REGIONE LAZIO

REGIONE LAZIO

Direzione: DIREZIONE PER L'INNOVAZIONE TECNOLOGICA E LA TRASFORMAZIONE DIGITALE

Area:

DETERMINAZIONE *(con firma digitale)*

N. G03854 **del** 05/04/2024 **Proposta n.** 10870 **del** 27/03/2024

Oggetto: ***Presenza annotazioni contabili***

PNRR - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5. Approvazione Studio di Fattibilità del Cyber Security Incident Response Team (CSIRT) - Id progetto 4_WP7_A6_Regione Lazio - CUP: F84F23000230006. Accertamento in entrata sul capitolo E0000229184 a carico dell'Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280), per una somma complessiva di € 1.500.000,00, e contestuali impegni di spesa a favore di LAZIOcrea S.p.A. (codice creditore 164838) per una somma complessiva di € 1.500.000,00 IVA inclusa sul capitolo U0000S25107, esercizi finanziari 2024-2025. Cod. MIR I202400030.

Proponente:

Estensore	D'AMBROGIO VIVIANA	_____*firma elettronica*_____
Responsabile del procedimento	MARTA LUCA	_____*firma elettronica*_____
Responsabile dell' Area		_____
Direttore Regionale	L. MARTA	_____*firma digitale*_____

Firma di Concerto

Ragioneria:

Responsabile del procedimento		_____
Responsabile dell'Area Ragioneria	DELLARNO GIUSEPPE	_____*firma digitale*_____
Ragioneria Generale	MARCO MARAFINI	_____*firma digitale*_____

Richiesta di pubblicazione sul BUR: SI

REGIONE LAZIO

Proposta n. 10870 **del** 27/03/2024

Annotazioni Contabili *(con firma digitale)*

PGC	Tipo Mov.	Capitolo	Impegno / Accertamento	Mod.	Importo	Miss./Progr./PdC finanz.

Descr. PdC finanz.

Azione

Beneficiario

1) E E0000229184 2024 750.000,00 101.10101 2.01.01.01.001

Trasferimenti correnti da Ministeri

7.01.08.04

Agenzia per la Cybersicurezza Nazionale

Intervento/Progetto: I202400030
Tipo mov. : CRONOPROGRAMMA PLURIENNALE

---

2) E E0000229184 2025 750.000,00 101.10101 2.01.01.01.001

Trasferimenti correnti da Ministeri

7.01.08.04

Agenzia per la Cybersicurezza Nazionale

Intervento/Progetto: I202400030
Tipo mov. : CRONOPROGRAMMA PLURIENNALE

---

3) I U0000S25107 2024 750.000,00 01.12 1.03.02.99.010

Formazione a personale esterno all'ente

7.01.08.04

LAZIOCREA S.P.A.

Intervento/Progetto: I202400030
Tipo mov. : CRONOPROGRAMMA PLURIENNALE

PGC	Tipo Mov.	Capitolo	Impegno / Accertamento	Mod.	Importo	Miss./Progr./PdC finanz.	
Descr. PdC finanz.							
Azione							
Beneficiario							
4)	I	U0000S25107	2025		750.000,00	01.12	1.03.02.99.010
Formazione a personale esterno all'ente							
7.01.08.04							
LAZIOCREA S.P.A.							
Intervento/Progetto: I202400030 Tipo mov. : CRONOPROGRAMMA PLURIENNALE							

REGIONE LAZIO

Proposta n. 10870 **del** 27/03/2024

PIANO FINANZIARIO DI ATTUAZIONE DELLA SPESA

Oggetto Atto: PNRR - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5. Approvazione Studio di Fattibilità del Cyber Security Incident Response Team (CSIRT) - Id progetto 4_WP7_A6_Regione Lazio - CUP: F84F23000230006. Accertamento in entrata sul capitolo E0000229184 a carico dell'Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280), per una somma complessiva di € 1.500.000,00, e contestuali impegni di spesa a favore di LAZIOcrea S.p.A. (codice creditore 164838) per una somma complessiva di € 1.500.000,00 IVA inclusa sul capitolo U0000S25107, esercizi finanziari 2024-2025. Cod. MIR I202400030.

INTERVENTO			RIFERIMENTI DI BILANCIO		
Pgc.	N.Imp.	Causale	Mi./Pr.	PdC fin al IV liv.	Capitolo
3		PNRR - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5. Approvazione Studio Fattibilità del progetto " 4_WP7_A6_Regione Lazio - CUP: F84F23000230006", accertamento in entrata sul capitolo E0000229184 a carico dell'Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280), per una somma complessiva di € 1.500.000,00, e contestuali impegni di spesa a favore di LAZIOcrea S.p.A. (codice creditore 164838) per una somma complessiva di € 1.500.000,00 IVA inclusa sul capitolo U0000S25107, esercizi finanziari 2024-2025. Cod MIR I202400030.	01/12	1.03.02.99.010	U0000S25107

PIANO FINANZIARIO

Anno	*Impegno*	*Liquidazione*	
	Importo (€)	*Mese*	*Importo (€)*
2024	750.000,00	Dicembre	750.000,00
		Totale	**750.000,00**

INTERVENTO			RIFERIMENTI DI BILANCIO		
Pgc.	N.Imp.	Causale	Mi./Pr.	PdC fin al IV liv.	Capitolo
4		PNRR - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5. Approvazione Studio Fattibilità del progetto " 4_WP7_A6_Regione Lazio - CUP: F84F23000230006", accertamento in entrata sul capitolo E0000229184 a carico dell'Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280), per una somma complessiva di € 1.500.000,00, e contestuali impegni di spesa a favore di LAZIOcrea S.p.A. (codice creditore 164838) per una somma complessiva di € 1.500.000,00 IVA inclusa sul capitolo U0000S25107, esercizi finanziari 2024-2025. Cod MIR I202400030.	01/12	1.03.02.99.010	U0000S25107

PIANO FINANZIARIO

Anno	*Impegno*	*Liquidazione*	
	Importo (€)	*Mese*	*Importo (€)*
2025	750.000,00	Dicembre	750.000,00
		Totale	**750.000,00**

OGGETTO: PNRR – Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5. Approvazione Studio di Fattibilità del Cyber Security Incident Response Team (CSIRT) – Id progetto 4_WP7_A6_Regione Lazio – CUP: F84F23000230006. Accertamento in entrata sul capitolo E0000229184 a carico dell'Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280), per una somma complessiva di € 1.500.000,00, e contestuali impegni di spesa a favore di LAZIOcrea S.p.A. (codice creditore 164838) per una somma complessiva di € 1.500.000,00 IVA inclusa sul capitolo U0000S25107, esercizi finanziari 2024-2025. Cod. MIR I202400030.

IL DIRETTORE DELLA DIREZIONE REGIONALE LAVORI PUBBLICI E INFRASTRUTTURE, INNOVAZIONE TECNOLOGICA

VISTO lo Statuto della Regione Lazio, e in particolare l'art. 48 che disciplina il potere di indirizzo politico-amministrativo di competenza della Giunta regionale prevedendo, tra l'altro, che la Giunta assegni ai dirigenti gli obiettivi ed i progetti da realizzare e le relative risorse finanziarie;

VISTA la legge regionale 18 febbraio 2002, n. 6, "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza e al personale regionale";

VISTO il Regolamento Regionale del 6 settembre 2002, n. 1, "Regolamento di organizzazione degli uffici e dei servizi della Giunta Regionale";

VISTO il D. Lgs. 23 giugno 2011, n. 118 recante "Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della Legge 5.5.2009, n. 42" e successive modifiche e integrazioni;
VISTA la Legge Regionale 29 dicembre 2023 n. 23 recante: "Legge di stabilità regionale 2024";

VISTA la Legge Regionale 29 dicembre 2023 n. 24 recante: "Bilancio di previsione finanziario della Regione Lazio 2024-2026";

VISTA la Deliberazione della Giunta regionale 29 dicembre 2023 n. 980 recante "Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del "Documento tecnico di accompagnamento", ripartito in titoli, tipologie e categorie per le entrate ed in missioni, programmi, titoli e macroaggregati per le spese";

VISTA la Deliberazione della Giunta regionale 29 dicembre 2023 n. 981 recante "Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del "Bilancio finanziario gestionale", ripartito in capitoli di entrata e di spesa ed assegnazione delle risorse finanziarie ai dirigenti titolari dei centri di responsabilità amministrativa";

VISTA la Deliberazione della Giunta Regionale 14 febbraio 2024, n. 75, concernente: "Indirizzi per la gestione del bilancio regionale 2024-2026 e approvazione del bilancio reticolare, ai sensi degli articoli 30, 31 e 32, della legge regionale 12 agosto 2020, n. 11";

VISTA la Legge Regionale 12 agosto 2020, n. 11, recante: "Legge di contabilità regionale";

VISTO il Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale";

VISTA la Legge 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";

VISTO il Regolamento Regionale 9 novembre 2017, n. 26, recante: "Regolamento regionale di contabilità" che, ai sensi dell'art.56, comma 2, L.R. n.11/2020, che fino alla data di entrata in vigore del regolamento di contabilità di cui all'art. 55 della L.R. n.11/2020, continua ad applicarsi, per quanto compatibile, con le disposizioni di cui alla medesima L.R. n. 11/2020;

VISTO il regolamento regionale 23 ottobre 2023, n. 9, concernente: "Modifiche al regolamento regionale 6 settembre 2002, n.1 (Regolamento di organizzazione degli uffici e dei servizi della giunta regionale) e successive modifiche. Disposizioni transitorie", il quale ha riorganizzato le strutture amministrative della Giunta regionale, in considerazione delle esigenze organizzative derivanti dall'insediamento della nuova Giunta regionale e in attuazione di quanto disposto dalla legge regionale 14 agosto 2023, n. 10;

VISTO il regolamento regionale 28 dicembre 2023, n.12, concernente: "Modifiche al regolamento regionale 6 settembre 2002, n.1 (Regolamento di organizzazione degli uffici e dei servizi della giunta regionale) e successive modifiche. Disposizioni transitorie", con il quale sono state modificate le disposizioni transitorie del r.r. 9/2023;

VISTO l'art. 9, c. 1 del Regolamento Regionale 23 ottobre 2023, n. 9, come modificato dal r.r. 12/2023 in attuazione del quale, alla sottoscrizione del contratto del Direttore della Direzione Regionale Lavori pubblici e infrastrutture, innovazione tecnologica le competenze ed il personale delle strutture organizzative a rilevanza dirigenziale transitano tra Direzioni secondo quanto riportato alla Tabella 1 allegata Direttiva II del Direttore generale prot. n. 132306 del 30 gennaio 2024;

VISTE le Direttive I e II del Direttore generale in attuazione della riorganizzazione dell'apparato amministrativo di cui al regolamento regionale 23 ottobre 2023, n. 9 rispettivamente prot. n.1414222 del 5 dicembre 2023 e prot. n. 132306 del 30 gennaio 2024 nonché le prime indicazioni operative di attuazione delle stesse riportate nella nota prot. n. 171148 del 6 febbraio 2024;

VISTA la deliberazione della Giunta regionale n. 9 del 11 gennaio 2024, con il quale è stato conferito l'incarico di Direttore della Direzione regionale "Lavori Pubblici e Infrastrutture, Innovazione Tecnologica" all'Ing. Luca Marta;

VISTO l'art. 9, c. 2 del Regolamento Regionale 23 ottobre 2023, n. 9, come modificato dal r.r. 12/2023 in attuazione del quale, alla sottoscrizione del contratto del Direttore della Direzione Regionale Lavori pubblici e infrastrutture, innovazione tecnologica, avvenuta in data 1° febbraio 2024, è cessata la Direzione regionale per l'Innovazione tecnologica e la trasformazione digitale;

VISTA la determinazione della Direzione "Personale enti locali e sicurezza" n. G01325 del 09 febbraio 2024 recante "Assegnazione del personale della Direzione regionale "Lavori pubblici e infrastrutture, innovazione tecnologica";

VISTO l'Atto di Organizzazione n. G01353 del 12 febbraio 2024 con il quale è stato definito l'assetto organizzativo della Direzione Regionale Lavori pubblici e Infrastrutture, Innovazione Tecnologica;

PRESO ATTO che il contratto accessivo all'incarico di cui al punto precedente è stato sottoscritto in data 20/12/2023;

ATTESO che, pertanto, il presente atto, ancora intestato alla Direzione regionale "per l'Innovazione Tecnologica e la Trasformazione Digitale", nelle more dell'adeguamento degli applicativi gestionali alla nuova organizzazione amministrativa disposta con il r.r. 9/2023, debba intendersi riferito per competenza alla Direzione regionale "Lavori pubblici e infrastrutture, innovazione tecnologica";

VISTO l'articolo 30, comma 2, del Regolamento Regionale di Contabilità n. 26/2017, laddove "nel rispetto delle disposizioni di cui all'art. 56, comma 6, del D. Lgs. n. 118/2011 e del principio contabile applicato concernente la contabilità finanziaria di cui all'allegato n. 4/2 del citato Decreto Legislativo, per ogni provvedimento che comporta l'assunzione di un impegno di spesa, a valere sul bilancio annuale e pluriennale, deve essere predisposto il piano finanziario di attuazione nel quale è indicato, dettagliatamente, il cronoprogramma degli impegni e dei pagamenti, nonché le sue relative rimodulazioni";

