



Decreto del Direttore amministrativo nr. 20 del 11/03/2026

Proponente: *Marco Chini*

Sira

Pubblicità/Pubblicazione: Atto soggetto a pubblicazione *integrale* (sito internet)

Visto per la pubblicazione - Il Direttore generale: Dott. Pietro Rubellini

Responsabile del procedimento: *Dott. Marco Chini*

Estensore: Jacopo Cappelli - Struttura stabile di supporto ai sensi dell'art. 15 del D.Lgs. n. 36/2023: Settore

Provveditorato

Oggetto: *Adesione al lotto 2 della Convenzione avente ad la fornitura di apparati infrastrutturali e networking per Regione Toscana, le Aziende Sanitarie/Ospedaliere ed enti del Servizio Sanitario Regionale Toscano, stipulata da ESTAR con Telecom Italia S.p.A. (mandataria), in R.T.I. con Wetech's S.p.A. Società Benefit a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity M1C1I1.5" - CUP E19B24000020006" per implementare un sistema EDR/XDR per la protezione degli endpoint e dell'infrastruttura di rete e un servizio SIEM che consenta una migliore visione e consapevolezza degli eventi che si manifestano nella rete*

ALLEGATI N.: 1

<i>Denominazione</i>	<i>Pubblicazione</i>	<i>Tipo Supporto</i>
Allegato "A" - relazione di acquisto	sì	digitale

Natura dell'atto: *immediatamente eseguibile*

Trattamento dati personali: *Sì* **Numerosità degli interessati:** *1 - 1.000*

Il Direttore amministrativo

Vista la L.R. 22 giugno 2009 n° 30 e s.m.i., avente per oggetto “Nuova disciplina dell’Agenzia regionale per la protezione ambientale della Toscana (ARPAT)”;

Visto il decreto del Direttore generale n. 96 del 10.06.2021, con il quale alla sottoscritta è stato attribuito, a decorrere dal 10.06.2021, l’incarico di Direttore amministrativo dell’Agenzia regionale per la protezione ambientale della Toscana;

Dato atto che con decreto del Direttore generale n. 50 del 05.03.2024 è stato adottato il Regolamento di organizzazione di ARPAT, ai sensi dell’art. 20 co. 3 della LRT n. 30/2009, (approvato dalla Giunta Regionale Toscana con delibera n. 968 del 05.08.2024), successivamente adeguato alla DGRT 968/24 con decreto del Direttore generale n. 167 del 05.09.2024;

Visto l’“Atto di disciplina dell’organizzazione interna” approvato con decreto del Direttore generale n. 270/2011, modificato ed integrato con decreti n. 87 del 18.05.2012 e n. 2 del 04.01.2013, nonché l’“Atto di disciplina dell’organizzazione interna” approvato con decreto del Direttore generale n. 225 del 27.11.2024 in corso di attuazione;

Preso atto che:

- ARPAT ha partecipato al bando dell’Agenzia per la Cybersicurezza Nazionale (ACN) a seguito di avviso pubblico n. 08/2024 a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity M1C1I1.5”, presentando una proposta di progetto denominata “ARPAT - Interventi di potenziamento della resilienza cyber”;
- l’obiettivo dell’investimento 1.5 “Cybersecurity M1C1I1.5” è rafforzare l’ecosistema digitale nazionale potenziando i servizi di gestione della minaccia cyber, grazie ad una rinnovata capacità di monitoraggio, prevenzione e scrutinio tecnologico a supporto della transizione digitale del Paese;
- l’Agenzia per la Cybersicurezza Nazionale (ACN), in stretto contatto con l’amministrazione titolare, il Dipartimento per la trasformazione digitale (DTD), cura l’attuazione dell’investimento connettendo il mondo della Pubblica Amministrazione, dell’impresa e dei fornitori di tecnologia;
- l’Agenzia per la Cybersicurezza Nazionale (ACN), con comunicazione del 25.09.2024 (ns. prot. n. 2024/75757) ha notificato l’approvazione del progetto individuato con CUP E19B24000020006 e la relativa concessione del finanziamento per complessivi euro 1.494.683,00 IVA compresa;
- il progetto approvato dall’ACN prevede le seguenti categorie di intervento:
 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.

