AGENZIA REGIONALE PROTEZIONE AMBIENTALE DELLA CAMPANIA

DELIBERAZIONE DEL DIRETTORE GENERALE N. 141 DEL 22/03/2024

DIREZIONE GENERALE U.O. SISTEMI INFORMATIVI E INFORMATICI

OGGETTO: AVVISO PUBBLICO N. 08/2024 PER LA PRESENTAZIONE DI PROPOSTE DI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER DEI GRANDI COMUNI, DEI COMUNI CAPOLUOGO DI REGIONE, DELLE CITTÀ METROPOLITANE, DELLE AGENZIE REGIONALI SANITARIE E DELLE AZIENDE ED ENTI DI SUPPORTO AL SERVIZIO SANITARIO NAZIONALE, DELLE AUTORITÀ DI SISTEMA PORTUALE, DELLE AUTORITÀ DEL BACINO DEL DISTRETTO IDROGRAFICO E DELLE AGENZIE REGIONALI PER LA PROTEZIONE DELL'AMBIENTE A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY", CODICE D'INVESTIMENTO M1C1I1.5 – APPROVAZIONE PROPOSTA DI PROGETTO, CUP E64F24000270006.

L'anno duemilaventiquattro, il giorno ventidue del mese di Marzo presso la sede dell'A.R.P.A.C. alla stregua dell'istruttoria compiuta dalla suindicata struttura e della dichiarazione di completezza e regolarità resa dal Dirigente Responsabile

PREMESSO CHE:

- l'Agenzia per la Cybersicurezza Nazionale *"ACN"*, in qualità di Soggetto attuatore dell'Investimento 1.5 "Cybersecurity" – Missione 1, Componente 1, del PNRR, a titolarità della Presidenza del Consiglio dei Ministri - Dipartimento per la Trasformazione Digitale "DTD", ha promosso l'Avviso Pubblico n. 08/2024, finanziato dall'Unione Europea – Next Generation EU -, per l'attuazione degli investimenti finalizzati alla realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione;
- l'Avviso ha lo scopo di individuare, mediante procedura valutativa con graduatoria, le proposte progettuali finalizzate ad irrobustire le infrastrutture ed i servizi digitali del Sistema Paese, nonché a migliorare le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza, quale elemento fondante per la transizione digitale sicura della Pubblica Amministrazione;
- nello specifico, esso intercetta la Misura #14 della Strategia Nazionale di Cybersicurezza, volta a coordinare interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella PA per la messa in sicurezza di dati e di servizi ai cittadini;
- al paragrafo 3 dell'Avviso "Soggetti Attuatori Ammessi" sono elencati i soggetti pubblici ammessi a partecipare, tra cui le Agenzie Regionali per la Protezione dell'Ambiente, come meglio specificato nell'Allegato E "Elenco dei soggetti attuatori ammessi" all'Avviso de quo;

CONSIDERATO CHE

- la nuova direttiva europea NIS 2 (Direttiva n. 2022/2555, entrata in vigore il 17 gennaio 2023 << … *relativa a misure per un livello comune elevato di cybersicurezza nell'Unione,….* > che abroga la precedente Direttiva (UE) 2016/1148 - "Direttiva NIS 1" -

recepita in Italia attraverso il D. Lgs. n. 65/2018 e da cui di fatto la nuova NIS 2 prende forma e sostanza) introduce, tra l'altro, misure più stringenti e specifiche in termini di cyber risk management e di segnalazione e *condivisione* delle informazioni relative agli incidenti di sicurezza, spingendo appunto alla condivisione delle stesse;

- in particolare l'aver esteso a livello europeo l'insieme di soggetti "*essenziali ed importanti*" interessati dalla NIS2 anche ad alcune PA (come da art. 2, c. 2, lett. f) e art. 3, c. 1, lett. d) della citata Direttiva) <<….*adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi*…>> fa capire la sempre maggiore importanza della questione Cybersicurezza, anche per l'Agenzia, da sempre fortemente impegnata in materia di digitalizzazione e sicurezza di sistemi e reti;

RITENUTO

- che l'esigenza di dover rispondere in maniera rapida ed efficace ai cambiamenti, anche imposti dall'ambiente esterno, pone la necessità di un sempre maggiore impegno verso le tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati;
- pertanto assolutamente opportuno per l'Ente partecipare alla selezione inerente l'Avviso ACN n. 08/2024 con un progetto mirato al potenziamento della propria postura di sicurezza informatica, anche attuando un adeguato processo di monitoraggio, misurazione e comunicazione della sicurezza delle informazioni nell'arco di tutta la fase progettuale;

ATTESO CHE tutti gli atti richiamati nella presente deliberazione sono depositati presso l'ufficio proponente;

VISTI

- la L.R. 10/98 ed il vigente Regolamento sull'Organizzazione di ARPAC;
- il D. Lgs. 36/2023;
- l'Avviso Pubblico ACN n. 08/2024 per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente, a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity", Codice d'investimento M1C1I1.5;
- la deliberazione n. 760/2023 di approvazione di Bilancio di previsione esercizio 2024 e pluriennale per il triennio 2024/2026;

Per tutto quanto premesso e considerato si propone di adottare la seguente

DELIBERAZIONE

Per le motivazioni espresse in narrativa che qui si intendono integralmente riportate e trascritte:

- di approvare la partecipazione di ARPAC all' < Avviso Pubblico ACN n. 08/2024 per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity", Codice d'investimento M1C1I1.5 >;

- di approvare il Progetto preliminare, allegato alla presente, redatto in conformità alle indicazioni previste nel modello Allegato B1 – Schema di Progetto -, con codice CUP E64F24000270006;

- di approvare il seguente Quadro finanziario:

Intervento	**Importo contributo richiesto (al netto di IVA)**	**Valore IVA [non compilare]**	**Importo totale contributo richiesto (IVA inclusa)**
1. Governance e programmazione cyber	469.500,00 €	103.290,00 €	572.790,00 €
2. Gestione del rischio cyber e della continuità operativa	197.000,00 €	43.340,00 €	240.340,00 €
3. Gestione e risposta agli incidenti di sicurezza	93.000,00 €	20.460,00 €	113.460,00 €
4. Gestione delle identità digitali e degli accessi logici	53.000,00 €	11.660,00 €	64.660,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	336.000,00 €	73.920,00 €	409.920,00 €
TOTALE COSTI DIRETTI			1.401.170,00 €
SPESE GENERALI 7%			98.081,90 €
TOTALE RICHIESTO A FINANZIAMENTO			1.499.251,90 €

- di dare atto che le spese previste per la realizzazione delle attività oggetto del progetto troverebbero integrale copertura finanziaria nell'ammontare complessivo del contributo riconosciuto ad ARPAC e non richiedono il ricorso a risorse aggiuntive proprie dell'Agenzia;

- di nominare Responsabile del Progetto la dott.ssa Loredana La Via, Dirigente della UO Sistemi Informativi e Informatici;

- di procedere, con successivi atti, alla nomina di un supporto amministrativo per le attività di rendicontazione finanziaria.