VISTO l'art.10, comma 3 lettera a) del Decreto Legislativo n. 118/2011 che autorizza l'assunzione di impegni pluriennali;

ATTESO che ai sensi dell'art. 5 della Legge Regionale 24 novembre 2014, n. 12 la Regione Lazio ha costituito una Società per Azioni "in house providing" denominata "LAZIOcrea S.p.A.", per lo svolgimento di attività connesse all'esercizio di funzioni amministrative della Regione Lazio;

VISTA la Deliberazione di Giunta Regionale del 16 dicembre 2021, n. 952, con la quale è stato approvato lo schema del nuovo contratto quadro tra la Regione Lazio e LAZIOcrea - poi sottoscritto in data 29 dicembre 2021 e registrato al Registro cronologico con n. 25960 del 11 gennaio 2022;

CONSIDERATO che, come indicato nel suddetto contratto quadro, la LAZIOcrea S.p.A., società con capitale interamente regionale, opera nei confronti della Regione Lazio secondo le modalità dell'in house providing e pertanto, nel rispetto delle direttive regionali in materia di esercizio del controllo analogo, è soggetta ai poteri di programmazione, indirizzo strategico operativo e controllo della Regione, analogamente a quelli che quest'ultima

esercita sui propri uffici e servizi, fatta salva l'autonomia della Società stessa nella gestione dell'attività imprenditoriale e nell'organizzazione dei mezzi necessari al perseguimento dei propri fini statutari;

VISTO 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 la Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersicurezza";

VISTA la Determina ACN prot. n. 21472 dell' 8 agosto 2023 con la quale è stato approvato l'Avviso pubblico n. 06/2023 avente ad oggetto la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" a valere sul "Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice d'Investimento M1C1I1.5 (di seguito "Avviso") e i relativi allegati;

VISTA la Deliberazione di Giunta Regionale 29 dicembre 2023, n. 990, con la quale è stato approvato il Piano Operativo Annuale (POA) LAZIOcrea per l'anno 2024, e in particolare il Progetto/Servizio ICT "CYBERSECURITY: ISTITUZIONE DI UN CSIRT REGIONALE" (PNRRCSIRT) - scheda POA n. 22.27, pag. 861-863; Allegato B - SEZIONE B1, pag. 954, che riguarda CYBERSECURITY: ISTITUZIONE DI UN CSIRT REGIONALE;

CONSIDERATO che le competenze della Direzione Regionale Lavori Pubblici e Infrastrutture, Innovazione Tecnologica riguardano tra l'altro:

- Istituire e potenziare il Cyber Security Incident Response Team (CSIRT) regionale per innalzare il livello di cyber resilienza dell'organizzazione regionale, contribuendo alla definizione di un percorso virtuoso di monitoraggio e di miglioramento continuo nella gestione del rischio cyber, anche attraverso un team organizzato di esperti di cybersicurezza (CSIRT) il cui obiettivo principale è la gestione degli incidenti informatici e la realizzazione di servizi volti a prevenire, mitigare e risolvere gli impatti di incidenti informatici;

VISTO il Piano Nazionale di Ripresa e Resilienza (PNRR), trasmesso dal Governo Italiano alla Commissione Europea il 30 aprile 2021 ai sensi degli articoli 18 e seguenti del Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021, che definisce un quadro di investimenti e riforme a livello nazionale, con corrispondenti obiettivi e traguardi cadenzati temporalmente, al cui conseguimento si lega l'assegnazione di risorse finanziarie messe a disposizione dall'Unione Europea;

VISTO il Piano Nazionale di Ripresa e Resilienza (PNRR) approvato con Decisione del Consiglio ECOFIN del 13 luglio 2021 e notificato all'Italia dal Segretario Generale del Consiglio con nota LT161/21 del 14 luglio 2021;

VISTO il Decreto Legge del 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge del 29 luglio 2021, n. 108, recante "Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure" nel quale, in ordine all'organizzazione della gestione del Piano Nazionale di Ripresa e Resilienza, vengono definiti i ruoli ricoperti dalle diverse amministrazioni coinvolte nonché le modalità di monitoraggio del Piano e del dialogo con le autorità europee e nel quale si prevedono misure di semplificazione che incidono in alcuni dei settori oggetto del PNRR al fine di favorirne la completa realizzazione;

RICHIAMATO quanto riportato all'art. 12 comma 1 del Decreto Legge del 31 maggio 2021, n.77, "*In caso di mancato rispetto da parte delle Regioni, delle province autonome di Trento e di Bolzano, delle città metropolitane, delle province e dei comuni degli obblighi e impegni finalizzati all'attuazione del PNNR e assunti in qualità di soggetti attuatori, consistenti anche nella mancata adozione di atti e provvedimenti necessari all'avvio dei progetti del Piano, ovvero nel ritardo, inerzia o difformità nell'esecuzione dei progetti, il Presidente del Consiglio dei ministri, ove sia messo a rischio il conseguimento degli obiettivi intermedi e finali del PNRR e su proposta della Cabina di regia o del Ministro competente, assegna al soggetto attuatore interessato un termine per provvedere non superiore a trenta giorni. In caso di perdurante inerzia, su proposta del Presidente del Consiglio dei ministri o del Ministro competente, sentito il soggetto attuatore, il Consiglio dei ministri individua l'amministrazione, l'ente, l'organo o l'ufficio, ovvero in alternativa nomina uno o più commissari ad acta, ai quali attribuisce, in via sostitutiva, il potere di adottare gli atti o provvedimenti necessari ovvero di provvedere all'esecuzione ai progetti, anche avvalendosi di società di cui all'art. 2 del decreto legislativo 19 agosto 2016, n. 175 o di altre amministrazioni specificamente indicate*";

VISTO il Decreto-legge del 6 maggio 2021, n. 59, convertito con modificazioni dalla Legge del 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";

VISTO il Decreto-legge del 9 giugno 2021, n. 80, convertito con modificazioni dalla Legge del 6 agosto 2021, n. 113, recante "Misure urgenti per il rafforzamento delle capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) e per l'efficienza della giustizia";

VISTO il Decreto del Ministero dell'Economia e delle Finanze del 06 agosto 2021 – G.U. n. 229 del 24 settembre 2021 - relativo all'assegnazione delle risorse finanziarie in favore di ciascuna Amministrazione titolare degli interventi PNRR e corrispondenti Milestone e Target previsti per l'attuazione degli stessi e ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione;

VISTI i principi trasversali previsti nel PNRR, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (c.d. tagging), il principio di parità e di genere e l'obbligo di protezione e valorizzazione dei giovani;

VISTI gli obblighi di assicurare il conseguimento di Milestone e Target e degli obiettivi finanziari stabiliti nel PNRR e nel PNC;

VISTO l'art. 6 del citato Decreto-legge 31 maggio 2021, n. 77, ai sensi del quale sono attribuiti al Servizio centrale per il PNRR, quale punto di contatto nazionale con la Commissione europea ai sensi dell'art. 22 del Regolamento (UE) 2021/241, funzioni di coordinamento operativo, monitoraggio, rendicontazione e controllo del PNRR;

VISTA la Deliberazione di Giunta Regionale del 9 novembre 2021, n. 755, recante: "Governance operativa regionale per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) e del Piano Nazionale Complementare al PNRR (PNC)";

VISTA la Legge n. 48 del 18 marzo 2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno";

VISTO il Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, che contiene un primo modello di governance sulla cyber security e indica nel DIS ("Dipartimento per le informazioni della sicurezza") e nel CISR (Comitato Interministeriale per la Sicurezza della Repubblica) i principali riferimenti di coordinamento;

VISTO il regolamento UE 2014/910, Regolamento Electronic Identification Authentication and Signature (Regolamento EIDAS), entrato in vigore il 17 settembre 2014, applicabile dallo scorso primo luglio, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che sostituisce il quadro normativo definito dalla Direttiva Europea 1999/93/EC sulle firme elettroniche e dalle relative leggi nazionali di recepimento;

VISTO il Regolamento (UE) 2016/679 sulla protezione dei dati;

VISTO il Decreto Legislativo n. 101 del 19 settembre 2018, con cui si adeguava il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679;

VISTA la direttiva UE n. 2016/680, entrata in vigore il 24 maggio 2016, sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI del Consiglio;

VISTA la direttiva n. 1148/2016, Direttiva Network and Information Security (Direttiva NIS) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

VISTA la Legge del 4 agosto 2021, n. 109, che ha convertito con modificazioni il Decreto-legge 14 giugno 2021, n. 82 recante "Disposizioni urgenti in materia di cyber sicurezza, definizione dell'architettura nazionale di cyber sicurezza e istituzione dell'Agenzia per la cyber sicurezza nazionale;

VISTA la Circolare 17/03/2017, n. 1/2017 pubblicata in Gazzetta Ufficiale (GU Serie Generale n.79 del 04/04/2017) dove si indicano le misure minime di sicurezza informatica che tutte le PA devono adottare entro il 31/12/2017 per proteggere il patrimonio informatico e i dati gestiti al loro interno;

VISTA la Direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva NIS – Network and Information Security") con la finalità di assicurare un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione Europea";

CONSIDERATA la Deliberazione della Giunta Regionale n. 113 del 28 febbraio 2024 concernente "Bilancio di previsione finanziario della Regione Lazio 2024-2026 – Variazione di bilancio, in termini di competenza e cassa, per l'anno 2024 e, in termini di competenza, per l'anno 2025, a integrazione del capitolo di entrata E0000229184 e del capitolo di spesa U0000S25107", con cui si assegnava nella competenza della Direzione regionale "Lavori pubblici e infrastrutture, Innovazione tecnologica, ai fini della relativa gestione, il capitolo di entrata di nuova istituzione E0000229184 e il capitolo di spesa di nuova istituzione U0000S25107";

VISTA la Determina ACN prot. n. 21472 dell'8 agosto 2023 con la quale è stato approvato l'Avviso pubblico n. 06/2023 avente ad oggetto la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" a valere sul "Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice d'Investimento M1C1I1.5 (di seguito "Avviso") e i relativi allegati;

VISTA la Determina ACN prot. n. 30697 del 30 novembre 2023 concernente Avviso Pubblico n. 06/2023 recante "Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5".Determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse";

VISTA la nota della Società LAZIOcrea S.p.A., prot. 2058 del 06 febbraio 2024, acquisita con prot, regionale n. 312088 del 06 marzo 2024, con cui si trasmetteva trasmette lo studio di fattibilità relativo al progetto a valere sui fondi PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 (id progetto: 4_WP7_A6_Regione Lazio – CUP: F84F23000230006), per la realizzazione di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici, per un valore complessivo del progetto pari ad Euro 1.255.327,87 oltre IVA (Euro 1.531.500,00 IVA inclusa - rendicontabili su fondi di natura corrente);

TENUTO CONTO che il 6 marzo 2024 con protocollo 315044 di pari data, è stata inviata dalla "Direzione Lavori Pubblici e Infrastrutture, Innovazione Tecnologica" all'Agenzia per la Cybersicurezza Nazionale, comunicazione di avvio attività per il progetto denominato 4_WP7_A6_Regione Lazio - CSIRT REGIONE LAZIO approvato con Determinazione n. 30697 DEL 30/11/2023 CUP F84F23000230006 della graduatoria definitiva delle proposte progettuali totalmente finanziabili ammesse in seguito all'Avviso Pubblico n. 06/2022 per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 WP-9;

VISTO il nuovo Studio di Fattibilità trasmesso dalla Società LAZIOcrea S.p.A. con prot. n. 4138 del 12 marzo 2024, acquisito con prot. reg. n. 342736 con pari data, con cui si comunicava il nuovo valore complessivo dell'iniziativa progettuale, pari ad Euro 1.500,000,00 Iva inclusa, per le annualità 2024 e 2025;

VISTA la nota della Società LAZIOcrea S.p.A., prot. 4451 del 15 marzo 2024, acquisita con prot. regionale n. 371156 del 18 marzo 2024, con cui si trasmetteva un nuovo studio di fattibilità che prevede che il suindicato progetto abbia una durata complessiva di 21 mesi, con un kick-off previsto per il mese di aprile 2024, e con un preventivo aggiornato del costo complessivo, e relativa suddivisione degli importi per annualità, per un valore complessivo pari ad Euro 1.500.000,00 IVA inclusa - rendicontabili su fondi di natura corrente;

RITENUTO di dover procedere alla nomina del responsabile del procedimento ai sensi degli artt. 4, 5 e 6 della Legge 241/90 individuando il Direttore della Direzione Regionale Lavori Pubblici e Infrastrutture, Innovazione Tecnologica, l'Ing Luca Marta;

RILEVATO che il pagamento avverrà sulla base di quanto indicato nel piano di attuazione;

CONSIDERATA l'urgenza e l'indifferibilità di consolidare le capacità di gestione degli incidenti informatici mediate la costituzione di un team organizzato di esperti di cybersicurezza dando attuazione all'intervento del PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5;

