa ex decreto legislativo 25 maggio 2016, n. 97, e gli obblighi in materia di comunicazione e informazione previsti dall'articolo 34 del Regolamento (UE) 2021/241;

- rendere nota l'origine del finanziamento e garantirne visibilità riportando in tutta la documentazione di progetto il logo dell'Unione Europea e utilizzando la dicitura "Finanziato dall'Unione Europea – Next Generation UE – PNRR M1C1 – Investimento 1.5";
- conservare - nel rispetto di quanto previsto dal decreto legislativo n. 82 del 2005 e dall'articolo 9, comma 4, del decreto-legge n. 77 del 2021 - la documentazione progettuale, inclusa quella relativa alle spese sostenute ed ai target realizzati, per assicurare la completa tracciabilità delle operazioni, che, nelle diverse fasi di controllo e verifica previste dal sistema di gestione e controllo del PNRR, deve essere messa prontamente a disposizione su richiesta dell'Agenzia, dell'Amministrazione centrale titolare dell'intervento, del Servizio centrale per il PNRR del MEF, dell'Unità di Audit, della Commissione europea, dell'Ufficio europeo per la lotta antifrode, della Corte dei Conti europea (ECA), della Procura europea (EPPO) e delle competenti Autorità giudiziarie nazionali;
- autorizzare la Commissione, l'Ufficio europeo per la lotta antifrode, la Corte dei conti e l'EPPO a esercitare i diritti di cui all'articolo 129, paragrafo 1, del Regolamento (UE; EURATOM) 1046/2018;
- partecipare, ove richiesto, alle riunioni convocate dall'Agenzia;
- reimpiegare per finalità sociali gli eventuali proventi derivanti dalla gestione diretta o indiretta del bene finanziato nell'ambito del presente Avviso e/o da qualunque utilizzo economico e/o commerciale dello stesso;
- garantire una tempestiva diretta informazione agli organi preposti, tenendo informata l'Agenzia sull'eventuale avvio e andamento di procedimenti di carattere giudiziario, civile, penale o amministrativo che dovessero interessare le attività oggetto del progetto finanziato;
- comunicare le irregolarità o le frodi eventualmente riscontrate a seguito delle verifiche di competenza e adottare le misure necessarie, nel rispetto delle procedure adottate dall'Agenzia, in linea con quanto indicato dall'articolo 22 del Regolamento (EU) 2021/241;
- garantire la massima collaborazione in occasione di verifiche e controlli richiesti dall'Agenzia, dal Servizio centrale per il PNRR, dall'Unità di audit, della Commissione europea, dell'Ufficio europeo per la lotta antifrode, della Corte dei conti europea (ECA), della Procura europea (EPPO) e dalle competenti Autorità giudiziarie nazionali, nonché eventualmente dalle forze di polizia nazionali.

8.3 Meccanismi sanzionatori

Nel caso di inadempimento e violazione degli obblighi posti in capo al Soggetto destinatario, può essere disposta la sospensione del finanziamento e dei servizi con la revoca parziale o totale del contributo ai sensi dell'articolo 8, comma 5, del decreto-legge n. 77 del 2021.

Sarà valutata la revoca totale o parziale del finanziamento nei seguenti casi di inadempimento e violazione da parte del Soggetto destinatario:

- parziale o mancato conseguimento di target, milestone e degli obiettivi previsti, anche di natura finanziaria, nei tempi assegnati, al fine di salvaguardare il raggiungimento di target e milestone intermedi e finali associati all'investimento;
- sospetta violazione dei principi generali di DNSH e/o del principio del tagging e/o accertamento della violazione;

- gravi violazioni di leggi e regolamenti e violazione e/o inadempienza agli obblighi di cui al presente Avviso;
- mancata collaborazione con l'Agenzia nella fase di rendicontazione delle spese.

9 RESPONSABILE DELL'AVVISO

Il Responsabile del procedimento, nominato dall'Agenzia, è il Dott. Luca Nicoletti.

Tale soggetto è responsabile della fase di progettazione dell'Avviso e di selezione dei Soggetti destinatari.

10 RICHIESTE DI INFORMAZIONI E CHIARIMENTI

Eventuali richieste di informazioni e chiarimenti potranno essere inoltrate all'indirizzo e-mail dedicato *pnrr-cybersecurity@acn.gov.it*, avendo cura di riportare nell'oggetto l'identificativo "Avviso Pubblico 7 - Investimento 1.5".

Con riferimento ai chiarimenti inerenti alla presentazione delle istanze di partecipazione, al fine di consentire l'elaborazione dei riscontri e la pubblicazione degli stessi, le richieste dovranno pervenire 10 giorni prima della scadenza del termine ultimo di presentazione delle istanze di cui al paragrafo "Termini e modalità di partecipazione".

I riscontri, ove pertinenti, saranno comunicati a tutti i Soggetti interessati a mezzo di pubblicazione di apposite FAQ sul sito dell'Agenzia e costituiranno parte integrante del presente Avviso.

11 TUTELA DELLA PRIVACY

Il trattamento dei dati raccolti nell'ambito della procedura di cui al presente Avviso è effettuato dall'Agenzia, in qualità di Titolare del trattamento, ai sensi del Regolamento (UE) 2016/679 (GDPR) e della disciplina nazionale in materia di protezione dei dati personali.

I dati personali saranno trattati esclusivamente ai fini dello svolgimento della procedura di cui al presente Avviso, secondo le disposizioni contenute nell'articolo 22 del Regolamento (UE) 2021/241.

Base giuridica del trattamento è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (articolo. 6.1 *e)* del GDPR).

I dati trattati non saranno trasferiti fuori dallo Spazio Economico Europeo.

I soggetti interessati potranno esercitare i diritti previsti dalla normativa applicabile scrivendo all'Agenzia o inviando un'e-mail al Responsabile per la protezione dei dati dell'Agenzia, all'indirizzo *dpo@acn.gov.it*.

È facoltà degli interessati, ove ritenessero violati i propri diritti, inoltrare un reclamo all'autorità nazionale competente (per l'Italia: Garante per la protezione dei dati personali, *protocollo@gpdp.it*) e/o adire la giurisdizione ordinaria.

12 DISPOSIZIONI FINALI E RINVIO

Per le controversie che dovessero sorgere in ordine al presente Avviso è competente, in via esclusiva, il Foro di Roma.

ALLEGATI

- **Allegato A** – Istanza di partecipazione corredata dall'Autodichiarazione relativa al rispetto dei principi previsti per gli interventi del PNRR;
- **Allegato B** – Scheda Fabbisogno;
- **Allegato C** – Schema di Convenzione.