Napoli, 21 marzo 2024

Il Dirigente UO Sistemi Informativi e Informatici

dott.ssa Loredana La Via

La proposta di deliberazione è accolta.

Napoli, 22/03/2024

Il Direttore Generale
Avv. Luigi Stefano SORVINO

OGGETTO: AVVISO PUBBLICO N. 08/2024 PER LA PRESENTAZIONE DI PROPOSTE DI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER DEI GRANDI COMUNI, DEI COMUNI CAPOLUOGO DI REGIONE, DELLE CITTÀ METROPOLITANE, DELLE AGENZIE REGIONALI SANITARIE E DELLE AZIENDE ED ENTI DI SUPPORTO AL SERVIZIO SANITARIO NAZIONALE, DELLE AUTORITÀ DI SISTEMA PORTUALE, DELLE AUTORITÀ DEL BACINO DEL DISTRETTO IDROGRAFICO E DELLE AGENZIE REGIONALI PER LA PROTEZIONE DELL'AMBIENTE A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY", CODICE D'INVESTIMENTO M1C1I1.5 – APPROVAZIONE PROPOSTA DI PROGETTO, CUP E64F24000270006.

AVVISO PUBBLICO n. 08/2024

per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul

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

M1C1I1.5

ALLEGATO B1 – SCHEDA DI PROGETTO

TITOLO PROGETTO " Assessment e potenziamento della resilienza cyber di ARPAC"

SOGGETTO PROPONENTE: Agenzia Regionale per la Protezione dell'Ambiente della Campania

Sezione 1 – ANAGRAFICA DEL SOGGETTO PROPONENTE

1.A Dati identificativi del Soggetto proponente	
Denominazione	Agenzia Regionale per la Protezione dell'Ambiente della Campania
Codice IPA	arlpa_
CF/P.IVA	07407530638
Posta elettronica certificata (PEC)	direzionegenerale.arpac@pec.arpacampania.it
1.B Dati identificativi del titolare del potere di impegnare il Soggetto proponente *(come riportato nell'Allegato A)*	
Nome e Cognome	Luigi Stefano Sorvino
Qualifica	Direttore Generale
Residente in (*indicare Via/Piazza, n. civico e CAP)*	Avellino, Via M. Pironti, 65 CAP 83100
Riferimenti di contatto	Mail: s.sorvino@arpacampania.it/segreteria@arpacampania.it N. Telefono: 0812326302
1.C Dati identificativi del Responsabile del Progetto proposto	
Nome e Cognome	Loredana La Via
Qualifica	Dirigente - UO Sistemi Informativi e Informatici/RTD
CF	LVALDN62A58H703A
Nato a *(indicare il luogo e la data di nascita)*	Salerno, 18/01/1962

Residente in (*indicare Via/Piazza, n. civico e CAP)*	Salerno, Via Trotula de Ruggiero, 30 CAP 84121
Riferimenti di contatto	Mail: l.lavia@arpacampania.it N. Telefono: 0812326362

Sezione 2 – ANAGRAFICA DEL PROGETTO PROPOSTO

2.A Codice Unico di Progetto (CUP) *Indicare il CUP e la tipologia*	CUP: E64F24000270006 ☒ generato in coerenza con le indicazioni di cui al Template CUP "PNRR" ☐ già in possesso, in quanto progetto già avviato
2.B Costo complessivo del progetto *Indicare il costo complessivo del progetto proposto, inclusivo di eventuali ulteriori fonti finanziarie, come risultante dal CUP*	1.499.251,90 €
2.C Importo contributo richiesto *Indicare l'importo del contributo richiesto a valere sul presente Avviso, come risultante dalla compilazione dell'**Allegato B2***	1.499.251,90 €
2.D Importi derivanti da altre fonti di finanziamento *Eventuale, da compilare esclusivamente se il costo del progetto (2.B) risulta maggiore dell'importo del contributo richiesto (2.C)*	_____, fonte: _____ _____, fonte: _____ _____, fonte: _____
2.E Interventi che si intende realizzare *Indicare gli interventi che si intende realizzare nell'ambito del progetto proposto, finalizzati all'analisi e al potenziamento delle capacità di resilienza cyber in termini di postura di sicurezza, processi e modello organizzativo, competenze, sistemi e tecnologie abilitanti, come descritti nel par. 4.1 dell'Avviso*	☒ 1. Governance e programmazione cyber ☒ 2. Gestione del rischio cyber e della continuità operativa ☒ 3. Gestione e risposta agli incidenti di sicurezza ☒ 4. Gestione delle identità digitali e degli accessi logici ☒ 5. Sicurezza delle applicazioni, dei dati e delle reti

Sezione 3 – DESCRIZIONE DEL SOGGETTO PROPONENTE

3.A Descrizione della struttura organizzativa preposta alla governance ed attuazione del progetto *Illustrare il modello organizzativo, il team preposto alla governance ed attuazione del progetto, e i processi e gli strumenti a disposizione, ai fini dell'attribuzione del criterio di valutazione 1.1 dell'Avviso* *Max 200 parole*
L'ARPAC, Ente strumentale della Regione Campania, si compone di un'organizzazione "a rete" con struttura centrale e cinque dipartimenti nelle province di Avellino, Benevento, Caserta, Napoli e Salerno. La struttura centrale (Direzione generale, Direzione tecnica e Direzione amministrativa) definisce le politiche di indirizzo e di sviluppo, coordina le attività tecnico-scientifiche e amministrative dell'ente e ne elabora le strategie di comunicazione. Nello specifico, la struttura deputata al governo e all'attuazione del progetto è la U.O. Sistemi Informativi e Informatici, facente capo alla Direzione Generale con la quale ci sarà una periodica condivisione dello stato di avanzamento della progettualità con la finalità di indirizzare le decisioni e garantire il raggiungimento degli obiettivi prefissati. La U.O. Sistemi Informativi e Informatici è composta da un dirigente e 6 dipendenti alla data di presentazione della candidatura (4 da Maggio 2024) e comporrà il team per la realizzazione del progetto avvalendosi anche di un team esterno con competenze tecniche, anche per la gestione dei processi di monitoraggio delle attività. Nello specifico, anche a seguito di un significativo evento di sicurezza informatica l'Ente ha attivato un servizio SOC esternalizzato, acquisendo anche strumenti di sicurezza perimetrale quali Firewall con l'obiettivo di garantire la sicurezza delle infrastrutture e delle reti.