VISTO l'articolo 25 c. 2 del Codice degli Appalti (D.Lgs n. 36/2023) secondo cui le stazioni appaltanti e gli enti concedenti utilizzano le piattaforme di approvvigionamento digitale per svolgere le procedure di affidamento e di esecuzione dei contratti pubblici, secondo le regole tecniche di cui all'articolo 26;

VISTO l'articolo 7 c. 2 del Codice degli Appalti (D.Lgs n. 36/2023) secondo cui Le stazioni appaltanti e gli enti concedenti adottano per ciascun affidamento un provvedimento motivato in cui danno conto dei vantaggi per la collettività, delle connesse esternalità e della congruità economica della prestazione, anche in relazione al perseguimento di obiettivi di universalità, socialità, efficienza, economicità, qualità della prestazione, celerità del procedimento e razionale impiego di risorse pubbliche;

RITENUTO necessario:

- istituire e potenziare il Cyber Security Incident Response Team (CSIRT) regionale per innalzare il livello di cyber resilienza dell'organizzazione regionale;
- contribuire alla definizione di un percorso virtuoso di monitoraggio e di miglioramento continuo nella gestione del rischio cyber, anche attraverso un team organizzato di esperti di cybersicurezza (CSIRT);
- raggiungere l'obiettivo di una gestione degli incidenti informatici e della realizzazione di servizi volti a prevenire, mitigare e risolvere gli impatti di incidenti informatici;

RITENUTO NECESSARIO, per le motivazioni sopra addotte:

- procedere alla nomina del Responsabile Unico di Progetto ai sensi dell'art. 15 del D.lgs. n. 36/2023 - per le fasi di programmazione e affidamento - individuando il Direttore della Direzione Regionale Lavori Pubblici e Infrastrutture, Innovazione Tecnologica, l'Ing Luca Marta;
- incaricare la società LazioCrea S.p.A. per la fase di esecuzione dell'appalto che provvederà alla nomina del RUP, individuando l'opportuna figura professionale competente e responsabile;
- approvare il Documento ALLEGATO B – PIANO DI PROGETTO CSIRT REGIONE LAZIO della Regione Lazio relativo all' AVVISO PUBBLICO 6/2023 a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 (Allegato 1 alla presente Determinazione Dirigenziale);
- approvare il Documento ALLEGATO C – ATTO D'OBBLIGO relativo all' Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 (Allegato 2 alla presente Determinazione Dirigenziale);
- accertare l'importo di € 1.500.000,00 sul capitolo di entrata E0000229184, come da tabella sotto riportata:

Capitolo di entrata	PIANO DEI CONTI FINANZIARIO - Titolo/Tipologia – Descrizione	Accertamento Anno 2024 in euro IVA inclusa	Accertamento Anno 2025 in euro IVA inclusa	DEBITORE
E0000229184	PCF: 2.01.01.01.001 TIT/TIP: 2.01.01 ENTRATE DERIVANTI DAL PNRR - DETERMINAZIONE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE, REGISTRO PROT. N. 30697 DEL 30/11/2023 - M1C1I1.5 CYBERSECURITY	750.000,00	750.000,00	Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280)

- impegnare a favore di LAZIOcrea (codice creditore 164838) la somma complessiva di € 1.500.000,00 Iva inclusa sul capitolo U0000S25107 per l'Intervento Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5"., esercizi finanziari 2024-2025, come da tabella sotto riportata:

Capitolo di spesa	PIANO DEI CONTI FINANZIARIO - MISSIONE/PROGRAMMA – Descrizione	Progetto/servizio ICT	Tipologia di spesa	Impegno Anno 2024 in euro IVA inclusa	Impegno Anno 2025 in euro IVA inclusa	CREDITORE
U0000S25107	PCF: 1.03.02.99.010 MISS/PRG: 1.12 PNRR - DETERMINAZIONE DELL'AGENZIA PER LA CYBERSICUREZZA	PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5" Istituzione e potenziamento del Cyber	Formazione a personale esterno all'ente	750.000,00	750.000,00	LAZIOcrea (codice creditore 164838)

	NAZIONALE, REGISTRO PROT. N. 30697 DEL 30/11/2023 - M1C1I1.5 CYBERSECURITY § ALTRI SERVIZI	Security Incident Response Team (CSIRT) regionale				

- dare atto che le obbligazioni riferite ai suddetti impegni giungeranno in scadenza come espresso nel piano di attuazione finanziario redatto ai sensi dell'art. 30, comma 2, del r.r. di contabilità n. 26/2017;

DETERMINA

per le motivazioni di cui in premessa che si intendono integralmente richiamate:

- di procedere alla nomina del responsabile del procedimento ai sensi degli artt. 4, 5 e 6 della Legge 241/90 individuando il Direttore della Direzione Regionale Lavori Pubblici e Infrastrutture, Innovazione Tecnologica, l'Ing Luca Marta;
- incaricare la società LazioCrea S.p.A. per la fase di esecuzione dell'appalto che provvederà alla nomina del RUP, individuando l'opportuna figura professionale competente e responsabile;
- di approvare il Documento ALLEGATO B – PIANO DI PROGETTO CSIRT REGIONE LAZIO della Regione Lazio relativo all' AVVISO PUBBLICO 6/2023 a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 (Allegato 1 alla presente Determinazione Dirigenziale);
- di approvare il Documento ALLEGATO C – ATTO D'OBBLIGO relativo all' Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 (Allegato 2 alla presente Determinazione Dirigenziale);
- di accertare l'importo di € 1.500.000,00 sul capitolo di entrata E0000229184, come da tabella sotto riportata:

Capitolo di entrata	PIANO DEI CONTI FINANZIARIO - Titolo/Tipologia – Descrizione	Accertamento Anno 2024 in euro IVA inclusa	Accertamento Anno 2025 in euro IVA inclusa	DEBITORE
E0000229184	PCF: 2.01.01.01.001 TIT/TIP: 2.01.01 ENTRATE DERIVANTI DAL PNRR - DETERMINAZIONE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE, REGISTRO PROT. N. 30697 DEL 30/11/2023 - M1C1I1.5 CYBERSECURITY	750.000,00	750.000,00	Agenzia per la Cybersicurezza Nazionale (cod. debitore 246280)

- di impegnare a favore di LAZIOcrea (codice creditore 164838) la somma complessiva di € 1.500.000,00 Iva inclusa sul capitolo U0000S25107 per l'Intervento Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5"., esercizi finanziari 2024-2025, come da tabella sotto riportata:

Capitolo di spesa	PIANO DEI CONTI FINANZIARIO - MISSIONE/PROGRAMMA – Descrizione	Progetto/servizio ICT	Tipologia di spesa	Impegno Anno 2024 in euro IVA inclusa	Impegno Anno 2025 in euro IVA inclusa	CREDITORE
U0000S25107	PCF: 1.03.02.99.010 MISS/PRG: 1.12 PNRR - DETERMINAZIONE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE, REGISTRO PROT. N. 30697 DEL 30/11/2023 - M1C1I1.5 CYBERSECURITY § ALTRI SERVIZI	PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5" Istituzione e potenziamento del Cyber Security Incident Response Team (CSIRT) regionale	Formazione a personale esterno all'ente	750.000,00	750.000,00	LAZIOcrea (codice creditore 164838)

- di provvedere alla pubblicazione del presente atto sul B.U.R.L. e sul sito web istituzionale della Regione Lazio alla Sezione "Amministrazione trasparente".

Avverso la presente determinazione è ammesso ricorso giurisdizionale dinanzi al Tribunale Amministrativo Regionale del Lazio entro 30 giorni dalla sua pubblicazione.

Il Direttore
Ing. Luca Marta

AVVISO PUBBLICO 6/2023

a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici

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

M1C1I1.5

ALLEGATO B – PIANO DI PROGETTO

CSIRT REGIONE LAZIO

Regione Lazio

Sezione 1 – ANAGRAFICA DEL SOGGETTO PROPONENTE

1.A Dati identificativi del Soggetto proponente	
Denominazione	Regione Lazio
Codice IPA	r_lazio
posta elettronica certificata (PEC)	direzione.itd@regione.lazio.legalmail.it
1.B Dati identificativi del titolare del potere di impegnare il Soggetto proponente *(come riportato nell'Allegato A)*	
Nome e Cognome	Stefano Calabrese
Qualifica	Responsabile per la Transizione al Digitale
Riferimenti di contatto	Mail: scalabrese@regione.lazio.it N. Telefono: 06 51688616, 06 51685367, 06 51685100
1.C Dati identificativi del Responsabile del Progetto proposto *(da valorizzare se diverso dal Soggetto di cui al punto 1B)*	
Nome e Cognome	_____
Qualifica	_____
CF	_____
Nato a *(indicare il luogo e la data di nascita)*	_____
Riferimenti di contatto	Mail: _____ N. Telefono: _____

Sezione 2 – ANAGRAFICA DEL PROGETTO PROPOSTO

2.A Codice Unico di Progetto (CUP) *Indicare il CUP e la tipologia*	CUP: F84F23000230006 ☒ generato in coerenza con le indicazioni di cui al Template CUP "PNRR ☐ già in possesso, in quanto progetto già avviato
2.B Tipologie di attività progettuali che si intende realizzare *Indicare le tipologie di attività progettuali che si intende realizzare nell'ambito del progetto proposto finalizzate al rafforzamento dell'organizzazione, delle competenze, delle tecnologie o dei processi di uno o più Area, come descritte nel par. 4.1*	☒ 1. Analisi, disegno e razionalizzazione dei processi in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato ☒ 2. Adeguamento e rafforzamento del modello organizzativo e potenziamento delle competenze professionali ☒ 3. Definizione, implementazione e miglioramento degli strumenti in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato ☒ 4. Definizione, implementazione e miglioramento finalizzato ai settori sanitario e/o efficientamento energetico e/o tutela del territorio e delle risorse idriche.
2.C Tempistiche di avvio del progetto proposto *Nel caso di progetto già avviato, si richiede di indicare la data di avvio del progetto che dovrà essere – in conformità a quanto previsto al par. 7 dell'Avviso – successiva al 1° febbraio 2020* *Nel caso di progetto da avviare ex novo, si richiede di indicare le tempistiche massime (in gg lavorativi) previste per l'avvio del*	☐ Progetto già avviato in data _____ ☒ Progetto da avviare *ex novo* entro 10 giorni dalla data di trasmissione dell'Atto d'Obbligo sottoscritto

progetto a valere dalla data di trasmissione dell'Atto d'Obbligo sottoscritto, nel rispetto della tempistica massima indicata al par. 4.3 dell'Avviso pari a 10 giorni lavorativi	
2.D Tempistiche di conclusione del progetto *Si richiede di indicare la data presunta di conclusione del progetto, ivi inclusi gli adempimenti connessi alla rendicontazione dello stesso.* *Nel caso in cui il progetto presentato preveda lo svolgimento di attività di cui ai punti 1), 2) e 3) del paragrafo 4.1, il progetto dovrà concludersi entro 24 mesi dalla data di trasmissione dell'Atto d'obbligo e comunque non oltre la data del 31 dicembre 2024.* *Nel caso in cui il progetto presentato preveda anche lo svolgimento di attività di cui al punto 4) del paragrafo 4.1, limitatamente a quest'ultime, i progetti ammessi a finanziamento potranno concludersi entro e non oltre la data del 31 dicembre 2025.*	Nel caso di previsione di attività di cui ai punti 1) e/o 2) e/o 3) del par. 4.1: 31/12/2024 Nel caso di previsione di attività di cui al punto 4) del par. 4.1: 31/12/2025

Sezione 3 – CARATTERISTICHE AS-IS DEL CSIRT REGIONALE

3.A Descrizione sintetica dei servizi attualmente offerti dal CSIRT o dalla struttura organizzativa del Soggetto proponente attualmente deputata alla gestione degli incidenti informatici *Max 200 parole*
Regione Lazio (di seguito anche "Ente"), con il supporto tecnico ed attuativo di LAZIOcrea, ha definito dal 2019 un piano strategico in materia di Cybersecurity comprendente iniziative progettuali volte a migliorare la postura di sicurezza, tra cui la progettazione e realizzazione di un Computer Emergency Response Team ("CERT") a livello Regionale, il cui compito è coordinare le azioni necessarie per limitare gli effetti degli incidenti e ripristinare le normali condizioni operative. Inoltre, il CERT fornisce servizi di prevenzione, formazione e sensibilizzazione alla sua comunità di riferimento sul tema della sicurezza informatica. L'istituzione ed il continuo miglioramento dei servizi erogati dal CERT a beneficio dell'ecosistema Regionale risulta fondamentale non solo per le dimensioni e la complessità organizzativa dei sistemi informativi gestiti, ma soprattutto per le categorie di dati trattati in termini di criticità e rilevanza. Nei primi mesi del 2023, con il supporto di LAZIOcrea, l'Ente ha attivato le seguenti iniziative legate alla progettazione di un CERT: • analisi e revisione delle attuali prassi per la gestione degli incidenti di sicurezza • realizzazione di un piano di Crisis Communication da utilizzare in occasione di specifici eventi. Nell'ambito delle iniziative di rafforzamento della sicurezza informatica, Regione Lazio, con D.G.R. n. 1195/2022, ha approvato lo Schema di Convenzione con il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) del Ministero dell'Interno per consolidare e potenziare le misure di prevenzione dei crimini informatici sui sistemi informativi critici della Giunta regionale.
3.B *(Se già presente un CSIRT o struttura organizzativa deputata alla gestione degli incidenti informatici)* **Descrizione sintetica dei processi, modello organizzativo e strumenti in essere per la gestione degli incidenti informatici**

