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 Rafforzamento dei processi e dei sistemi relativi alla cybersecurity

SOGGETTO PROPONENTE Agenzia Regionale per la Protezione Ambientale delle Marche (ARPAM)

Sezione 1 – ANAGRAFICA DEL SOGGETTO PROPONENTE

1.A Dati identificativi del Soggetto proponente	
Denominazione	Agenzia Regionale per la Protezione Ambientale delle Marche (ARPAM)
Codice IPA	arpam
CF/P.IVA	01588450427
Posta elettronica certificata (PEC)	arpam@emarche.it
1.B Dati identificativi del titolare del potere di impegnare il Soggetto proponente *(come riportato nell'Allegato A)*	
Nome e Cognome	Rossana Cintoli
Qualifica	Direttore Generale
Residente in (*indicare Via/Piazza, n. civico e CAP)*	Viale dei Noccioli n. 6 CAP 01012 Capranica (VT)
Riferimenti di contatto	Mail: rossana.cintoli@ambiente.marche.it N. Telefono: 0712132720
1.C Dati identificativi del Responsabile del Progetto proposto	
Nome e Cognome	Rossana Cintoli
Qualifica	Direttore Generale
CF	CNTRSN61D60H501U
Nato a *(indicare il luogo e la data di nascita)*	Roma il 20/04/1961

Residente in (*indicare Via/Piazza, n. civico e CAP)*	Viale dei Noccioli n. 6 CAP 01012 Capranica (VT)
Riferimenti di contatto	Mail: rossana.cintoli@ambiente.marche.it N. Telefono: 0712132720

Sezione 2 – ANAGRAFICA DEL PROGETTO PROPOSTO

2.A Codice Unico di Progetto (CUP) *Indicare il CUP e la tipologia*	CUP: I76G24000090006 ☒ 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*	€ 757.132,00
2.C Importo contributo richiesto *Indicare l'importo del contributo richiesto a valere sul presente Avviso, come risultante dalla compilazione dell'**Allegato B2***	€ 757.132,00
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'ARPAM è un Ente Strumentale della Regione Marche, inserita nel contesto ambientale come componente del SNPA (Sistema Nazionale per la Protezione Ambientale composto da ISPRA e ARPA). In tale contesto, l'ARPAM si relaziona con la Regione per aspetti informatici infrastrutturali, con previsione di incremento di interazione con il CSIRT Regionale di prossima implementazione. Partecipa al tavolo di coordinamento del SNPA in materia di Cybersecurity, finalizzato alla condivisione e miglioramento di aspetti di sicurezza informatica delle singole Agenzie. Il Team preposto alla governance ed attuazione si compone del RTD, dell'U.O. Informatica (composta da n. 1 dirigente e n. 4 dipendenti dedicati alla gestione complessiva dell'ICT) e del supporto amministrativo della Direzione e U.O. Contratti (organico complessivo dell'ARPAM pari a circa 240 dipendenti). In relazione alla natura e ai tempi di conclusione del progetto, per la sua realizzazione si prevede di acquisire competenze da soggetti esterni, utilizzando in prima istanza gli strumenti delle convenzioni e accordi quadro esistenti. Tra i processi e le procedure a disposizione si rappresenta che il tema della sicurezza informatica è attualmente inquadrato nell'ambito di un processo articolato sia mediante implementazione di strumenti (ad es. EDR, firewall) che l'attuazione di interventi formativi per il personale.

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				
2				
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					
2					
3					
4					
5					
6					
7					
8					
9					
10					

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 (allegato certificato RINA n. 43785/23/S)
2. ISO 17025:2017 (allegato certificato ACCREDIA n. 0271L rev 04)
3. _____
4. _____
5. _____

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. _____
2. _____
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)*	**Necessità di disporre di un approccio olistico per la gestione del rischio cyber e per la protezione di sistemi e informazioni. Necessità di incrementare la formazione e consapevolezza del personale in relazione alla sicurezza informatica**
2. Gestione del rischio cyber e della continuità operativa *(da valorizzare solo se scelto)*	**Necessità di definire processi di valutazione sia del rischio Cyber che del processo di backup e restore, in particolar modo per le informazioni ambientali, Core Business dell'Agenzia**
3. Gestione e risposta agli incidenti di sicurezza *(da valorizzare solo se scelto)*	**Necessità di definire il processo di incident management e di estendere il sistema di analisi/risposta di malware sul traffico di rete introducendo anche un MDR**
4. Gestione delle identità digitali e degli accessi logici *(da valorizzare solo se scelto)*	**Utilizzo prevalente di autenticazione a singolo fattore (utente/password)**
5. Sicurezza delle applicazioni, dei dati e delle reti *(da valorizzare solo se scelto)*	**Necessità di migliorare il sistema di analisi delle vulnerabilità. Necessità di incrementare la sicurezza per l'accesso alla rete e di migliorare la sicurezza per la condivisione dati e di posta elettronica anche in ambito cloud**