3.B Indicazione di precedenti progetti in ambito IT e cybersecurity gestiti dal Soggetto proponente, similari al progetto presentato per ambito di intervento e per importo gestito, che possano essere a valore aggiunto nell'attuazione del progetto a valere sul presente Avviso

Indicare, per ciascun progetto, l'oggetto, il periodo di riferimento (MM-AAAA di inizio e MM-AAAA di fine) e il relativo valore annuo ai fini dell'attribuzione dei criteri di valutazione 1.2 e 1.3 dell'Avviso

MAX 10 progetti, con riferimento all'ultimo quinquennio (2019 – 2023)

	Nome progetto	Oggetto del progetto	Periodo di riferimento	Valore annuo
1	**Deliberazione n. 445 del 04/10/2018**	**ADESIONE CONTRATTO QUADRO CONSIP SPC LOTTO 2 (SERVIZI DI GESTIONE DELLE IDENTITA' DIGITALI E SICUREZZA APPLICATIVA).** Per il soddisfacimento delle esigenze dell'Amministrazione, per la durata di 36 mesi, sono state condotte le attività volte al soddisfacimento delle esigenze di seguito sintetizzate: • DLP Data loss/leak prevention: soluzioni in grado di rilevare e fermare potenziali pericoli per i dati sensibili sugli end point indicati. Le soluzioni di Data Loss prevention consentono infatti di identificare, monitorare e proteggere i dati attraverso una corretta analisi del contenuto informativo. • Database Security: Analisi e monitoraggio degli accessi ai DB avvalendosi delle sonde installate presso il CED dell'Amministrazione. • Dynamic Application Security Testing Tipologia Silver: individuazione e analisi delle vulnerabilità applicative sul parco applicativo dell'Amministrazione. La tecnologia utilizzata è IBM Rational Appscan. Tipologia silver.	**2019 - 2023**	**€ 70.195,00**

		• Vulnerability assessment: per tutti gli indirizzi IP pubblici e privati indicati. • Servizio di monitoraggio da remoto: Team di esperti a supporto per il monitoraggio e la correlazione degli eventi di sicurezza, la gestione degli incidenti informatici, Early Warning sulle vulnerabilità. Nell'ambito del catalogo dei servizi previsti sono stati richiesti ed erogati anche Servizi Professionali oltre che sui sopracitati ambiti, anche su un'attività di consulenza, erogata in parte on premises e in parte da remoto		
2	**Deliberazione n. 173/2023 corretta con nuovo schema in Deliberazione n. 233 del 05.04.2023**	**PROTOCOLLO D'INTESA, TRA IL CENTRO OPERATIVO PER LA SICUREZZA CIBERNETICA - POLIZIA POSTALE E DELLE COMUNICAZIONI DI CAMPANIA, BASILICATA E MOLISE, E L'AGENZIA REGIONALE PROTEZIONE AMBIENTALE DELLA CAMPANIA** , per la prevenzione e contrasto dei crimini informatici sui sistemi informativi "critici" dipendenti dall'Agenzia, in cui, anche attraverso l'interscambio di dati, le Parti si impegnano a sviluppare un piano di collaborazione volto: 1 alla condivisione ed all'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture informatiche dell'Agenzia Regionale per la Protezione Ambientale della Campania per le finalità meglio in premessa specificate; 2 alla segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione; 3 all'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche gestite dall'Agenzia Regionale Protezione Ambientale Campania o che traggano origine dalle medesime; 4 alla realizzazione e alla gestione di attività di comunicazione fra le Parti per	**2023 – attivo**	**N/A**

		fronteggiare situazioni di emergenza.		
3				
4				
5				
6				
7				
8				
9				
10				

3.C Indicazione di precedenti progetti gestiti dal Soggetto proponente finanziati da Fondi nazionali, europei o internazionali

Indicare, per ciascun progetto, l'oggetto, il periodo di riferimento (MM-AAAA di inizio e MM-AAAA di fine) e il relativo valore annuo, precisando inoltre la denominazione e la tipologia del fondo (nazionale, europeo o internazionale) ai fini dell'attribuzione del criterio di valutazione 1.4 dell'Avviso

MAX 10 progetti, con riferimento all'ultimo quinquennio (2019 – 2023)

	Nome progetto	**Denominazione e tipologia del fondo**	**Oggetto del progetto**	**Periodo di riferimento**	**Valore annuo**
1	**Deliberazione n. 81 del**	**Fondo Comunitario**	POR FESR CAMPANIA 2014-2020- O.S. 2.2-	**2020 - 2023**	**€ 2.566.234,00**

	2020		AZIONE 2.2.2. DG 10. PROGETTO SERVIZI SMART INFORMATIVI AL CITTADINO, ALLE IMPRESE ED AGLI ENTI SULLA QUALITA' DELL'ARIA, SULLE ACQUE SOTTERRANEE E SULLE EMISSIONI ODORIGENE. CUP: E61D19000020006- SURF: 19050BP000000001" approvato con DD 74 del 04/03/2020 durata 24 mesi oltre proroghe. Importo complessivo progetto: € 2'566'234,00. Funzione ARPAC: soggetto beneficiario del finanziamento e attuatore del progetto		
2	**Deliberazione n. 81 del 2020**	**Fondo Comunitario**	ARPAC – Servizi di E-GOV di Prodotti Climatici Avanzati, finanziato con Fondo Europeo di Sviluppo Regionale	**2020 - attivo**	**€ 320.860,00**
3	**Deliberazione n. 81 del 2020**	**Fondo Comunitario**	ARPAC – Servizi di E-GOV in materia di controlli ambientali, finanziato con Programma Campania per l'Ambiente / Fondo Europeo di Sviluppo Regionale	**2020 – attivo**	**€ 166.896,00**
4	**Deliberazione n. 387 del 2021**	**Fondo Comunitario**	ARPAC – Studio e modellizzazione per il monitoraggio del Covid nei Reflui (SARI), finanziato con Fondi Comunitari	**2021 – attivo**	**€ 200.000,00**