Max 300 parole
Nell'ambito delle iniziative tecnologiche legate alla progettazione e realizzazione del CERT Regionale, in corso di progressiva attivazione dai primi mesi del 2023, con il supporto di LAZIOcrea, in qualità di in-house e di principale erogatore di Servizi, è stata posta particolare attenzione ai seguenti ambiti: • analisi, evoluzione ed utilizzo di una piattaforma per la gestione end-to-end degli incidenti di sicurezza informatica, • predisposizione di indicatori e dashboard per il monitoraggio periodico degli aspetti cyber • analisi e revisione delle logiche di allarmistica sulle piattaforme di monitoraggio, al fine di poter migliorare le capability di detection • pianificazione di verifiche tecnologiche volte a valutare la robustezza dei sistemi IT gestiti e individuare eventuali vulnerabilità. Parallelamente alle iniziative volte all'ampliamento e miglioramento del CERT Regionale, il piano di Security Enforcement attuato col supporto di LAZIOcrea per l'evoluzione della postura di sicurezza prevede le seguenti progettualità in corso di attivazione dai primi mesi del 2023: • progettazione e attivazione di un servizio di monitoraggio h24 degli eventi di sicurezza e Security Intelligence; • revisione e aggiornamento di regole e politiche finalizzate al miglioramento dei processi di detection e response degli attacchi informatici; • definizione di requisiti funzionali e tecnici volti all'identificazione di possibili soluzioni tecnologiche per la rilevazione di minacce e vulnerabilità; • analisi del livello di maturità cyber, definizione del piano strategico e di attuazione delle misure di miglioramento identificate di breve-medio e lungo periodo; • identificazione degli elementi di evoluzione, ottimizzazione e adeguamento tecnologico relativi alla progettazione del Security Operation Center (SOC), definizione delle azioni correlate.

Sezione 4 – PROPOSTA PROGETTUALE PER L'ATTIVAZIONE E/O IL POTENZIAMENTO DEL CSIRT REGIONALE

4.A Mandato del CSIRT Regionale previsto al completamento della proposta progettuale

(descrive gli obiettivi di base di un CSIRT, in termini di servizi forniti verso la Regione o Provincia Autonoma)

Max 300 parole

Con il presente progetto, Regione Lazio intende ora attivare e potenziare i servizi di:

- Disegno del **Modello** in termini di processi, modello organizzativo e servizi che verranno erogati alla constituency con l'obiettivo di declinare i ruoli e le responsabilità interne a Regione Lazio, il modello operativo e le modalità di adesione da parte dei futuri membri della constituency.
- Disegno delle **Procedure e dei Processi** interni e condivisi con i membri della Constituency per identificare nettamente le responsabilità ed azioni in carico a ciascun Ente e/o fornitore coinvolto mediante apposita RACI, disegno del flusso di lavoro per la gestione degli eventi ed incidenti di sicurezza, nonché degli ulteriori servizi direttamente erogati dal CSIRT sulla base delle Linee Guida promosse dall'Agenzia Nazionale per la Cybersicurezza.
- Security Intelligence verso un concetto più ampio di **Digital Risk Protection**, al fine di prevenire e ridurre la probabilità di occorrenza di diverse minacce informatiche potenziando le capacità di identificazione e monitoraggio dell'esposizione digitale dell'Ente e, al contempo, condividendo tali informazioni verso i CSIRT attivati a livello nazionale per caratterizzare al meglio le vulnerabilità applicabili alla superficie di attacco. In particolare, attraverso la ricerca di dati e informazioni sensibili su fonti OSINT (Open Source INTelligence), CLOSINT (CLOsed Source INTelligence), Deep e Dark Web, sarà possibile rilevare eventuali perdite di dati, proteggere il business e la reputazione aziendale.
- Security Incident Management attraverso l'inserimento di capability di ***Automation*** e ***Orchestration***, in grado di rilevare le attività ripetitive svolte dal personale di sicurezza e definire successivamente dei possibili scenari di automazione; attraverso un'analisi puntuale dei benefici, sarà possibile calcolare per tali scenari il livello di efficienza ed efficacia e valutare, infine, la relativa implementazione.

- **Knowledge Transfer** inteso come fasi e momenti di formazione ovvero training-on-the-job degli attori interni al CSIRT regionale per supportarli nel recepimento delle politiche e procedure nonché nell'esecuzione autonoma delle attività di natura tecnica, con l'obiettivo di potenziare le conoscenze e le capabilities interne al CSIRT.

4.B Constituency del CSIRT Regionale previsto al completamento della proposta progettuale

(*descrivere il perimetro di intervento del CSIRT Regionale che si intende attivare e/o potenziale, vale a dire i sistemi informativi rispetto ai quali vengono erogati i servizi inclusi nel Mandato*)

Max 300 parole

Il CSIRT di Regione Lazio erogherà i propri servizi in relazione ai sistemi informativi Regionali erogati a beneficio degli Enti dell'ecosistema tramite il supporto di LAZIOcrea in qualità di in-house.
Nello specifico, i servizi verranno erogati dal CSIRT a beneficio anche degli Enti Sanitari, con particolare riferimento ai servizi critici gestiti centralmente dall'Amministrazione regionale a beneficio delle ASL/AO:

- Anagrafe Vaccinale Regionale
- Sistema Regionale gestione ausili assistenza Protesica
- Cartella Sociale
- Sistema Informativo per l'Assistenza Territoriale Sociale SIATESS
- Distinta Contabile Riepilogativa
- Gestione piani terapeutici Epatite C
- Piani Terapeutici Farmaci Biologici
- Sistema Gestione Piani terapeutici
- Sistema Informativo Assistenza Domiciliare
- Sistema Informativo Assistenza Riabilitativa (ex-art.26)
- Sistema Informativo Residenze Sanitarie Assistenziali

- Acquisizione gestione dati pronto soccorso
- Acquisizione gestione dati pronto soccorso
- Acquisizione gestione dati pronto soccorso
- Anagrafe Sanitaria Unica Regionale
- Registro Regionale Dialisi e Trapianto Lazio
- Piattaforma per la gestione e prenotazione delle prestazioni ambulatoriali
- Colleziona tutti i dati dei tamponi, quarantene, positivi e guariti COVID19
- Gipse-web - Pronto Soccorso
- Sistema Informativo Assistenza Territoriale
- Sistema Informativo Assistenza Territoriale e SocioSanitaria
- Fascicolo Sanitario Elettronico
- Sistema Trasfusionale
- Ricetta Digitale
- Cartella diabetologica
- Sistema Informativo Ospedaliero
- Sistema di gestione del Rischio Clinico

In visione prospettica, le PAL (Pubbliche Amministrazioni Locali) facenti parte della constituency potranno accedere direttamente ai servizi offerti dal CERT di Regione Lazio a valle di un processo di accreditamento che prevederà come requisiti:

- la nomina di referenti unici per la sicurezza delle informazioni, i quali saranno punto di contatto unico verso i referenti del CERT di Regione Lazio;
- la comprovata disponibilità di personale minimo e sufficiente per espletare attività correlate;
- un adeguato budget dedicato alla sicurezza al fine di supportare azioni correttive ed evolutive (es. onboarding di nuove fonti e log, configurazioni aggiuntive, aggiornamento dei sistemi di sicurezza, ecc.) che rimarranno in capo ad esse.

Tramite l'adesione al CERT, le Amministrazioni aderenti alla *constituency* potranno attivare i servizi offerti per la gestione degli incidenti di sicurezza informatica sulla base di modalità attuative regolamentate da protocolli di comunicazione e da procedure operative di risoluzione ed *escalation*, nonché supporto negli ulteriori servizi erogati sulla base del modello operativo che verrà definito.

4.C Descrizione sintetica del modello di servizio del CSIRT Regionale che si intende attivare e/o potenziare

(descrivere i principali obiettivi della proposta progettuale in coerenza con le linee guida al fine di attivare e/o potenziare un CSIRT in conformità al profilo di maturità minimo, c.d. "profilo base")

Max 300 parole

Modello Organizzativo e Operativo del CSIRT

In linea con quanto definito nel paragrafo 3, servizio 9.4 "Processi" delle Linee Guida ACN, tale attività ha l'obiettivo di definire il modello organizzativo per la costituzione di un CSIRT Regionale che verrà affidato alla società in house LAZIOcrea nell'ambito del Contratto Quadro di Servizio. L'attività è essenziale per contribuire al raggiungimento del livello di maturità base definito da ENISA e dalle Linee Guida ACN.

Processi e Procedure

In linea con quanto definito nel paragrafo 3, servizio 9.4 "Processi" delle Linee Guida ACN, tale attività ha l'obiettivo di produrre e diffondere, internamente ai membri della constituency, politiche e procedure per la gestione degli eventi e degli incidenti di sicurezza e gli ulteriori servizi erogati dal CSIRT, con esplicito riferimento alla definizione di ruoli e responsabilità ai soggetti incaricati. L'attività è essenziale per contribuire al raggiungimento del livello di maturità base definito da ENISA e dalle Linee Guida ACN.

Digital Risk Protection

In linea con quanto definito nel paragrafo 3, servizi 5.1 "Monitoring and Detection" e 8.3 "Communication", delle Linee Guida ACN, tale attività ha l'obiettivo di potenziare le misure di sicurezza atte a prevenire i rischi cyber e a potenziare lo scambio di informazioni e la collaborazione sinergica sia tra i diversi CSIRT attivati a livello regionale sia con lo CSIRT di ACN.

Automation

In linea con quanto definito nel paragrafo 3, servizio 5.1 “Monitoring and Detection”, delle Linee Guida ACN, tale attività ha l’obiettivo di individuare e introdurre nuove soluzioni di automazione che supportino il personale di sicurezza nel migliorare l’efficacia e la tempestività di gestione delle minacce potenziali e degli incidenti cibernetici.

Knowledge Transfer

In linea con quanto definito nel par. 3, servizio 9.2.3 “Knowledge Transfer”, delle Linee Guida ACN, tale attività ha l’obiettivo di supportare i membri interni del CSIRT nel costante e continuativo aggiornamento dele competenze necessarie a svolgere le attività operative giornaliere del CSIRT.

4.D In coerenza con le Linee Guida, indicare le Aree di operatività che si intende attivare e/o potenziare

Selezionare, per ciascuna Area di operatività, le funzioni che si intende erogare all’esito del progetto presentato

Area	Servizio	Funzione
Info Security Event Management	Monitoring and Detection	☐ Log and sensor management ☒ Detection use case management ☒ Contextual data management
	Event Analysis	☐ Correlation ☐ Qualification
Info Security Incident Management	Information security incident report acceptance	☒ Info Security Incident report receipt ☐ Info security Incident Triage and processing
	Information security incident analysis	☐ Info Security Incident Triage ☐ Information collection

		☐ Detailed analysis coordination ☐ Info Security Incident root cause analysis ☒ Cross – incident correlation
	Artifact and forensic evidence analysis	☐ Media or surface analysis ☐ Reverse engineering ☐ Run time or dynamic analysis ☐ Comparative analysis
	Mitigation and recovery	☐ Response plan establishment ☐ Ad hoc measures and containment ☐ System restoration ☐ Other Info Security entities support
	Information security incident coordination	☒ Communication ☒ Notification distribution ☒ Relevant information distribution ☒ Activities coordination ☒ Reporting ☐ Media communication
	Crisis management support	☐ Information distribution to constituents ☐ Information Security Status reporting ☐ Strategic decisions communication
Vulnerability Management	Vulnerability Discovery/ Research	☐ Incident response vulnerability discovery ☒ Public source vulnerability Discovery ☒ Vulnerability Research
	Vulnerability Report intake	☐ Vulnerability report receipt ☐Vulnerability report triage and processing
	Vulnerability Analysis	☐ Vulnerability Triage

		☐ Vulnerability root cause analysis ☐ Vulnerability remediation development
	Vulnerability coordination	☐ Vulnerability notification/ reporting ☐Vulnerability Stakeholder coordination
	Vulnerability disclosure	☐ Vulnerability disclosure policy and infrastructure maintenance ☐ Vulnerability announcements/ Communication/ dissemination ☐ Post- vulnerability Disclosure feedback
	Vulnerability Response	☐ Vulnerability detection/scanning ☐ Vulnerability remediation
Situational Awareness	Data acquisition	☐ Policy aggregation distillation, and guidance ☐ Asset mapping to function, roles, actions, and key risks ☐ Collection ☐ Data processing and preparation
	Analysis and Synthesis	☐ Projection and inference ☐ Event detection ☐ Info Security incident management decision support ☐ Situational impact
	Communication	☐ Internal and External communication ☐ Reporting and recommendations ☐ Implementation ☒ Dissemination/ Integration/ Information sharing ☐ Management of Info Sharing ☐ Feedback
Knowledge Transfer	Awareness Building	☐ Research and information aggregation ☐ Reports and awareness materials development

		☐ Information dissemination ☐ Outreach
	Training and Education	☐ Knowledge, skill, and ability requirements gathering ☐ Educational and training materials development ☐ Content delivery ☐ Mentoring ☒ CSIRT staff professional development
	Exercises	☐ Requirements analysis ☐ Format and environment development ☐ Scenario development ☐ Exercises execution ☐ Exercise outcome review
	Technical and Policy	☐ Risk management support ☐ Business continuity and disaster recovery planning support ☒ Policy support ☒ Technical advice

4.E *(Se previsto)* **In coerenza con le Linee Guida, descrivere l'approccio metodologico proposto per l'analisi, il disegno e la razionalizzazione dei processi che si intendono attivare e/o potenziare in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio Mandato**

Max 300 parole

Nell'ambito dell'analisi e potenziamento del **Modello** e delle **Procedure**, essenziali per traguardare il livello di maturità base definito da ENISA e dalle Linee Guida ACN, si intende adottare un approccio agile e condiviso il quale:

- Normalizzi e consolidi la nomenclatura e le tassonomie, così come persone di riferimento, già esistenti nel SOC e nel CERT di Regione Lazio;
- Individui precisi ruoli e responsabilità da assegnare ai membri del CSIRT affinché le attività di risposta agli incidenti abbiano ownership ben definite, anche attraverso la valorizzazione di canali di escalation formalmente accordati con il SOC ed il CERT esistenti;
- Instauri, tra il CSIRT ed altri enti istituzionali (es. C.N.A.I.P.I.C., CSIRT nazionale e ulteriori CSIRT Regionali), una collaborazione continua basata sull'interscambio di informazioni afferenti a nuove vulnerabilità, incidenti di sicurezza ed eventi avversi critici con l'obiettivo di massimizzare la cooperazione tra gli attori coinvolti.