Considerato che con decreto del Direttore generale n. 228 del 29.11.2024 si è preso atto:

- dell’ammissione al finanziamento del progetto presentato a valere sull’avviso pubblico n. 08/2024, approvato con la Determina di ACN (prot. n. 30550 del 23.9.2024) per un importo complessivo di euro 1.494.683,00 IVA inclusa;
- della sottoscrizione dell’atto d’obbligo di accettazione del finanziamento, sottoscritto dal legale rappresentante di ARPAT ed inviato all’Agenzia per la Cybersicurezza Nazionale (ACN) con ns. prot. 84691 del 24.10.2024;
- che il termine ultimo per la conclusione delle attività di progetto è il 31.03.2026;

Preso atto inoltre che:

- in data 04.11.2021 Estar (Ente di Supporto Tecnico Amministrativo Regionale), quale ente avvalso del Soggetto Aggregatore Regione Toscana, ha indetto una procedura aperta suddivisa in 2 lotti, volta alla stipula di una Convenzione per la fornitura di apparati infrastrutturali e networking per Regione Toscana, le Aziende Sanitarie/Ospedaliere ed enti del Servizio Sanitario Regionale Toscano;
- con Determinazione del Direttore di Estar n. 782 del 27.5.2022 la sopracitata procedura è stata aggiudicata come segue:
 - lotto 1: a Telecom Italia S.p.A. (mandataria), in R.T.I. costituendo con Webkornier s.r.l. di Montevarchi (AR) (mandante),
 - lotto 2: a Telecom Italia S.p.A. (mandataria) in R.T.I. costituendo con Itech Project and Consulting S.r.l. di Calenzano (FI) (mandante);
- che dal 1.1.2023 la società Solarisys S.r.l. e la Società Itech Project and Consulting S.r.l. si sono fuse per incorporazione nella società Webkornier S.r.l. che, nella sua veste di incorporante, ha cambiato la propria denominazione in Wetech's S.p.A. Società Benefit;
- che la società Wetech's S.p.A. Società Benefit è subentrata in tutti i rapporti attivi e passivi precedentemente intestati alle società incorporate.

Vista la "Richiesta di avvio di procedura di affidamento" (RAP) di cui alla PG.SG.10 avente ad oggetto "Approvvigionamento e valutazione dei fornitori", agli atti, con la quale il Responsabile del Settore SIRA - al fine di implementare un sistema EDR/XDR (Intervento 5B "Implementazione di un sistema EDR/XDR per la protezione degli endpoint e dell'infrastruttura di rete", e un servizio SIEM (Intervento 3D "implementazione di un servizio SIEM che consenta una migliore visione e consapevolezza degli eventi che si manifestano nella rete") - ha chiesto di aderire al lotto 2 della Convenzione/Accordo Quadro, della durata di 48 mesi, stipulata da ESTAR con Telecom Italia S.p.A. (mandataria), in R.T.I. con Wetech's S.p.A. Società Benefit (mandante) per un importo complessivo di euro 65.522,60 (oltre IVA);

Vista la relazione di acquisto "Allegato "A" a firma del dirigente responsabile della transazione digitale, Dott. Alessandro Gignoli e del dirigente responsabile del Settore SIRA nella quale vengono specificati i beni e servizi da acquistare, ricompresi nel lotto 2 della sopra citata convenzione, nonché l'offerta del fornitore, (allegato "3" e "4" alla relazione di acquisto) di seguito specificati:

- "Apex One as a Service with XDR: New, Normal, 501-1000 User License,12 months" (codice OS01144788) al costo unitario di euro 26,89 oltre IVA per 780 utenze: totale euro 20.974,20 oltre IVA,
- "Apex One as a Service with XDR: Renew, Normal, 501-1000 User License,12 months" (codice OS01144836) al costo unitario di euro 26,89 oltre IVA per 780 utenze: totale euro 20.974,20 oltre IVA,
- "Apex One as a Service with XDR: Renew, Normal, 501-1000 User License,12 months" (codice OS01144836) al costo unitario di euro 26,89 oltre IVA per 780 utenze: totale euro 20.974,20 oltre IVA,
- "Sistemista Senior reti e sicurezza 10 anni esperienza" (codice 72000000-5 B) al costo unitario di euro 650,00 oltre IVA per 4 giornate/uopmo: totale euro 2,600,00 oltre IVA,