5	**Deliberazione n. 386 del 2021**	**Fondo Comunitario**	ARPAC – Potenziamento dei servizi e delle prestazioni analitiche di ARPAC per il monitoraggio ambientale delle matrici di acqua e aria (AIMA), finanziato con fondi comunitari (D.G.R. 191/2021 – Programma di Azioni integrate per il Monitoraggio Ambientale in Campania)	**2021 – attivo**	**€ 2.837.709,00**
6	**Deliberazione n. 461 del 2022**	**Fondo Statale (Fondi complementari al PNNR)**	RAFFORZAMENTO DEI LABORATORI DELL'ARPAC NELL'AMBITO DEL PIANO NAZIONALE PER GLI INVESTIMENTI OMPLEMENTARI (PNC) PROGETTO "SALUTE AMBIENTE, BIODIVERSITA' E CLIMA"	**2022 – attivo**	**€ 5.596.017,00**
7	**Deliberazione n. 243 del 2023**	**Fondo Comunitario**	ARPAC/Regione Campania – Via vicinale Santa Maria del Piano Torre 1 / Strumentazione Tecnico Scientifica (Finanziato con Fondi U.E.)	**2023 – attivo**	**€ 2.837.709,00**
8	**Deliberazione n. 243 del 2023**	**Fondo Statale**	STRUTTURE TECNICHE DELL'AGENZIA INSISTENTI NEI CAPOLUOGHI DI PROVINCIA DELLA REGIONE*VIA SANTA MARIA DEL PIANTO NAPOLI*STRUMENTAZIONE TECNICO SCIENTIFICA. AVVISO PUBBLICO CONCERNENTE IL PIANO	**2023 – attivo**	**€ 4.591.000,00**

			NAZIONALE PER GLI INVESTIMENTI COMPLEMENTARI (PNC SISTEMA "SALUTE AMBIENTE, BIODIVERSITÀ E CLIMA") DECRETO MEF 15 LUGLIO 2021, N. 77		
9	**Deliberazione n. 547 del 2023**	**Fondo Statale**	PROGRAMMA SALUTE, AMBIENTE, BIODIVERSITÀ E CLIMA - ISS*VIA ARENA*LAVORI DI RISTRUTTURAZIONE DELLE SEDI DI CASERTA E SALERNO FINALIZZATI AL MIGLIORAMENTO DELLA CLASSE ENERGETICA E L'INSTALLAZIONE DI PANNELLI FOTOVOLTAICI PER LA PRODUZIONE DI ENERGIA ELETTRICA. AVVISO PUBBLICO CONCERNENTE IL PIANO NAZIONALE PER GLI INVESTIMENTI COMPLEMENTARI (PNC) - SISTEMA "SALUTE, AMBIENTE, BIODIVERSITÀ E CLIMA"" - DECRETO MEF 15 LUGLIO	**2023 – attivo**	**€ 1.247.734,00**
10	**Deliberazione n. 548 del 2023**	**Fondo Statale**	PROGRAMMA SALUTE, AMBIENTE, BIODIVERSITÀ E CLIMA - ISS*VIA ARENACCIA*LAVORI DI RISTRUTTURAZIONE	**2023 – attivo**	**€ 2.075.070,00**

			ED ADEGUAMENTO DELLA STRUTTURA EX CASERMA VV.FF. - VIA ARENACCIA NAPOLI - NUOVA SEDE LABORATORIO UOC SICB. AVVISO PUBBLICO CONCERNENTE IL PIANO NAZIONALE PER GLI INVESTIMENTI COMPLEMENTARI (PNC) - SISTEMA "SALUTE, AMBIENTE, BIODIVERSITÀ E CLIMA" - DECRETO MEF 15 LUGLIO 2021, N. 77		

3.D Indicazione delle certificazioni relative alla sicurezza informatica e/o alla gestione dei processi e della qualità possedute dal Soggetto proponente

Indicare le certificazioni possedute da parte delle strutture organizzative interne al Soggetto proponente, a qualunque titolo coinvolte nella governance ed attuazione del progetto presentato a valere sul presente Avviso, allegandone una copia, ai fini dell'attribuzione del criterio di valutazione 1.5 dell'Avviso

☐ **Nessuna certificazione**

☒ **Possesso di certificazioni** *(indicare le certificazioni possedute e il riferimento puntuale del relativo allegato a comprova. Eventualmente aggiungere righe)*:

1. ISO 9001:2015 – Sistema di gestione della qualità
2. UNI CEI EN ISO/IEC 17025:2018 – Requisiti generali per la competenza dei laboratori di prova e di taratura
3. ISO 45001:2018 – Sistemi di gestione per la salute e la sicurezza sul posto di lavoro
4. ISO 14001:2015 – Sistema di gestione dell'ambiente

3.E Indicazione delle certificazioni informatiche e di project management possedute dal team preposto alla governance ed attuazione del progetto

Indicare le certificazioni possedute (allegandone una copia) e le figure professionali interne che le detengono, in coerenza con il modello organizzativo presentato

al punto 3.A, ai fini dell'attribuzione del criterio di valutazione 1.6 dell'Avviso
☐ **Nessuna certificazione** ☒ **Possesso di certificazioni** *(indicare le certificazioni possedute e il riferimento puntuale del relativo allegato a comprova. Eventualmente aggiungere righe)*: 1. Certificazione ITIL v3 - ITIL v3 Foundation 02782099-01 G53X ITIL/105175 (11/2013 APMG International) detenuta da una risorsa dell'Ente con profilo professionale di "Collaboratore Tecnico Professionale Senior" 2. 2. Certificazione Lean Six Sigma Belt - Yellow Belt GR765000288VL (11/2014 International Association for Six Sigma Certification (IASSC) - PEOPLECERT GROUP) detenuta da una risorsa dell'Ente con profilo professionale di "Collaboratore Tecnico Professionale Senior" 3. _____ 4. _____ 5. _____

Sezione 4 – PROPOSTA PROGETTUALE

4.A Indicazione delle attuali criticità riscontrate sui sistemi informativi *Indicare, per ciascuno degli interventi selezionati nella Sezione 2.E, le criticità riscontrate*	
1. Governance e programmazione cyber *(da valorizzare solo se scelto)*	L'esigenza di dover rispondere in maniera rapida ed efficace ai cambiamenti, anche imposti dall'ambiente esterno, pone la necessità di un maggior impegno verso le tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati. Difatti, l'Ente, nel 2022, ha dovuto affrontare taluni eventi di sicurezza che hanno accentuato la propria attenzione alle tematiche in oggetto. A tal fine, si rileva di fondamentale importanza il rafforzamento del livello di maturità di ARPAC dal punto di vista del sistema di gestione.