Nell'ambito dell'analisi e potenziamento del processo di **Digital Risk Protection**, si intende adottare un approccio metodologico che prevede:

- normalizzazione delle informazioni raccolte affinché vengano condivise fra i diversi CSIRT eventualmente attivi a livello nazionale;
- il censimento degli asset e delle principali aree da monitorare dell'Ente (es. VIP, tecnologie, domini, indirizzi IP, etc.);
- la selezione del metodo di gestione del servizio e la definizione di processi e procedure a supporto;
- la fornitura periodica di report contestualizzati per l'Ente attraverso l'aggregazione e la correlazione delle minacce individuate.

Nell'ambito dell'analisi e potenziamento del processo di **Security Automation**, si intende adottare un approccio metodologico che prevede:

- l'identificazione dei driver di automazione e relativi Use-Case, funzionali a supportare le attività ripetitive svolte;
- la rappresentazione degli scenari di automazione, corroborati da un'analisi puntuale dei benefici, in termini di efficienza ed efficacia, apportati dalla loro implementazione;
- l'implementazione di un sottoinsieme degli scenari di automazione individuati, il test e il tuning in funzione dell'attivazione degli stessi.

4.F *(Se previsto)* **In coerenza con le Linee Guida, descrivere l'approccio metodologico proposto per il rafforzamento del modello organizzativo e delle competenze professionali delle risorse impiegate e/o da impiegare in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio Mandato**

Max 300 parole

Sulla base del CERT esistente in Regione Lazio, l'approccio metodologico proposto pone un accento sulla definizione di ruoli e responsabilità in capo alla sopra citata struttura nonché al CSIRT al fine di creare uniformità di azioni, referenti e punti di contatto in casi di escalation. Il modello di servizio sarà così efficientato permettendo la corretta gestione degli incidenti di sicurezza nel più breve tempo possibile e, contemporaneamente, creando sinergia tra gli attori coinvolti. Le competenze professionali del personale di sicurezza, a valle del potenziamento dei servizi di Digital Risk Protection e di Automation, subiranno una notevole rimodulazione in ottica di snellimento dei processi e ponendo l'accento su una più dettagliata suddivisione dei compiti atta a rendere più efficace ed agevole la gestione degli incidenti. Le competenze verranno, inoltre, potenziate attraverso una costante condivisione delle informazioni opportunamente aggregate e normalizzate che permetterà la cooperazione continua tra i diversi CSIRT attivati a livello regionale e nei confronti dello CSIRT di ACN.

Il trasferimento delle competenze professionali del personale di sicurezza, ed il relativo costante aggiornamento nel tempo, sarà garantito mediante l'erogazione del servizio di Knowledge Transfer che permetterà ad ogni professionista di acquisire informazioni peculiari circa l'esecuzione delle proprie attività all'interno del CSIRT mediante apposita formazione ovvero training-on-the-job.

Nell'ambito dell'analisi e potenziamento del servizio di **Knowledge Transfer**, si intende fornire consulenza tecnica volta a supportare il miglioramento delle infrastrutture, degli strumenti e dei servizi relativi alla sicurezza informatica della Constituency in linea con le evoluzioni del quadro tecnologico di riferimento, nonché fornire consulenza in merito alle potenziali evoluzioni delle procedure sopra citate qualora la Constituency ravveda la necessità di apportare nel tempo sostanziali modifiche alle suddette procedure.

4.G *(Se previsto)* **In coerenza con le Linee Guida, descrivere l'approccio metodologico proposto per la definizione, implementazione e miglioramento degli strumenti in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio Mandato**
Max 300 parole

Nell'ambito del potenziamento degli strumenti a supporto della **Digital Risk Protection** si prevede di acquistare, configurare ed utilizzare una tecnologia volta a monitorare il perimetro esterno dell'Ente e fornire informazioni olistiche su minacce emergenti.
In tal modo, l'Ente potrà raggiungere gli obiettivi prefissati, in particolare:

- disseminare Indicatori di Compromissione (IoC) all'interno delle soluzioni di difesa perimetrale;
- rilevare potenziali dati sensibili esposti che attori di minaccia possono sfruttare a loro vantaggio;
- ricercare in maniera continuativa le vulnerabilità presenti all'interno della superficie di attacco;
- identificare e condividere informazioni relative alle minacce e vulnerabilità individuate e di conseguenza alle relative azioni di contenimento/eliminazione delle stesse;
- identificare minacce potenziali rivolte agli executives e VIP dell'Ente mediante analisi dei social media, forum e deep & dark web;
- notificare eventi rilevanti (data breach) che non hanno interessato direttamente l'Ente ma altre istituzioni appartenenti al medesimo settore.

Nell'ambito del potenziamento degli strumenti a supporto della **Security Automation** si prevede di acquistare, configurare ed utilizzare una tecnologia con capacità di orchestrare e automatizzare i processi attraverso il coordinamento dei flussi di lavoro.
In tal modo l'Ente potrà raggiungere gli obiettivi prefissati, in particolare:

- centralizzare la raccolta e l'analisi delle segnalazioni di sicurezza, strutturate e non strutturate, prevenienti dalle molteplici sorgenti;
- supportare il processo di triage attuato dagli analisti, analizzando e classificando preliminarmente un evento di sicurezza;
- arricchire le informazioni, relative a identità e asset oggetto di analisi, raccogliendole e collezionandole dalle molteplici fonti in perimetro;
- arricchire le informazioni relative agli indicatori di compromissione con il duplice obiettivo di identificare preliminarmente il possibile attore di minaccia e, raccogliere eventuali ulteriori riscontri non rilevati sul perimetro;
- estrarre le metriche di servizio, dalle molteplici sorgenti, a supporto della stesura preliminare della reportistica periodica e, instradare le notifiche verso le strutture di competenza, sia per finalità di raccolta dati sia di informativa.

4.H *(Se previsto)* **In coerenza con le Linee Guida, descrivere le attività proposte per la definizione, implementazione e miglioramento volte all'erogazione di servizi anche ai settori sanitario e/o efficientamento energetico e/o tutela del territorio e delle risorse idriche** *Max 300 parole*
Il parco applicativo della Regione Lazio è installato presso il Data Center regionale, infrastruttura complessa che ospita sia sistemi basati su architetture tradizionali sia una piattaforma Cloud privata, oltre ad interagire con Cloud Service Provider esterni. All'interno del Data Center sono gestiti oltre 130 sistemi applicativi, in gran parte di elevata complessità tecnologica, e altamente strategici per l'erogazione di servizi ai cittadini ed imprese. Con particolare riferimento ai servizi dedicati al settore sanitario erogati dalla Regione Lazio e gestiti a livello ICT da LAZIOcrea, si riporta di seguito l'elenco dei servizi regionali centralizzati "critici": • Anagrafe Vaccinale Regionale • Sistema Regionale gestione ausili assistenza Protesica • Cartella Sociale • Sistema Informativo per l'Assistenza Territoriale Sociale SIATESS • Distinta Contabile Riepilogativa • Gestione piani terapeutici Epatite C • Piani Terapeutici Farmaci Biologici • Sistema Gestione Piani terapeutici • Sistema Informativo Assistenza Domiciliare • Sistema Informativo Assistenza Riabilitativa (ex-art.26) • Sistema Informativo Residenze Sanitarie Assistenziali • Acquisizione gestione dati pronto soccorso • Acquisizione gestione dati pronto soccorso • Acquisizione gestione dati pronto soccorso

- Anagrafe Sanitaria Unica Regionale
- Registro Regionale Dialisi e Trapianto Lazio
- Piattaforma per la gestione e prenotazione delle prestazioni ambulatoriali
- Colleziona tutti i dati dei tamponi, quarantene, positivi e guariti COVID19
- Gipse-web - Pronto Soccorso
- Sistema Informativo Assistenza Territoriale
- Sistema Informativo Assistenza Territoriale e SocioSanitaria
- Fascicolo Sanitario Elettronico
- Sistema Trasfusionale
- Ricetta Digitale
- Cartella diabetologica
- Sistema Informativo Ospedaliero
- Sistema di gestione del Rischio Clinico

Le attività di potenziamento del CSIRT Regionale, oggetto del presente progetto, saranno personalizzate in funzione della specificità dei servizi sanitari sopra elencati allo scopo di rafforzare le capacità di prevenzione, gestione e risposta di eventuali incidenti di sicurezza rilevati. In particolare, tali servizi sanitari potranno beneficiare delle seguenti personalizzazioni:

- verranno delineati, nell'ambito del servizio di miglioramento delle procedure, specifiche politiche e processi che terranno conto della specifica normativa applicabile (es: NIS/NIS2) per quanto attiene l'interscambio di informazioni afferenti eventi ed incidenti di sicurezza, in maniera tale da velocizzare l'ingaggio del CSIRT e mitigare i danni alle infrastrutture sanitarie coinvolte
- verranno effettuate, nell'ambito del servizio di Digital Risk Protection, particolari ricerche di vulnerabilità note, nonché di potenziali attacchi informatici dipendentemente dalla categoria degli Enti coinvolti, sfruttando le potenzialità degli strumenti introdotte, con conseguente rapida notifica di situazioni avverse critiche

- verranno identificati, nell'ambito del servizio di Security Automation, precisi vettori di attacco solitamente afferenti a tale contesto, così da aumentare la visibilità su potenziali eventi avversi, attuando particolari tecniche di contenimento ed eradicazione di artefatti malevoli.

Sezione 5 – QUADRO FINANZIARIO DEL PROGETTO PROPOSTO

In riferimento al paragrafo n. 5.2 “Spese ammissibili” dell’Avviso pubblico recante “Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all’attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”M1C1I1.5”, nella presente sezione, deve essere dettagliato il preventivo finanziario.
Si specifica che il Soggetto attuatore dell’intervento potrà presentare esclusivamente costi strettamente connessi allo svolgimento delle attività previste nel Piano di Progetto coerenti e pertinenti con le finalità dell’intervento 1.5, Missione M1C1, e successivamente comprovabili con opportuna documentazione giustificativa. Ai fini dell’ammissibilità delle spese si rimanda alla normativa nazionale ed europea di riferimento vigente e alle indicazioni operative ripotate nel Manuale per i Soggetti Attuatori adottato dall’Agenzia.

Il finanziamento concesso con il presente Avviso è cumulabile con altri finanziamenti a valere su programmi e strumenti dell’Unione europea, a condizione che gli stessi non interessino i medesimi costi in applicazione del principio di addizionalità di cui all’art.9 del Regolamento (UE) 2021/241. Dovrà pertanto essere esplicitato nel preventivo finanziario l’eventuale contributo a carico di altre fonti finanziarie.

Nel caso in cui l’intervento sia stato avviato con una diversa copertura finanziaria a valere sul bilancio dell’Unione, all’atto della sottoscrizione dell’Atto d’Obbligo il Soggetto attuatore dell’intervento dovrà formalmente dimostrare di aver rinunciato al precedente finanziamento, ove questo sia riferito ai medesimi costi per cui si chiede il contributo a valere sul PNRR.