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
L'intervento risulta di particolare rilevanza per traguardare il miglioramento del processo complessivo di gestione della sicurezza informatica. L'attuazione dell'intervento si declina su varie tipologie di azioni: - *Svolgimento di un'analisi di dettaglio basata sul Framework Nazionale per la Cybersecurity per poter definire un programma evolutivo in termini di processi, organizzazione e tecnologie cyber, che consentirà di poter meglio pianificare varie tipologie di azioni sia nel breve che medio/lungo periodo, in particolare per quanto attiene a processi o investimenti tecnologici* - *Identificazione dei ruoli e delle responsabilità in ambito cyber all'interno dell'amministrazione e definizione di un'architettura documentale a supporto di un modello organizzativo per la gestione della sicurezza delle informazioni e della cybersecurity* - *Promozione ed esecuzione di iniziative di cybersecurity awereness e di phishing education rivolte ai dipendenti dell'amministrazione, finalizzata a incrementare e consolidare la consapevolezza del personale relativamente all'effetto delle proprie azioni verso altri utenti della rete* - *Aggiornamento delle licenze del sw di gestione dell'asset inventory, integrato con sistema di distribuzione delle patch per la mitigazione delle vulnerabilità*	

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
L'intervento si focalizza su azioni di analisi e di progetto, che possano poi consentire di pianificare le implementazione di soluzioni tecnologiche adeguate al contesto di riferimento. *Le attività previste riguardano:* - *la valutazione del rischio e della Business Impact Analysis sui servizi in perimetro* - *la definizione della metodologia di valutazione del rischio e del processo di backup e restore*	

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

Anche per questa tipologia di intervento l'approccio è basato sull'analisi e miglioramento del processo complessivo di identificazione e gestione degli incidenti di sicurezza informatica.

A tal fine sono state individuate le seguenti azioni, propedeutiche per una eventuale integrazione di ulteriori soluzioni tecnologiche:

- *definizione di processi di gestione degli incidenti, dei log e di un playbook per la risposta ad incidenti noti*
- *l'aggiornamento della piattaforma EDR, comprendente sistema di Attack Surface Risk Management, integrata da componenti di collaboration security*
- *implementazione di sistema Anti-APT, per aggiungere un livello di protezione sul traffico di rete*
- *attivazione di un servizio di Managed Detection & Response (MDR) sia per l'EDR che l'anti-APT*

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

L'intervento si struttura su varie tipologie di misure, volte a migliorare sia la fase di analisi che quella di processo e di sviluppo di nuovi sistemi.

A tal fine, si avvieranno le seguenti azioni:

- *valutazione e hardening della postura di sicurezza dell'Active Directory*
- *definizione del processo di gestione delle identità e degli accessi al sistema informatico*
- *evoluzione verso Microsoft 365 Business Premium, contenenti applicazioni per la sicurezza (Intune, ecc.)*
- *acquisizione di smartphone da assegnare al personale dell'Ente per gestione della MFA. L'acquisizione si basa sul noleggio dello smartphone, compresi i canoni di connettività e i servizi di gestione*

Si ritiene che questo approccio consentirà di estendere il perimetro dell'uso del doppio fattore di sicurezza anche ad altre applicazioni che potranno interagire con l'app Authenticator di Microsoft o con eventuali altre app specifiche.

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

L'intervento viene declinato su varie tipologie di azioni, basate su aspetti di analisi, di miglioramento dei processi, di implementazione di nuovi sistemi e di previsione di attività formativa. Nello specifico si rappresentano le seguenti:

- *analisi della postura focalizzata su procedure di Vulnerability Assessment e Penetration Test, alle quali è poi associata una stima di costi per eventuali interventi di rafforzamento delle configurazioni e di applicazioni software*
- *attività formative per i tecnici del settore ICT*
- *implementazione di NAC ridondato (attività comprensiva di analisi, implementazione, configurazione e manutenzione); l'intervento è previsto in forma integrata con la sostituzione di alcuni apparati LAN (switch) ritenuti non idonei per la nuova architettura*
- *migrazione a Microsoft 365 per incrementare il livello di sicurezza della posta elettronica e di altre applicazioni condivise. L'azione comprende interventi di tipo infrastrutturale e di aggiornamento dei client, oltre a supporto tecnico e formazione. L'intervento è inoltre integrato all'intervento indicato nel presente progetto per il miglioramento della gestione delle identità digitali mediante implementazione di MFA*
- *sostituzione di alcuni pc portatili con notebook aventi disco allo stato solido al fine di incrementare le dotazioni mobili con disco crittografato e ridurre l'impatto in termini di sicurezza dei dati, ad es. in caso di furto del pc.*