	Allo stato attuale, infatti, non risulta esser stata condotta una attività di assessment tale da fornire una puntuale "fotografia" della postura cyber dell'Ente, così come non si è proceduto alla definizione di un Piano delle iniziative in ambito Cybersecurity. Al contempo, data la mancanza di processi formalizzati, anche in riferimento allo scenario normativo privacy vigente, si rileva la necessità di definire una governance formale dei processi di sicurezza ed il relativo monitoraggio anche in linea con il Piano triennale per l'Informatica della PA.
2. Gestione del rischio cyber e della continuità operativa *(da valorizzare solo se scelto)*	Allo stato attuale, ARPAC non risulta aver identificato i processi critici e, dunque, non sono state condotte le opportune attività volte alla continuità operativa. Al contempo, l'Ente, pur avendo assunto l'impegno di avviare un processo di irrobustimento della propria postura, non ho, allo stato, formalizzato un piano di continuità operativa. Le principali criticità in oggetto, dunque, possono ricondursi all'attuale livello di resilienza cyber che, anche a fronte degli obblighi imposti dal panorama normativo vigente, richiedono un massiccio intervento da parte dell'Ente in materia. Inoltre, rileva la mancata formalizzazione e adozione di metodologie di analisi del rischio cyber e le relative esecuzioni. Da ultimo, occorre evidenziare l'assenza di una metodologia di gestione del rischio delle terze parti così come la successiva conduzione di attività di audit sulle stesse.
3. Gestione e risposta agli incidenti di sicurezza *(da valorizzare solo se scelto)*	Il panorama delle minacce informatiche, unitamente agli obblighi normativi vigenti, richiede all'Ente un rafforzamento della capacità e della prontezza da parte dello stesso nella risposta e nella gestione degli incidenti di sicurezza, che consenta di ridurre i tempi di ripristino dei sistemi, a fronte di eventuali interruzioni di servizi critici. Allo stato attuale, invero, la governance in materia di risposta agli incidenti non risulta sufficientemente matura, mancando, da un lato un adeguato piano di risposta agli incidenti e, dall'altro, le più idonee procedure atte a

	disciplinare i processi in ambito. Inoltre, al fine di sfruttare le potenzialità delle tecnologie di protezione e monitoraggio degli eventi di cui l'Ente si è dotato, diventa di primaria importanza l'implementazione di soluzioni organizzative e la definizione di piani di risposta tempestiva agli incidenti di sicurezza, volte a ridurre il rischio di danni di natura reputazionale e finanziaria, con l'obiettivo di garantire la conformità alla normativa nazionale e sovrannazionale in ambito.
4. Gestione delle identità digitali e degli accessi logici *(da valorizzare solo se scelto)*	L'attuale livello di gestione delle identità digitali e degli accessi logici, non sufficientemente maturo, richiede una verifica approfondita dell'attuale gestione dei processi rilevanti in ambito e delle relative tecnologie. L'assenza di una gestione centralizzata delle procedure di ciclo di vita delle identità, della corretta profilazione e ricertificazione periodica, rischia di rappresentare un rischio di sicurezza diffuso e difficilmente tracciabile. La gestione delle utenze privilegiate necessiterà di una particolare attenzione per garantire gli standard di sicurezza richiesti così come sarà necessario approfondire le attuali modalità di autenticazione e valutare l'adeguato aggiornamento alle pratiche più recenti. In aggiunta, si rileva la mancata formalizzazione di una metodologia di identificazione e gestione degli Amministratori di sistema, anche ai sensi della normativa vigente.
5. Sicurezza delle applicazioni, dei dati e delle reti *(da valorizzare solo se scelto)*	Allo stato attuale, l'Ente non ha condotto e non ha definito un piano di attività periodiche volte all'identificazione degli asset critici al fine di identificare lo stato di esposizione alle vulnerabilità nonché la predisposizione di attacchi simulati (atti a verificare concretamente la possibilità di rilevare vulnerabilità identificate). A tal fine, non risulta attivo alcun servizio specialistico finalizzato alla definizione e al rafforzamento delle configurazioni di sicurezza unitamente ad una procedura di Vulnerability Management. In aggiunta, non risulta esser stata definita e adottata una metodologia di security e privacy by design con lo scopo di garantire un adeguato livello di sicurezza nonché protezione delle informazioni e dei dati personali sin

	dalla fase di progettazione dei servizi e dei sistemi. Ciò può affermarsi tenendo comunque conto che l'Ente si è dotato di una componente tecnologica di maggior impatto quale, in primis, l'acquisizione di strumenti di sicurezza perimetrale quali firewall e da tecnologie atte al monitoraggio tramite l'acquisizione di un servizio SOC H24 Remoto che sarà necessario estendere in termini di durata del servizio.

4.B Indicazione e descrizione delle tipologie di intervento che si intende realizzare per ciascun intervento

Indicare per ciascun intervento selezionato nella Sezione 2.E, una o più tipologie di intervento che si intende realizzare, e fornire descrizione di dettaglio dei contenuti operativi delle specifiche attività previste

1. Governance e programmazione cyber *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione ☒ C. Formazione e miglioramento della consapevolezza delle persone ☐ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

Il progetto prevede l'esecuzione di un **assessment della postura di sicurezza dell'ente** mediante un approccio basato su interviste, condotto mediante l'utilizzo del Framework Nazionale per la Cybersecurity e la Data Protection. L'attività in oggetto verrà condotta sulla base di un approccio multilivello, in cui si innesteranno anche attività di Cyber Testing (successivo punto 4).

I risultati dell'assesment consentiranno all'Ente di **definire una Roadmap evolutiva delle iniziative di cybersecurity**, che rappresenterà la traccia per

irrobustire la postura di sicurezza e che sarà **oggetto di costante monitoraggio per l'intera durata della progettualità** (anche mediante **attività specifiche di PMO**).

Inoltre, alla luce dell'articolazione territoriale dell'Agenzia, che si compone di una **Struttura Centrale e di cinque Dipartimenti Provinciali**, in ottica di maggior capillarità, verranno svolti anche degli **assessment verticali sui singoli Dipartimenti citati**.