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

- le attività legate al disegno di un processo di gestione del ciclo di vita delle fonti, interne ed esterne, per l’identificazione di potenziali minacce di interesse;
- l’implementazione di un framework documentale a supporto dell’esecuzione periodica delle attività di controllo del CSIRT;
- il reclutamento di personale a tempo determinato dedicato alla definizione di un CSIRT Regionale, in linea con le indicazioni attuative in relazione all’art. 1 del decreto-legge n. 80 del 2021, convertito con modificazioni in Legge n. 113 del 2021, di cui alla circolare RGS del 18 gennaio 2022 n. 4, recante “Modalità speciali per il reclutamento del personale e il conferimento di incarichi professionali per l'attuazione del PNRR da parte delle Amministrazioni Pubbliche”;

- la partecipazione a corsi di formazione specialistici, con eventuale acquisizione di certificazioni, per l'ottenimento di competenze necessarie al raggiungimento degli obiettivi del mandato del CSIRT;
- l'acquisizione di piattaforme di vulnerability management, per l'identificazione, la classificazione e il tracciamento di vulnerabilità rilevate sul proprio ambito di applicazione.

5.A Indicazione e descrizione delle **risorse finanziarie** necessarie alla realizzazione del progetto per ogni macro-attività

COSTO COMPLESSIVO DEL PROGETTO (*inclusivo di ulteriori fonti finanziarie, come risultante dal CUP indicato*): € € 1.500.000,00

IMPORTO CONTRIBUTO RICHIESTO *(*come derivante dalla compilazione di cui alla *Tabella 1* e alla *Tabella 2)*: € 1.500.000,00

(eventuale, se il costo complessivo del progetto è maggiore dell'importo del contributo richiesto) **IMPORTI DA ALTRE FONTI DI FINANZIAMENTO:**

- € _____, *fonte:* _____
- € _____, *fonte:* _____
- € _____, *fonte:* _____

Tabella 1 – Contributo richiesto per tipologia di attività come indicate nella sezione 2.B della presente Scheda Progetto

Compilare con l'importo previsto per ogni attività di cui al par. 4.1, comprensivo delle spese generali[1]. Nel caso in cui una o più attività non siano previste, indicare zero.

AREA DI INTERVENTO	***IMPORTO CONTRIBUTO RICHIESTO*** *(al netto di IVA)*	***VALORE IVA[2]***	***IMPORTO TOTALE CONTRIBUTO RICHIESTO*** *(al lordo di IVA)*
1. Analisi, disegno e razionalizzazione dei processi in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato	261.639,34	57.560,65	319.199,99

[1] *Le spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale sono riconosciti nella misura pari al 7% dei costi diretti ammissibili (art. 5.2 dell'Avviso)*

[2] *Come richiamato dal DPR. 22/2018, art. 15: "Ai sensi dell'articolo 69, paragrafo 3, lettera c), del regolamento (UE) n. 1303/2013, l'imposta sul valore aggiunto (IVA) realmente e definitivamente sostenuta dal beneficiario è una spesa ammissibile solo se questa non sia recuperabile, nel rispetto della normativa nazionale di riferimento […]". Pertanto, questa potrà essere computata nella colonna "importo finanziamento richiesto" esclusivamente al verificarsi di tale fattispecie*.

2. Adeguamento e rafforzamento del modello organizzativo e potenziamento delle competenze professionali	180.983,61	39.816,39	220.800,00
3. Definizione, implementazione e miglioramento degli strumenti in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato	377.049,18 €	82.950,82	460.000,00
4. Definizione, implementazione e miglioramento volti all'erogazione di servizi anche ai settori sanitario e/o efficientamento energetico e/o tutela del territorio e delle risorse idriche	409.836,07 €	90.163,94	500.000,01
TOTALE	1.229.508,20	270.491,80	1.500.000,00

Tabella 2 – Dettaglio dei costi preventivati per ogni attività e area di intervento

Compilare la seguente tabella con il dettaglio dei costi preventivati per ogni attività e area di intervento (rif. Paragrafo 4.1 dell'avviso) prevista per il progetto (rif. Sezione 2.B) aggiungendo se necessarie ulteriori righe.

AREA DI INTERVENTO[3]	ATTIVITA'	CATEGORIA DI COSTO[4]	IMPORTO CONTRIBUTO RICHIESTO *(al netto di IVA)*	*VALORE IVA[5]*	IMPORTO TOTALE CONTRIBUTO RICHIESTO *(IVA inclusa)*	STIMA ANNO DI RIFERIMENTO PER LA REALIZZAZIONE DELLA SPESA
1. Analisi, disegno e razionalizzazione dei processi in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato	*Definizione modello CSIRT e relativi processi* *Analisi e razionalizzazione processo di Digital Risk Protection* *Analisi e razionalizzazione del processo di Security Automation*	Acquisizione di Servizio	261.639,34	57.560,65	319.199,99	2024
2. Adeguamento e rafforzamento del modello organizzativo e	*Knowledge Transfer*	Acquisizione di Servizio	180.983,61	39.816,39	220.800,00	2024

[3] Indicare la tipologia di intervento in coerenza con quanto selezionato nella Sezione 2.B "Tipologie di attività progettuali che si intende realizzare".

[4] Per categoria di costo indicare ad esempio: acquisizione di beni; acquisizione di servizi; costo personale interno; …)

[5] Come richiamato dal DPR. 22/2018, art. 15: "Ai sensi dell'articolo 69, paragrafo 3, lettera c), del regolamento (UE) n. 1303/2013, l'imposta sul valore aggiunto (IVA) realmente e definitivamente sostenuta dal beneficiario è una spesa ammissibile solo se questa non sia recuperabile, nel rispetto della normativa nazionale di riferimento […]". Pertanto, questa potrà essere computata nella colonna "importo finanziamento richiesto" esclusivamente al verificarsi di tale fattispecie.

potenziamento delle competenze professionali						
3. Definizione, implementazione e miglioramento degli strumenti in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato	*Acquisizione e configurazione della Piattaforma di Digital Risk Protection* *Acquisizione e configurazione della Piattaforma di Security Automation*	Acquisizione di Beni e Servizi	377.049,18 €	82.950,82	460.000,00	2024
4. Definizione, implementazione e miglioramento volti all'erogazione di servizi anche ai settori sanitario e/o efficientamento energetico e/o tutela del territorio e delle risorse idriche	*Acquisizione e configurazione della Piattaforma di Digital Risk Protection* *Acquisizione e configurazione della Piattaforma di Security Automation* *Personalizzazione del servizio di Digital Risk Protection* *Personalizzazione del servizio di Security Automation*	Acquisizione di beni e Servizi	409.836,07 €	90.163,94	500.000,01	2024- 2025

a) TOTALE COSTI DIRETTI	1.500.000,00	
b) SPESE GENERALI 7% DEI COSTI DIRETTI AMMISSIBILI (a*7%)	0	
c) TOTALE RICHIESTO A FINANZIAMENTO (a+b)	1.500.000,00	

Sezione 6 – CRONOPROGRAMMA DEL PROGETTO PROPOSTO

6.A Indicazione e descrizione del **cronoprogramma delle attività** di implementazione del progetto
Compilare la tabella sottostante (è possibile aggiungere righe alla tabella)

Area di intervento *(rif. Sezione 2.B)*	Attività (breve descrizione)	Data di inizio prevista in BIMESTRI (es B4 2023)	Data di fine prevista in BIMESTRI (es. B4 2024)	Durata espressa in gg solari e continuativi
1. Analisi, disegno e razionalizzazione dei processi in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal	Definizione modello CSIRT e relativi processi Analisi e razionalizzazione processo di Digital Risk Protection Analisi e razionalizzazione del processo di Security Automation	B1 2024	B6 2024	365

proprio mandato				
. Adeguamento e rafforzamento del modello organizzativo e potenziamento delle competenze professionali	Knowledge Transfer	B1 2024	B6 2024	365
3. Definizione, implementazione e miglioramento degli strumenti in modo da renderli adeguati al raggiungimento degli obiettivi prefissati dal proprio mandato	Acquisizione e configurazione della Piattaforma di Digital Risk Protection Acquisizione e configurazione della Piattaforma di Security Automation	B1 2024	B6 2024	365
4. Definizione, implementazione e miglioramento	Acquisizione e configurazione della Piattaforma di Digital Risk Protection	B1 2024	B6 2025	730

volti all’erogazione di servizi anche ai settori sanitario e/o efficientamento energetico e/o tutela del territorio e delle risorse idriche	Acquisizione e configurazione della Piattaforma di Security Automation			

Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici

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

M1C1I1.5

ALLEGATO C – ATTO D'OBBLIGO

PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE M1C1 "DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA P.A." – INVESTIMENTO 1.5 "CYBERSICUREZZA"

ATTO D'OBBLIGO CONNESSO ALL'ACCETTAZIONE DEL FINANZIAMENTO CONCESSO DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE PER IL PROGETTO 4_WP7_A6_Regione Lazio - CSIRT REGIONE LAZIO – CUP F84F23000230006

VISTI

- la legge 7 agosto 1990, n. 241 recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*", la quale stabilisce, tra l'altro, che 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;
- la legge 16 gennaio 2003, n. 3 recante "*Disposizioni ordinamentali in materia di pubblica amministrazione*", con particolare riferimento all'articolo 11, comma 2 *bis,* ai sensi del quale "*Gli atti in materia di pubblica amministrazione anche di natura regolamentare adottati dalle Amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, che dispongono il finanziamento pubblico o autorizzano l'esecuzione di progetti di investimento pubblico, sono nulli in assenza dei corrispondenti codici di cui al comma 1 che costituiscono elemento essenziale dell'atto stesso*";
- il Regolamento di esecuzione (UE) n. 821/2014 del 28 luglio 2014, recante le disposizioni necessarie per l'elaborazione dei programmi finanziati dei fondi strutturali e di investimento europei;
- la Direttiva (UE) 2015/849 del Parlamento Europeo e del Consiglio, del 20 maggio 2015, recante *"prevenzione dell'uso del sistema finanziario e fini di riciclaggio o funzionamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione"* e, nello specifico, l'articolo 3, comma 6, che definisce il titolare effettivo come *"la persona o le persone fisiche che, in ultima istanza, possiedono o controllano il cliente e/o le persone fisiche per conto delle quali è realizzata un'operazione o un'attività"*;
- il decreto legislativo 31 marzo 2023, n. 36 avente ad oggetto *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"*;

- la 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"* e il relativo decreto legislativo n. 65/2018 (decreto attuativo NIS);
- il decreto del Presidente del Consiglio dei ministri 5 febbraio 2018, n.22 avente per oggetto *"Regolamento recante i criteri sull'ammissibilità delle spese per i programmi cofinanziati dai Fondi strutturali di investimenti europei (SIE) per il periodo di programmazione 2014/2020";*
- il Regolamento (UE) 2018/1046 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 recante "*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 (cd. *"Cybersecurity Act"*);
- il decreto-legge 21 settembre 2019, n. 105 recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"*, convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 133;
- la legge del 18 novembre 2019, n. 133 convertita, con modificazioni, dal decreto-legge 21 settembre 2019, n. 105, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"*;
- la delibera CIPE 26 novembre 2020, n. 63, che introduce la normativa attuativa della riforma CUP;
- la legge 30 dicembre 2020, n. 178, con particolare riferimento all'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; e al comma 1043, 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 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 del 6 maggio 2021, n. 59, convertito con modificazioni dalla legge di conversione 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 del 31 maggio 2021, n. 77, convertito con modificazioni dalla legge di conversione del 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 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*" che prevede l'istituzione dell'Agenzia a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;
- 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 del 15 settembre 2021 con il quale sono stati individuati gli strumenti per il monitoraggio del PNRR*;*
- il decreto ministeriale dell'11 ottobre 2021, con il quale il Ministero dell'Economia ha reso note le procedure per la gestione del PNRR in merito alle risorse;

- 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 alle Amministrazione centrali dello Stato delle Istruzioni tecniche per la selezione dei progetti PNRR*;
- il decreto-legge 6 novembre 2021, n. 152, recante "*Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose*";
- la circolare del 30 dicembre 2021, n. 32, del Ministero dell'Economia e delle Finanze, *"Piano Nazionale di Ripresa e Resilienza – Guida operativa per il rispetto del principio di non arrecare danno significativo all'ambiente (DNSH)"*, individuato dall'articolo 17 del Regolamento (UE) 2020/852 del Parlamento Europeo e del Consiglio del 18 giugno 2020 e dalla 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 resilienza"*;
- la circolare del 31 dicembre 2021, n. 33, del Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria generale dello Stato- Piano Nazionale di Ripresa e Resilienza (PNRR) 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*";
- la circolare del 18 gennaio 2022, n. 4, del Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria generale dello Stato - recante *"Piano Nazionale di Ripresa e Resilienza (PNRR) - art. 1 comma 1 del decreto-legge n. 80 del 2021- indicazioni attuative";*
- la circolare del 24 gennaio 2022, n. 6, del Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria generale dello Stato – 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 10 febbraio 2022, n. 9 del Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria generale dello Stato – 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 29 aprile 2022, n.21, del Ministero dell'Economia e delle Finanze Dipartimento della Ragioneria Generale dello Stato, 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, n. 79, recante *"Ulteriori modifiche urgenti per l'attuazione del PNRR"*;
- la circolare del 21 giugno 2022, n. 27, del Ministero dell'Economia e delle Finanze Dipartimento della Ragioneria Generale dello Stato, recante *"Piano Nazionale di Ripresa e Resilienza (PNRR) Monitoraggio delle misure PNRR"*;
- la circolare del 4 luglio 2022, n. 28, del Ministero dell'Economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato, 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 26 luglio 2022, n. 29, del Ministero dell'Economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato, recante *"Modalità di erogazione delle risorse PNRR e principali modalità di contabilizzazione da parte degli enti territoriali soggetti"*;
- la circolare dell'11 agosto 2022, n. 30, del Ministero dell'economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato, recante *"Circolare sulle procedure di controllo e rendicontazione delle misure PNRR"*;
- la circolare del 2 gennaio 2023, n. 1, del Ministero dell'Economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato, 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 PNRR"*
- la circolare del 22 marzo 2023, n.11, del Ministero dell'economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato, recante *"Registro Integrato dei Controlli PNRR – Sezione controlli milestone e target";*
- la circolare del 13 marzo 2023, n. 10, del Ministero dell'Economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato, 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";*
- i principi trasversali previsti dal PNRR, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (c.d. tagging), il principio di parità di genere e l'obbligo di protezione e valorizzazione dei giovani;
- rispettare la normativa applicabile in tema di trattamento dei dati personali, in particolare il Regolamento (UE) 2016/679 (GDPR);