Dato atto che ARPAT per l'utilizzo del lotto 2 della citata Convenzione per la fornitura di apparati infrastrutturali e networking, la cui scadenza è fissata al 13.07.2026, deve accedere al Negozio Elettronico del Sistema telematico START di Estar, inviando tramite il portale un "Ordinativo di Fornitura" direttamente al fornitore;

Considerato che, al fine di ottemperare alle condizioni previste dal Piano nazionale di ripresa e resilienza (PNRR), si rende necessario integrare la documentazione della suddetta Convenzione con i seguenti documenti, che verranno richiesti agli operatori economici interessati:

1. Dichiarazione assenza conflitto interessi dell'operatore economico;

2. Dichiarazione titolare effettivo da parte dell'operatore economico;
3. copia dell'ultimo Rapporto sulla situazione del personale redatto, con attestazione della sua trasmissione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità;

Tenuto presente che saranno finanziati con i fondi erogati dall'Agenzia per la Cybersicurezza Nazionale (ACN) nell'ambito del progetto di cui trattasi solamente le prestazioni erogate ed i servizi svolti dal R.T.I. aggiudicatario della citata Convenzione che saranno concluse entro e non oltre il 31.03.2026, riservandosi di valutare successivamente l'eventuale necessità di avvalersi di ulteriori prestazioni e servizi svolti dal R.T.I. aggiudicatario, prevedendone la copertura con risorse proprie dell'Agenzia;

Ritenuto inoltre:

- di individuare, quale "Responsabile del Procedimento" secondo l'art. 15 ("Responsabile unico del progetto (RUP)") del D.Lgs. n. 36/2023, il Dott. Marco Chini, in qualità di Responsabile del Settore SIRA;
- di nominare quale "Direttore dell'esecuzione del contratto", secondo l'art. 114 ("Direzione dei lavori e dell'esecuzione dei contratti") del D.Lgs. n. 36/2023, Silvia Giubbilini del Settore SIRA, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto, e quali "Assistenti al Direttore dell'esecuzione del contratto" con funzioni di "Direttore operativo" Rita Gargani e Stefano Paci, assegnati al Settore SIRA, e Jacopo Cappelli e Filippo Del Campana, assegnati al Settore Provveditorato, per le attività di controllo, principalmente ma non esclusivamente, contabile ed amministrativo sulla fase di esecuzione del contratto e di verifica/certificazione della regolare esecuzione delle attività contrattuali;

Visto l'art. 45 del D.Lgs. n. 36/2023 ("Incentivi alle funzioni tecniche") e, in particolare, i commi 2 e 3;

Visto altresì l'allegato I.10 "Attività tecniche a carico degli stanziamenti previsti per le singole procedure" al vigente Codice appalti che elenca le attività tecniche (articolo 45, comma 1);

Dato atto che l'art. 32 dell'allegato II.14 al D.Lgs. n. 36/2023 definisce i servizi e forniture di particolare importanza e stabilisce che ai fini dell'individuazione dei contratti di servizi e forniture di particolare importanza, per qualità o importo delle prestazioni, nei quali è previsto, ai sensi dell'articolo 114, comma 8, del codice, che il direttore dell'esecuzione deve essere diverso dal RUP, si applica il vocabolario comune per gli appalti pubblici (CPV - "Common Procurement Vocabulary"), adottato con regolamento (CE) n. 213/2008 della Commissione europea, del 28 novembre 2007;

Rilevato che l'art. 32, comma 2, lett. c) dell'allegato II.14 al D.Lgs. n. 36/2023 individua tra questi, in via di prima applicazione, i servizi informatici e affini, tra i quali rientrano i "Servizi informatici: consulenza, sviluppo di software, Internet e supporto CPV 72000000-5";

Ritenuto, in via prudenziale, nelle more dell'adozione della nuova modalità di riparto degli incentivi per le funzioni tecniche, alla luce delle recenti sopracitate disposizioni, di accantonare la quota massima del 2% dell'importo posto a base della procedura di affidamento di cui trattasi, pari a euro 1.310,40, con riserva di verificare successivamente l'effettiva spettanza e il quantum;