Sulla base delle criticità sopra rappresentate e sui risultati dell'assessment verrà inoltre implementato un sistema di gestione per la sicurezza – integrato con la **normativa in ambito privacy** – che consisterà nella **definizione di un modello organizzativo** finalizzato a definire ruoli e responsabilità, unitamente alla **formalizzazione dei processi di sicurezza** e, dunque, delle relative **policy e procedure** aventi impatto sull' U.O. Sistemi Informativi e Informatici nonché sull'intera organizzazione. E' previsto anche un supporto, a valle della formalizzazione del framework documentale, per l'ingaggio delle funzioni dell'Ente impattate con una finalità informativa e formativa.

Inoltre, con l'obiettivo di **rafforzare la consapevolezza** delle persone, saranno erogate **attività di formazione** (sia in aula virtuale che in aula fisica) al **personale Dirigente dell'ente**, coinvolgendo anche **il personale dei Dipartimenti Provinciali**, irrobustendo le pratiche di igiene informatica e di base e formazione in materia di cybersicurezza, come previsto dallo scenario normativo vigente.

Infine, saranno condotte attività di **follow up dell'assessment** con l'obiettivo di monitorare lo stato di evoluzione della postura a seguito degli interventi oggetto dell'intera progettualità.

2. Gestione del rischio cyber e della continuità operativa *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione ☒ C. Formazione e miglioramento della consapevolezza delle persone ☐ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

Con riguardo alle attività in oggetto, si prevede, in primis, **l'identificazione dei processi con impatto critico** sulle attività dell'Ente su cui dovranno essere condotte le attività di **Business Impact Analysis** (BIA) al fine di eseguire una valutazione degli impatti, con relativa definizione di RTO e RPO. Parimenti verrà definito il **framework documentale in ambito Business Continuity Management** in linea con lo standard ISO 22301 finalizzato alla definizione dei processi di gestione della crisi ICT per contenere l'impatto relativo all'indisponibilità dei sistemi IT, ripristinare rapidamente le attività e continuare ad erogare i servizi prioritari.

Tali attività saranno condivise con le UU.OO. coinvolte, mediante l'erogazione di un **workshop** volto al coinvolgimento attivo dell'organizzazione oltre per una finalità di carattere formativo.

Compatibilmente con quanto sopra definito sarà formalizzata una **procedura di gestione dei backup e restore** in linea con quanto già avviato dall'Ente dal punto di vista operativo.

Sarà infine predisposta e adottata una **metodologia di analisi del rischio cyber** finalizzata all'identificazione del rischio attuale dei processi critici con l'esecuzione della medesima analisi e la relativa definizione dei piani di trattamento**.** Sulla base di essa, **saranno condotte analisi del rischio cyber per un perimetro selezionato di processi.**

Da ultimo, sarà predisposto un modello di **gestione del rischio cyber delle terze parti** con l'obiettivo di disciplinare la catena di fornitura per i servizi ICT dell'Ente e minimizzare il rischio derivante dai soggetti terzi. Saranno inoltre identificati i servizi esternalizzati critici dell'ente al fine di condurre attività di **audit sulle terze** parti identificate.

3. Gestione e risposta agli incidenti di sicurezza *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☐ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione ☒ C. Formazione e miglioramento della consapevolezza delle persone

	☐ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

Con riguardo a tale tipologia di intervento, verrà formalizzato uno specifico **processo di rilevazione e gestione degli incidenti** (IRP) che descriva il modello operativo comprensivo di ruoli, responsabilità e attività da condurre per la gestione degli incidenti di sicurezza, sulla base degli strumenti tecnologici di monitoraggio in uso presso l'Ente.

A tal proposito, infatti l'obiettivo sarà valorizzare anche l'adozione degli attuali servizi di monitoraggio SOC mediante la formalizzazione del corpo documentale atto a disciplinare le fasi (Identification, Forensic investigation, Remediation & response, Eradication e Recovery & Lesson Learned) che consentano una risposta efficace in caso di violazioni o gravi incidenti. Il modello di incident management che l'Ente si propone di adottare prevede siano inclusi:

- **Processo di rilevazione, risposta agli incidenti e modello di ripartenza e relativa Procedura di Incident Response Management** (comprensiva di Template di Incident Response Report): l'obiettivo di questa fase è quello di definire gli standard relativi alla gestione degli incidenti di Cybersecurity e condividerli con gli stakeholder nonché di definire il modello per la gestione della ripartenza dei servizi;
- **Workflow di rilevazione e risposta agli incidenti (Incident response Playbooks):** in tale fase verrà quindi predisposta la redazione delle procedure operative relative alla gestione degli incidenti di Cybersecurity, definendo azioni, ruoli e responsabilità.

A seguito di tali attività saranno condotte **sessioni formative** al personale IT (interno ed esterno all'Ente) volte alla condivisione dell'assetto di sicurezza di cui l'Ente si è dotato.

Da ultimo, con riferimento all'azione in oggetto, verranno erogate **attività formative Tabletop** (ossia esercitazioni atte a simulare scenari di incidente informatico) anche con le figure apicali, al fine di verificare ed accrescere la consapevolezza dell'organizzazione in materia.

4. Gestione delle identità digitali e degli accessi logici *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione ☐ C. Formazione e miglioramento della consapevolezza delle persone ☐ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

Nell'ambito delle attività di assessment, descritte nel precedente paragrafo 1, sarà condotta un'attività di assessment quale **deep-dive relativi alla Gestione delle identità digitali** e degli **accessi logici** con l'obiettivo di verificare lo stato di maturità corrente ed identificare le iniziative per garantire la conformità ed efficienza operativa sulla gestione ottimale delle identità digitali e dei relativi accessi.

La definizione dei processi operativi e la formalizzazione del corpo documentale verrà eseguito sulla base del dettaglio della gap-analysis, risultato dell'analisi, e con particolare attenzione all'adattamento dei processi e procedure attualmente in uso o in alternativa al disegno di processi da best-practice.

Sarà necessario garantire un'adeguata gestione dei processi Joiner-Mover-Leaver relativi al ciclo di vita delle identità, i processi di ricertificazione delle assegnazioni e di monitoraggio degli accessi.

Sarà oggetto di tale intervento anche la definizione di un processo di gestione e monitoraggio delle utenze privilegiate al fine di adottare un'adeguata gestione in tale ambito e garantire la minimizzazione del rischio derivante da una gestione approssimativa e con la finalità di efficientare gli attuali strumenti in uso.