- gli obblighi di assicurare il conseguimento di target e milestone previsti nella Componente e nell'Investimento del PNRR;
- gli Accordi Operativi – Operational Arrangements – con i quali sono stati stabiliti i meccanismi di verifica periodica relativi al raggiungimento di Milestone e Target contenuti negli allegati alla Decisione di esecuzione del Consiglio relativa alla "*Approvazione del Piano per la ripresa e la resilienza dell'Italia*";
- la Misura M1, Componente C1, Investimento 1.5 del PNRR;
- il target M1C1-20 (target finale UE), in scadenza al T4 2024: *"Dispiego integrale dei servizi nazionali di cybersecurity"*;
- il decreto Legislativo 7 marzo 2005, n. 82, recante *"Codice dell'Amministrazione Digitale";*
- il decreto del Ministro dell'economia e delle finanze del 6 agosto 2021 e ss.mm.ii. relativo all'assegnazione delle risorse in favore di ciascuna Amministrazione titolare degli interventi PNRR e corrispondenti milestone e target che individua la Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante *"Cybersicurezza*";
- 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"* che ha istituito l'Agenzia per la cybersicurezza nazionale;
- l'articolo 7, comma 1, lettere m) e n), del suddetto decreto-legge n. 82 del 2021 che hanno attribuito all'Agenzia per la Cybersicurezza Nazionale tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale e i compiti di cui all'articolo 33-septies, comma 4, del Decreto Legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221, nonché la responsabilità di sviluppare *"capacità nazionali di prevenzione, monitoraggio, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici […]";*
- l'articolo 7, comma 1, lettera t), del suddetto decreto-legge n. 82 del 2021 che individua l'Agenzia quale autorità che *"promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza nazionale e dei correlati servizi applicativi […]";*
- 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. In particolare:

- la Misura #33 avente ad oggetto *"Accrescere le capacità di risposta e ripristino a seguito di crisi cibernetiche implementando una rete di CERT settoriali integrata con il CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati, con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici"*;

- il decreto del Presidente del Consiglio dei ministri del 16 settembre 2021, concernente la *"Definizione dei termini e delle modalità del trasferimento di funzioni, beni strumentali e documentazione dal Dipartimento delle informazioni per la sicurezza all'Agenzia per la cybersicurezza nazionale",* con il quale il Governo ha definito in favore dell'Agenzia il trasferimento di funzioni, beni strumentali e documentazione anche di natura classificata dal Dipartimento delle informazioni per la sicurezza (DIS);

- l'Accordo n. 34/2021 del 14 dicembre 2021, di cui al prot. ACN n. 896 del 15 dicembre 2021, stipulato dall'Agenzia per la Cybersicurezza Nazionale (ACN) con il Dipartimento per la trasformazione digitale (DTD), ai sensi dell'articolo 5, comma 6, del decreto legislativo n. 50/2016, disciplinante lo svolgimento in collaborazione delle attività di realizzazione dell'"Investimento 1.5";

- l'atto di organizzazione protocollo n. 1776 del 01/03/2022, avente per oggetto *"Adozione del modello organizzativo dell'Agenzia per la Cybersicurezza Nazionale per l'attuazione dell'Investimento 1.5 recante "Cybersicurezza" Missione 1, Componente 1, del PNRR e individuazione del personale incaricato a svolgere le funzioni e i compiti delegati all'Agenzia, in qualità di Soggetto attuatore dell'investimento, dal Dipartimento per la Trasformazione Digitale"*;

- le Linee guida per i Soggetti Attuatori emanate dal Dipartimento per la Trasformazione Digitale ai fini della presentazione della Richiesta Rimborso delle spese sostenute per la realizzazione degli interventi previsti dal PNRR e parte integrante del SiGeCo, adottato dall'Unità di Missione a marzo 2023 (versione 3);

- il Manuale Operativo di cui alle Linee guida per i Soggetti Attuatori individuati tramite Avvisi Pubblici emanato dall'Agenzia per la Cybersicurezza Nazionale pubblicati sul sito istituzionale www.acn.gov.it;

VISTI ALTRESI'

- la determina n. 21472 del 08/08/2023 con la quale è stato approvato l'Avviso Pubblico, avente ad oggetto "*Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione, monitoraggio, rilevamento, analisi e risposta degli incidenti di sicurezza informatica e degli attacchi informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5*";

- la ricezione delle domande di partecipazione complete delle informazioni anagrafiche inerenti al Soggetto attuatore dell'intervento e delle dichiarazioni relative al possesso dei requisiti di partecipazione previsti dall'Avviso;
- le proposte progettuali (cd. "Piano di Progetto") dove sono stati dettagliati gli obiettivi dell'intervento proposto, le informazioni identificative al momento disponibili (es. CUP, CIG attivi, etc.), le attività previste e i relativi tempi di attuazione, il quadro finanziario complessivo dell'intervento, l'entità del contributo richiesto e l'indicazione delle tipologie di costi previsti nonché di eventuali altri fonti di finanziamento;
- la determina n. 30697 del 30/11/2023 con la quale sono state individuate le proposte progettuali ammesse al finanziamento e i Soggetti attuatori degli interventi a valere sull'Avviso pubblico in oggetto;

CONSIDERATA la necessità di perfezionare l'atto di assegnazione delle risorse finanziarie con la stipula di un Atto d'Obbligo;

TUTTO CIO' PREMESSO E RITENUTO

il Soggetto attuatore dell'intervento Regione Lazio, CF/P.IVA 80143490581, con sede legale in Via Cristoforo Colombo n. 212, cap. 00147, tel. 06 51685100, posta elettronica certificata (PEC) direzione.itd@regione.lazio.legalmail.it, in persona del Soggetto titolare del potere di impegnare l'Amministrazione Stefano Calabrese, nato a Roma prov. (RM), il 28/02/1969, CF CLBSFN69B28H501V, documento d'identità n. 4391729AA, rilasciato dal Ministero dell'Interno in data 17/06/2015 con scadenza in data 28/02/2026;

DICHIARA SOTTO LA PROPRIA RESPONSABILITÀ QUANTO SEGUE

Articolo 1 - Oggetto

1. Il Soggetto attuatore dell'intervento dichiara di aver preso visione della determina prot. n. 30697 del 30/11/2023 adottata dall'Agenzia per la Cybersicurezza Nazionale per l'individuazione delle proposte progettuali ammesse al finanziamento e dei Soggetti attuatori degli interventi a valere sull'Avviso pubblico (nel prosieguo "Avviso"), di cui questo atto è parte integrante come allegato, e di accettare espressamente e integralmente tutti i termini, gli obblighi e le condizioni ivi previste;
2. Il Soggetto attuatore dell'intervento dichiara altresì, di accettare, in qualità di **Soggetto attuatore dell'intervento**, il finanziamento concesso a valere sul PNRR, Missione M1C1 "Digitalizzazione, innovazione e sicurezza nella P.A." Componente 1 Investimento 1.5, fino ad un **importo massimo di euro 1.500.000,00 (unmilionecinquecentomila/00),** destinato alla copertura dei costi così come declinati e dettagliati nel documento descrittivo del progetto presentato e allegato al presente atto, dichiara di impegnarsi a svolgere il progetto nei tempi e nei modi indicati.

Articolo 2 - Termini di attuazione del progetto e durata dell'Atto d'Obbligo

1. Il Soggetto attuatore dell'intervento si impegna a dare piena attuazione alle attività previste nel Piano Progetto, nel rispetto delle tempistiche indicate nel cronoprogramma, e ad individuare eventuali fattori che possano determinare ritardi che incidano sulle tempistiche attuative e di spesa, relazionando al Soggetto attuatore dell'Investimento sugli stessi e mettendo in atto tutte le azioni necessarie a mitigarne i rischi.
2. Nel caso di interventi *ex novo*, le attività indicate nel Piano di Progetto dovranno essere avviate entro 10 giorni lavorativi a partire dalla data di trasmissione del presente Atto all'Agenzia per la Cybersicurezza Nazionale, salvo eventuali tempistiche migliorative proposte. In tal caso, il Soggetto attuatore dell'Intervento dovrà provvedere a comunicare tempestivamente, e comunque nel rispetto dei termini massimi individuati dall'Avviso, al Soggetto attuatore dell'Investimento della data di avvio del progetto.
3. Le attività previste dal Piano di Progetto dovranno essere realizzate nel rispetto del cronoprogramma presentato e completate entro la data ivi indicata. Per completamento degli interventi si intendono anche gli adempimenti connessi alla rendicontazione, coerentemente con quanto previsto dall'Avviso. Eventuali modifiche dovranno essere approvate con le modalità di cui all'art. 8 del presente Atto, fermo restando che gli interventi dovranno comunque concludersi nel rispetto delle tempistiche indicate nell'Avviso o, ove migliorative, proposte in fase di partecipazione, in coerenza con la milestone e il target M1C1-20.

Articolo 3 - Obblighi del Soggetto attuatore dell'Intervento

1. Il Soggetto attuatore dell'Intervento dichiara di obbligarsi alla realizzazione dell'intervento progettuale proposto, in conformità alle modalità e ai termini previsti nell'Avviso e nel Piano di Progetto e, in ogni caso, nel rispetto della normativa vigente anche se non espressamente richiamata.
2. Il Soggetto attuatore dell'Intervento, in particolare, si impegna a:
   - assicurare il rispetto di tutte le disposizioni previste dalla normativa europea e nazionale, con particolare riferimento a quanto previsto dal Reg. (UE) 2021/241 e dal decreto-legge n. 77 del 31/05/2021 recante "*Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*", come modificato dalla legge 29 luglio 2021, n. 108;
   - assicurare l'adozione di misure adeguate volte a rispettare il principio di sana gestione finanziaria secondo quanto disciplinato nel Regolamento finanziario (UE, Euratom) 2018/1046 e nell'art. 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 garantire l'assenza del c.d. doppio finanziamento ai sensi dell'art. 9 del Regolamento (UE) 2021/241;

- garantire il rispetto dei principi trasversali di parità di trattamento, non discriminazione, trasparenza, proporzionalità e pubblicità;
- rispettare, ove applicabile, le indicazioni relative ai principi orizzontali di cui all'art. 5 del Reg. (UE) 2021/241 ossia il principio di "non arrecare un danno significativo" agli obiettivi ambientali ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 (DNSH) 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 gli ulteriori principi trasversali previsti per il PNRR dalla normativa nazionale ed europea, con particolare riguardo alle misure a sostegno della parità di genere, anche 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 31 maggio 2021, n. 77 (c.d. decreto Semplificazioni), convertito, con modificazioni, dalla Legge 29 luglio 2021, n. 108, e del superamento dei divari territoriali;
- rispettare le norme europee e nazionali applicabili in ambito di tutela dei soggetti diversamente abili;
- garantire, nel caso in cui si faccia ricorso a procedure di appalto, il rispetto della normativa vigente di riferimento;
- garantire, nel caso in cui si faccia ricorso diretto ad esperti esterni dell'Amministrazione, la conformità alla pertinente disciplina europea e nazionale nonché alle eventuali specifiche circolari che potranno essere adottate dall'Amministrazione centrale Titolare dell'Intervento;
- rispettare quanto previsto dall'articolo 11 della legge 16 gennaio 2003, n. 3, in merito alla richiesta dei Codici Unici di Progetto, CUP, e garantirne l'indicazione su tutti gli atti amministrativo-contabili relativi all'attuazione dell'investimento;
- rispettare gli adempienti in materia di trasparenza amministrativa ex d. lgs. 25 maggio 2016, n. 97, e gli obblighi in materia di comunicazione e informazione previsti dall'art. 34 del Regolamento (UE) 2021/241;
- rendere nota l'origine del finanziamento 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 e

garantirne visibilità riportando in tutta la documentazione di progetto l'emblema dell'Unione Europea e utilizzando la dicitura "*Finanziato dall'Unione Europea – Next Generation UE – PNRR M1C1 – Intervento 1.5* 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;