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		
2		
3		
4		
5		

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**	**Arpam non risulta direttamente coinvolta nell'ambito di applicazione della Direttiva NIS. Tuttavia, alcune delle attività svolte sono rivolte verso soggetti rientranti nell'attuazione della NIS. A tal fine si ritiene rilevante evidenziare le seguenti, svolte direttamente da Arpam, che si integrano nel processo delle attività dei soggetti coinvolti dalla NIS:** - **analisi laboratoristica in materia di acque potabili, con ricadute sia verso il settore della sanità che quello della fornitura e distribuzione di acqua potabile** - **attività in materia di epidemiologia, in relazione ad aspetti sanitari** - **monitoraggi ambientali, con effetti sul settore sanitario** **Il potenziamento della resilienza cyber riveste pertanto un ruolo di particolare rilevanza per consentire a soggetti coinvolti nell'ambito della direttiva NIS di svolgere le azioni di rispettiva competenza.**

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**	Il progetto prevede un percorso orientato a migliorare aspetti di natura procedurale, organizzativa e tecnologica. Le azioni di assessment sono finalizzate a migliorare la comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati al fine di definire: - processi, risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali - attività per il ripristino dei processi e dei servizi impattati da un incidente, al fine di garantire la resilienza dei sistemi e delle infrastrutture Sono inoltre previsti interventi di implementazione di misure e procedure volti: - all'incremento della protezione dei processi di business e degli asset aziendali - all'attuazione di attività per identificare e gestire tempestivamente incidenti di sicurezza informatica - all'attuazione delle attività per intervenire quando un incidente di sicurezza informatica venisse rilevato, al fine di contenere l'impatto determinato Si ritiene pertanto che tra gli impatti del progetto si possano considerare sia il miglioramento dell'approccio strutturale e infrastrutturale che quello culturale nel contesto della cybersecurity. Di seguito si riporta un riepilogo delle principali azioni previste, connesse alle Funzioni del Cybersecurity Framework:

	Funzioni del Cybersecurity Framework / **Azioni**
	Identify: Assessment, governance, valutazione rischio
	Protect: Sistema EDR, Anti APT, MFA, formazione, valutazione rischio, valutazione incidenti, NAC, VA/PT
	Detect: EDR, MDR, valutazione incidenti, NAC
	Respond: MDR, formazione, valutazione incidenti
	Recover: Backup , formazione, valutazione incidenti

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

Attraverso un approccio olistico che abbraccia attività di assessment, procedure, tecnologia e formazione, il progetto proposto mira a rafforzare la sicurezza cibernetica per proteggere il patrimonio informativo dell'ente da attacchi informatici, frodi e violazioni dei dati.

L'assessment iniziale ha il principale obiettivo di fare una valutazione quantitativa degli aspetti che possono migliorare i processi e i sistemi di sicurezza, grazie all'elaborazione di un gap analysis che consentirà di determinare una roadmap strutturata di miglioramento

Gli interventi proposti sono finalizzati a ridurre la probabilità di successo dei vari tentativi di intrusione, grazie ad una maggiore consapevolezza del personale (formazione e campagne di phishing), ad un sistema di autenticazione più robusto (MFA), e ad una maggiore attenzione sui comportamenti anomali (Anti-APT e MDR).

Lo sviluppo di una governance adeguata e di una strategia strutturata per la gestione degli incidenti consentirà una maggiore resilienza in caso di attacchi informatici e capacità di garantire la continuità dei servizi resi.

Gli interventi di valutazione del rischio e la revisione delle procedure di backup e recovery sono finalizzati ad irrobustire i processi di gestione della continuità operativa.

Gli interventi di vulnerability assessment, penetration test e gestione delle vulnerabilità sono finalizzati a migliorare la postura di sicurezza, riducendo i punti deboli che potrebbero essere sfruttati da eventuali aggressori

Le attività progettate consentiranno inoltre di poter programmare ulteriori interventi al termine del progetto per poter dare continuità al processo di incremento della sicurezza informatica.

L'intervento è inoltre inserito nel contesto della strategia regionale di sicurezza informatica in cui Arpam, in qualità di Ente strumentale della Regione, ne risulta parte. Le attività previste sono inoltre finalizzate a perseguire gli obiettivi di sicurezza del Piano Triennale AGID e ad incrementare l'interazione e sinergia con il CSIRT regionale di prossima implementazione.

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.