5. Sicurezza delle applicazioni, dei dati e delle reti *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione

	☐ C. Formazione e miglioramento della consapevolezza delle persone ☒ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

Nell'arco della durata progettuale, con cadenza periodica, verranno condotti **Vulnerability Assessment e Penetration Test (VAPT)** su un perimetro selezionato di sistemi IT dell'Ente, a seguito della definizione di un piano di test cadenzato che tenga conto della criticità dei sistemi.

Le attività di VAPT verranno eseguite mediante metodologie globalmente riconosciute come standard per la conduzione delle stesse con l'obiettivo di identificare le vulnerabilità dell'ente mediante le possibili tecniche di attacco e di intrusione a cui l'Ente potrebbe essere soggetto.

Le attività sopra menzionate, inoltre, risulteranno abilitanti per la definizione di un piano strategico di iniziative tattiche in ambito cybersecurity che tenga conto sia delle risultanze della cyber posture sopra descritta, sia delle azioni in oggetto.

Con specifico riferimento ai risultati delle attività di VAPT, peraltro, verrà predisposto uno specifico piano di rientro, atto a definire le azioni specifiche necessarie per mitigare o risolvere le vulnerabilità identificate durante l'analisi.

A tal fine verrà definita una roadmap dettagliata, contenente parametri di priorità (calcolati a partire dal rischio associato alla vulnerabilità e dall'impatto della stessa sull'operatività), raccomandazioni, workaround e soluzioni di protezione per affrontare le vulnerabilità in modo efficace e ridurre il rischio di compromissione della sicurezza dell'Ente.

Coerentemente con l'azione di rafforzamento del modello organizzativo nonché dei **processi, politiche e procedure**, con riferimento all'ambito in oggetto verranno redatte politiche ad hoc (es. security e privacy by design; processo di gestione delle vulnerabilità).

In linea di continuità con la governance sopra definita, e a fronte delle esigenze riscontrate in sede di assessment, saranno **acquisite le opportune tecnologie abilitanti** la sicurezza dei dati, delle applicazioni e delle reti (es. rinnovo servizio SOC; SIEM; SOAR).

4.C Indicazione delle amministrazioni locali coinvolte nel progetto presentato e descrizione delle relative modalità di coinvolgimento
Ai fini dell'attribuzione del criterio di valutazione 3.1 dell'Avviso

Amministrazioni locali coinvolte *(aggiungere eventuali righe ulteriori)*		Descrizione delle modalità di coinvolgimento dell'amministrazione indicata
1	**Struttura Centrale - Napoli**	L'organizzazione "a rete" di ARPAC si compone di una Struttura Centrale, con sede a Napoli, e di cinque Dipartimenti Provinciali. La progettualità coinvolgerà, in ottica di maggior capillarità, non solo la struttura centrale bensì anche le articolazioni provinciali nonché la U.O.C. Siti Contaminati e Bonifiche (con sede a Pozzuoli), così consentendo alle amministrazioni in contatto con i singoli Dipartimenti di giovare del rafforzamento della postura cyber degli stessi, ottenendo maggiori garanzie in termini di Riservatezza, Integrità e Disponibilità delle informazioni trattate anche per conto delle competenti amministrazioni territoriali.
2	**Dipartimento Provinciale ARPAC – Napoli**	La progettualità in oggetto coinvolgerà il Dipartimento Provinciale di Napoli (struttura decentrata rispetto a quella centrale sopra citata), così consentendo alle amministrazioni della Provincia, in contatto con il Dipartimento, di giovare del rafforzamento della postura cyber dello stesso, ottenendo maggiori garanzie in termini di Riservatezza, Integrità e Disponibilità delle informazioni trattate anche per conto delle competenti amministrazioni territoriali.
3	**Dipartimento Provinciale ARPAC – Avellino**	La progettualità in oggetto coinvolgerà il Dipartimento Provinciale di Avellino, così consentendo alle amministrazioni della Provincia, in contatto con il Dipartimento, di giovare del rafforzamento della postura cyber dello stesso, ottenendo maggiori garanzie in termini di Riservatezza, Integrità e Disponibilità delle informazioni trattate anche per conto delle competenti amministrazioni territoriali.
4	**Dipartimento Provinciale ARPAC – Benevento**	La progettualità in oggetto coinvolgerà il Dipartimento Provinciale di Benevento, così consentendo alle amministrazioni della Provincia, in contatto con il Dipartimento, di giovare del rafforzamento della postura cyber dello stesso, ottenendo maggiori garanzie in termini di Riservatezza, Integrità e Disponibilità delle informazioni trattate anche per conto delle competenti amministrazioni territoriali.

5	**Dipartimento Provinciale ARPAC – Caserta**	La progettualità in oggetto coinvolgerà, il Dipartimento Provinciale di Caserta, così consentendo alle amministrazioni della Provincia, in contatto con il Dipartimento, di giovare del rafforzamento della postura cyber dello stesso, ottenendo maggiori garanzie in termini di Riservatezza, Integrità e Disponibilità delle informazioni trattate anche per conto delle competenti amministrazioni territoriali.
6	**Dipartimento Provinciale ARPAC – Salerno**	La progettualità in oggetto coinvolgerà il Dipartimento Provinciale di Salerno, così consentendo alle amministrazioni della Provincia, in contatto con il Dipartimento, di giovare del rafforzamento della postura cyber dello stesso, ottenendo maggiori garanzie in termini di Riservatezza, Integrità e Disponibilità delle informazioni trattate anche per conto delle competenti amministrazioni territoriali.

4.D Indicazione dei settori di riferimento della Direttiva NIS impattati dal progetto proposto *Ai fini dell'attribuzione del criterio di valutazione 3.2 dell'Avviso*	
Settori di riferimento della Direttiva NIS impattati	**Descrizione degli impatti del progetto proposto sul potenziamento della resilienza cyber in relazione ai settori di riferimento della Direttiva NIS indicati** *Max 300 parole*