- conservare la documentazione progettuale in fascicoli cartacei o informatici per assicurare la completa tracciabilità delle operazioni - nel rispetto di quanto previsto dal d. lgs. 82/2005 e all'art. 9, punto 4, del decreto-legge 77 del 31 maggio 2021 che, nelle diverse fasi di controllo e verifica previste dal sistema di gestione e controllo del PNRR, devono essere messi prontamente a disposizione su richiesta dell'Agenzia per la Cybersicurezza Nazionale, dell'Amministrazione centrale responsabile dell'Investimento, del Servizio centrale per il PNRR del Ministero dell'Economia e delle Finanze, dell'Organismo di Audit, della Commissione europea, dell'OLAF, della Corte dei conti europea (ECA), della Procura europea (EPPO) e delle competenti Autorità giudiziarie nazionali;
- autorizzare la Commissione, l'OLAF, la Corte dei conti e l'EPPO a esercitare i diritti di cui all'articolo 129, paragrafo 1, del Regolamento finanziario (UE; EURATOM) 1046/2018;
- contribuire al raggiungimento dei milestone e target associati alla Misura e fornire, su richiesta dal Soggetto attuatore dell'investimento, le informazioni necessarie per la predisposizione delle dichiarazioni sul conseguimento dei target e milestone e delle relazioni e documenti sull'attuazione dei progetti;
- fornire i documenti e le informazioni necessarie secondo le tempistiche previste e le scadenze stabilite dai Regolamenti europei e dal Soggetto attuatore dell'investimento per tutta la durata del progetto;
- garantire una tempestiva diretta informazione agli organi preposti, tenendo informato il Soggetto attuatore dell'Investimento 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 frodi riscontrate a seguito delle verifiche di competenza e adottare le misure necessarie, nel rispetto delle procedure adottate dal Soggetto attuatore dell'Investimento, in linea con quanto indicato dall'articolo 22 del Regolamento (EU) 2021/2041;
- adottare il sistema informatico utilizzato dal Soggetto attuatore dell'Investimento, finalizzato a raccogliere, registrare e archiviare in formato elettronico i dati per ciascuna operazione necessari per la sorveglianza, la valutazione, la gestione finanziaria, la verifica e l'audit, secondo quanto previsto dall'art. 22.2, lettera d), del

Regolamento (UE) 2021/241 e tenendo conto delle indicazioni che verranno fornite dall'Agenzia;

- 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. 178/2020 (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 milestone e target della misura e assicurarne, per quanto di competenza, l'inserimento nel sistema informativo e gestionale adottato dal Soggetto attuatore dell'Investimento nel rispetto delle indicazioni che saranno fornite dalla stessa Agenzia;
- partecipare, ove richiesto, alle riunioni convocate dal Soggetto attuatore dell'Investimento;
- garantire, anche attraverso la trasmissione di relazioni periodiche sullo stato di avanzamento del progetto, che il Soggetto attuatore dell'investimento 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;
- garantire la massima collaborazione in occasione di verifiche e controlli richiesti dall'Agenzia per la Cybersicurezza Nazionale, dal Servizio centrale per il PNRR, dall'Unità di Audit, degli organismi europei, nonché eventualmente dell'autorità giudiziaria e delle forze di polizia nazionali.

Articolo 4 - Procedura di rendicontazione della spesa e dell'avanzamento verso milestone e target del PNRR

1. Il Soggetto attuatore dell'Intervento si impegna a seguire le procedure di rendicontazione delle spese nel rispetto del quadro economico-finanziario e del cronoprogramma approvato, nelle modalità e tempistiche previste dall'Avviso e dal Manuale Operativo di cui alle *"Linee Guida per i Soggetti attuatori individuati tramite Avvisi Pubblici"* dell'Agenzia.
2. Nel caso di utilizzo delle opzioni di costo semplificato che comportino l'adozione preventiva di una metodologia dei costi, il Soggetto attuatore dell'Intervento si impegna a rispettare quanto indicato nella relativa metodologia, previa approvazione da parte dell'Amministrazione centrale Titolare dell'Intervento.
3. Il Soggetto attuatore dell'Intervento si impegna altresì a garantire di essere in possesso di una Contabilità Speciale correttamente profilata sull'Investimento 1.5 e/o di un Conto di Tesoreria da utilizzare per l'erogazione dei pagamenti e l'adozione di 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.

4. Al fine di garantire il monitoraggio delle attività e il rispetto delle tempistiche di programmazione, il Soggetto attuatore dell'Intervento si impegna a rispettare le disposizioni contenute ,nel Manuale Operativo di cui alle *"Linee Guida per i Soggetti attuatori individuati tramite Avvisi Pubblici"* dell'Agenzia, in conformità alle disposizioni contenute nel Sistema di Gestione e Controllo (SIGECO) dell'Amministrazione centrale titolare della misura PNRR in oggetto e a fornire la necessaria collaborazione ai fini della registrazione sul sistema informativo adottato dall'Amministrazione centrale dei dati relativi a tutti gli aspetti procedurali, fisici e finanziari che caratterizzano l'attuazione dell'intervento, inclusi i giustificativi di spesa e di pagamento, per consentire l'espletamento dei controlli amministrativo-contabili a norma dell'art. 22 del Reg. (UE) 2021/241 e dell'art. 9 del decreto-legge n. 77 del 31/05/2021, convertito, con modificazioni, dalla legge n. 108/2021.

5. Il Soggetto attuatore dell'intervento, pertanto, dovrà inoltrare con cadenza bimestrale nelle modalità di cui al Manuale Operativo di cui alle *"Linee Guida per i Soggetti attuatori individuati tramite Avvisi Pubblici"* dell'Agenzia, la rendicontazione dettagliata di tutte le spese effettivamente sostenute nel periodo di riferimento o dei costi esposti maturati nel caso di ricorso alle opzioni semplificate in materia di costi e da tutta la documentazione attestante lo stato di avanzamento del progetto e il contributo dello stesso nel perseguimento di target e milestone dell'Investimento, come specificatamente indicata nell'Avviso e nel Manuale Operativo di cui alle *"Linee Guida per i Soggetti attuatori individuati tramite Avvisi Pubblici".*

6. Le spese incluse nelle domande di rimborso del Soggetto attuatore dell'intervento, se afferenti ad operazioni estratte a campione, sono sottoposte alle verifiche, se del caso anche in loco da parte delle strutture deputate al controllo dell'Agenzia per la Cybersicurezza Nazionale e dell'Amministrazione centrale titolare. Nello specifico, le strutture coinvolte a diversi livelli di controllo eseguono le verifiche sulle procedure, sulle spese e sui target in conformità con quanto stabilito dall'art. 22 del Regolamento (UE) 2021/241 al fine di garantire la tutela degli interessi finanziari dell'Unione, la prevenzione, individuazione e rettifica di frodi, di casi di corruzione e di conflitti di interessi, nonché il recupero di somme erroneamente versate o utilizzate in modo non corretto.

7. Il Soggetto attuatore dell'Intervento si impegna a:
    a. collaborare e a fornire tutti i chiarimenti e le integrazioni che potranno essere richiesti nelle diverse fasi di verifica sulla regolarità e ammissibilità delle spese presentate nonché sulla riferibilità delle spese al progetto ammesso al finanziamento sul PNRR;
    b. facilitare le verifiche dell'Ufficio competente per i controlli del Soggetto attuatore dell'investimento, dell'Unità di Audit, della Commissione europea e di altri organismi autorizzati, che verranno effettuate anche attraverso controlli in loco;

c. garantire la disponibilità dei documenti giustificativi relativi alle spese sostenute e delle milestone e target realizzati così come previsto ai sensi dell'articolo 9, punto 4, del decreto-legge n. 77 del 31/05/2021, convertito, con modificazioni, dalla legge n. 108/2021.

Articolo 5 - Procedura di pagamento al Soggetto attuatore dell'Intervento

1. Le procedure di pagamento al Soggetto Attuatore dell'intervento seguono le modalità individuate nell'Avviso e nel Manuale Operativo di cui alle *"Linee Guida per i Soggetti attuatori individuati tramite Avvisi Pubblici".*

Articolo 6 - Variazioni del progetto

1. Il Soggetto attuatore dell'Intervento può proporre variazioni al Piano di Progetto nelle modalità e nei termini previsti nel Manuale Operativo di cui alle *"Linee Guida per i Soggetti attuatori individuati tramite Avvisi Pubblici".*

2. Eventuali richieste di modifica al progetto ammesso a finanziamento dovranno:
   - non comportare una modifica sostanziale in relazione alla tipologia/natura del progetto e dei singoli interventi;
   - non riguardare le previsioni inerenti a target e milestone PNRR;
   - garantire il rispetto di finalità, obiettivi, risultati attesi valutati in sede di ammissione al finanziamento;
   - non comportare l'incremento del finanziamento già concesso;
   - non riguardare una rimodulazione delle attività del cronoprogramma tali da prevedere ritardi alla conclusione del progetto rispetto ai termini proposti e a quelli massimi previsti per il raggiungimento della milestone e del target di riferimento (dicembre 2024).
3. Le richieste di modifica dovranno essere accolte con autorizzazione scritta dell'Agenzia.
4. L'Agenzia si riserva la facoltà di non riconoscere ovvero di non approvare spese relative a variazioni delle attività del progetto non autorizzate.
5. L'Agenzia si riserva la facoltà di chiedere al Soggetto Attuatore dell'Intervento ogni eventuale chiarimento e documentazione integrativa utile ai fini della valutazione della richiesta, che dovrà essere presentata perentoriamente entro il termine comunicato dalla stessa Agenzia.
6. Le eventuali modifiche approvate al Piano di Progetto non comportano alcuna revisione del presente Atto.

Articolo 7 - Disimpegno delle risorse

1. L'eventuale disimpegno delle risorse del Piano, previsto dall'articolo 24 del Reg. 2021/241 e dall'articolo 8 della legge n. 77 del 31/05/2021, come modificato dalla legge di conversione 29 luglio 2021, n. 108, comporta la riduzione o revoca delle risorse relative ai progetti che non hanno raggiunto gli obiettivi previsti, nel rispetto di quanto previsto dall'Avviso.

Articolo 8 - Rettifiche finanziarie

1. Ogni difformità rilevata nella regolarità della spesa, prima o dopo l'erogazione del contributo pubblico in favore del Soggetto attuatore dell'Intervento, dovrà essere immediatamente rettificata e gli importi eventualmente corrisposti dovranno essere recuperati secondo quanto previsto dall'articolo 22 del Regolamento (UE) n. 2021/241.
2. A tal fine il Soggetto attuatore dell'Intervento si impegna, conformemente a quanto verrà disposto dall'Agenzia, a recuperare e restituire le somme indebitamente corrisposte.
3. Il Soggetto attuatore dell'Intervento è obbligato a fornire tempestivamente ogni informazione in merito ad errori o omissioni che possano dar luogo a riduzione o revoca del contributo.

Articolo 9 - Risoluzione di controversie

1. Il presente Atto è regolato dalla legge italiana. Il Soggetto attuatore dell'intervento accetta che qualsiasi controversia, in merito all'interpretazione, esecuzione, validità o efficacia, è di competenza esclusiva del Foro di Roma.

Articolo 10 - Comunicazioni e scambio di informazioni

1. Ai fini della digitalizzazione dell'intero ciclo di vita del progetto, tutte le comunicazioni con l'Agenzia devono avvenire per posta elettronica istituzionale o posta elettronica certificata, ai sensi del d. lgs. n. 82/2005.
2. Nello specifico, si stabiliscono le seguenti modalità di invio telematico:
   - Atto d'obbligo, obbligatorio l'invio a mezzo posta elettronica certificata del documento firmato digitalmente dal Soggetto attuatore dell'intervento;
   - comunicazioni in autocertificazione ai sensi del DPR n. 445/2000, invio a mezzo posta elettronica istituzionale con allegata fotocopia del documento del dichiarante ove non le stesse non siano firmate digitalmente;
   - comunicazioni ordinarie, invio a mezzo posta elettronica istituzionale.
3. Per le sole comunicazioni ordinarie è consentito l'utilizzo della posta elettronica istituzionale.

4. Il Responsabile del Progetto, individuato dal Soggetto attuatore dell'Intervento, è l'Ing. Stefano Calabrese, mail scalabrese@regione.lazio.it, tel. 06 51685367. Eventuali modifiche riguardanti l'individuazione di un nuovo referente potranno essere comunicate a mezzo di posta elettronica istituzionale e non comportano alcuna modifica del presente Atto.

Articolo 11 - Efficacia e durata

1. L'efficacia del presente Atto, debitamente sottoscritto dal Soggetto attuatore dell'intervento, decorre dalla data di trasmissione dello stesso al Soggetto attuatore dell'investimento.
2. Il Soggetto attuatore dell'intervento, ai sensi e per gli effetti degli artt. 1341-1342 c.c., dichiara di approvare specificamente le suddette clausole del presente atto d'obbligo, artt. da 1 a 11.

Luogo e data	Nominativo e firma digitale
Roma, 20 dicembre 2023	_____