☐ **energia** ☐ **trasporti** ☐ **banche** ☐ **mercati finanziari** ☒ **sanità** ☒ **fornitura e distribuzione di acqua potabile** ☐ **infrastrutture digitali** ☐ **motori di ricerca** ☐ **servizi cloud** ☐ **piattaforme di commercio elettronico**	Tenuto conto di quanto definito dalle disposizioni normative della Direttiva NIS si ritiene che i settori impattati in relazione alle iniziative progettuali richieste tramite tale documento possano considerarsi in maniera trasversale laddove il rafforzamento della postura di sicurezza derivante dall'implementazione delle iniziative sopra descritte comporterà dei riflessi in ciascuno dei servizi che l'Ente è deputato ad erogare. Con ciò si fa riferimento ai servizi individuati, ossia "**Sanità**" e "**Fornitura e distribuzione di acqua potabile**", laddove ARPAC ha competenza, diretta o indiretta, nell'erogazione di servizi volti a contribuire alla salubrità ambientale nonché idrogeologica e pertanto impattanti sui settori individuati. Il progetto, inoltre, basandosi su un approccio "multirischio" nell'adozione di misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete, si pone in linea con le prescrizioni dettate dalla Direttiva NIS. A tal fine, l'Ente, si pone l'obiettivo di rafforzare i propri requisiti minimi di sicurezza, al fine di allinearsi al corpo normativo vigente in materia, anche innalzando il proprio livello di cybersicurezza, con specifico riferimento agli obblighi di gestione del rischio cyber previsti dalla normativa nonché con riferimento all'adozione di misure tecniche, operative e organizzative adeguate e proporzionate alla gestione del citato rischio cyber connesso alla sicurezza dei sistemi informatici e delle reti dell'Ente. Da ultimo, inoltre, verrà rafforzata la consapevolezza dei Dirigenti dell'Ente per ciò che concerne il loro coinvolgimento in processi che saranno oggetto di definizione e formalizzazione, anche mediante campagne di formazione.

4.E Indicazione delle funzioni del Cybersecurity Framework impattate dal progetto proposto *Ai fini dell'attribuzione del criterio di valutazione 3.3 dell'Avviso*	
Funzioni del Cybersecurity Framework	**Descrizione degli impatti del progetto proposto sull'incremento di maturità delle funzioni del Cybersecurity Framework indicate** *Max 300 parole*
☒ **Identify** ☒ **Protect** ☒ **Detect** ☒ **Respond** ☒ **Recover**	In considerazione della progettualità tutta e degli interventi sopra descritti, si ritiene che saranno impattate tutte le funzioni del Cybersecurity Framework al fine di indentificare la strategia di sicurezza in linea con la strategia di potenziamento della postura cyber del Paese. In dettaglio: • ***Identify:*** sono previste attività di assessment orientate all'individuazione dei gap ed alla definizione delle azioni di miglioramento al fine di migliorare la governance di tutti i processi fondanti in ambito cybersecurity. Le attività prevedono la valutazione delle interconnessioni tecnico/normative relative alla gestione cyber-privacy; • ***Protect***: le attività, per tale *function*, riguarderanno gli aspetti tecnici rispetto all'assessment effettuato, definendo delle linee di azione atte a garantire la protezione olistica del patrimonio informativo dell'Ente. In particolare, si tenderà ad incrementare la postura di sicurezza in relazione agli aspetti di IGA garantendo la disponibilità delle informazioni secondo i principi di "*need to know*" e "*least privilege*" e la gestione degli aspetti operativi connessi al "*joiner-mover-leaver*"; • ***Detect:*** Con l'obiettivo di definire e attuare un modello di identificazione e gestione delle vulnerabilità, saranno svolte periodiche attività di Vulnerability Assessment/Penetration test e sarà valutata l'acquisizione di tecnologie abilitanti la sicurezza dei dati, delle applicazioni e delle reti in ambito. In aggiunta sarà incrementata l'awareness dell'Ente rispetto alla gestione in casi di eventi anomali; • ***Respond:*** con l'obiettivo di minimizzare gli impatti derivanti dagli incidenti di sicurezza, sarà definito un

	processo e formalizzato il framework documentale atto a governare gli eventi, unitamente all'erogazione di attività formative tecniche al personale identificato (inclusi i playbooks). Infine, sarà valutata l'acquisizione di tecnologie come riportato al punto precedente; • ***Recover:*** al fine di incrementare la *readiness* dell'Ente rispetto a possibili eventi anomali nell'ambito di riferimento, saranno intraprese attività finalizzate alla formalizzazione dei processi e sarà condotta attività formativa alle funzioni principali per relativamente alla gestione degli incidenti (es. Tabletop).

4.F Indicazione delle finalità perseguite dal progetto proposto e del relativo impatto sulla risoluzione delle criticità dichiarate sui sistemi informativi

Ai fini dell'attribuzione del criterio di valutazione 3.5 dell'Avviso

Max 300 parole

Tenendo conto del panorama di minacce cyber e dello scenario normativo applicabile, ARPAC prevede l'adozione di un approccio volto a rispondere alle mutate esigenze di contesto. L'obiettivo principale è potenziare la propria postura di sicurezza informatica, anche attuando un adeguato processo di monitoraggio, misurazione e comunicazione della sicurezza delle informazioni nell'arco di tutta la fase progettuale.
L'ente intende, dunque, perseguire i seguenti macro-obiettivi:

- Stabilire il livello di maturità dell'Ente e predisporre una roadmap di iniziative volte al consolidamento della maturità dell'Ente. L'obiettivo è perseguito anche mediante l'esecuzione di azioni finalizzate a mitigare i rischi inerenti all'organizzazione e ai servizi erogati, anche in linea con lo scenario normativo privacy vigente;
- Aumentare la consapevolezza delle persone attraverso sessioni formative mirate, al fine di potenziare le capacità di protezione e prevenzione dalle minacce informatiche;
- Valutare e gestire i rischi associati alle relazioni con le terze parti, garantendo la sicurezza dei dati e la conformità normativa;
- Rafforzare la resilienza (BC) e la capacità di migliorare la gestione degli incidenti per irrobustire i processi di Incident Management;
- Condurre una verifica dell'attuale gestione dei processi in ambito e delle relative tecnologie nonché garantire una gestione centralizzata delle procedure di ciclo di vita delle identità, della corretta profilazione e ricertificazione periodica nonché della gestione delle utenze privilegiate;
- Identificare lo stato di esposizione alle vulnerabilità mediante la raccolta di informazioni concernente i servizi erogati, le applicazioni, l'architettura e le componenti tecnologiche nonché eseguire attacchi simulati (PT) per verificare concretamente la possibilità di sfruttare

vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi;

- Valutare l'acquisizione di idonee tecnologie abilitanti atte a rafforzare la sicurezza delle applicazioni, dei dati e delle reti.

Ai fini della compilazione del Quadro finanziario e del Cronoprogramma si rimanda all'Allegato B2.

Glossario

Termini	Descrizione esemplificativa
Identify (Identificazione)	Comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati, al fine di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.
Protect (Protezione)	Implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
Detect (Rilevamento)	Definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
Respond (Risposta)	Definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato, al fine di contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
Recover (Ripristino)	Definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente, al fine di garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.