Preso atto che per l'espletamento del presente appalto non sono rilevabili i rischi interferenti per i quali sia necessario adottare specifiche misure di sicurezza e che, pertanto, non risulta necessario prevedere la predisposizione del "Documento Unico di Valutazione dei Rischi da Interferenze" (DUVRI), ai sensi dell'art. 26, comma 3-bis, del D.Lgs. n. 81/2008 e s.m.i. e non sussistono, di conseguenza, specifici costi della sicurezza di cui al medesimo art. 86;

Ritenuto il presente affidamento legittimo e conforme all'interesse pubblico ai sensi dell'art. 17, comma 5 del D.Lgs. n. 36/2023;

Visto il decreto del Direttore generale n. 192 del 30.12.2015 avente ad oggetto “Modifica del decreto del Direttore generale n. 138 del 26.09.2013 e adozione del Disciplinare interno in materia di gestione dei rapporti tra le strutture di ARPAT ed il Collegio dei revisori”;

Visto il parere positivo di regolarità contabile in esito alla corretta quantificazione ed imputazione degli effetti contabili del provvedimento sul bilancio e sul patrimonio dell’Agenzia espresso dal Responsabile del Settore Bilancio e Contabilità riportato in calce;

Visto il parere positivo di conformità formale alle norme vigenti, espresso dal Responsabile del Settore Affari Generali, riportato in calce;

decreta

1. di disporre, per le motivazioni espresse in narrativa, l’adesione al lotto 2 della Convenzione avente ad oggetto la fornitura di apparati infrastrutturali e networking per Regione Toscana, le Aziende Sanitarie/Ospedaliere ed enti del Servizio Sanitario Regionale Toscano, stipulata da ESTAR con Telecom Italia S.p.a. (mandataria), in R.T.I. con Wetech’s Spa Società Benefit (mandante) per acquistare quanto segue e previsto nel listino della citata Convenzione di Estar:
 - “Apex One as a Service with XDR: New, Normal, 501-1000 User License,12 months” (codice OS01144788) al costo unitario di euro 26,89 oltre IVA per 780 utenze: totale euro 20.974,20 oltre IVA,
 - “Apex One as a Service with XDR: Renew, Normal, 501-1000 User License,12 months” (codice OS01144836) al costo unitario di euro 26,89 oltre IVA per 780 utenze: totale euro 20.974,20 oltre IVA,
 - “Apex One as a Service with XDR: Renew, Normal, 501-1000 User License,12 months” (codice OS01144836) al costo unitario di euro 26,89 oltre IVA per 780 utenze: totale euro 20.974,20 oltre IVA,
 - “Sistemista Senior reti e sicurezza 10 anni esperienza” (codice 72000000-5 B) al costo unitario di euro 650,00 oltre IVA per 4 giornate/uopmo: totale euro 2,600,00 oltre IVA,al fine di implementare un sistema EDR/XDR (Intervento 5B “Implementazione di un sistema EDR/XDR per la protezione degli endpoint e dell’infrastruttura di rete”, e un servizio SIEM (Intervento 3D “implementazione di un servizio SIEM che consenta una migliore visione e consapevolezza degli eventi che si manifestano nella rete”) così come descritti nell’allegato “3” (Tabella elenco prodotti servizi) al presente decreto e nell’offerta del fornitore (allegato “4”) per un importo complessivo di euro 65.522,60 (oltre IVA);
2. di dare atto che non sono rilevabili i rischi interferenti per i quali sia necessario adottare specifiche misure di sicurezza e che, pertanto, non risulta necessario predisporre il “Documento Unico di Valutazione dei Rischi da Interferenze” (DUVRI), ai sensi dell’art. 26, comma 3-bis del D.Lgs. n. 81/2008 e s.m.i. e non sussistono, di conseguenza, specifici costi della sicurezza;
3. di dare, altresì, atto che
 - il costo dell’affidamento è di 65.522,60 oltre IVA (euro 79.937,57 IVA compresa), e che tale importo sarà ricompreso alla voce “Acquisti di beni e servizi” del 2026;
 - il costo dell’intervento sarà finanziato con le risorse erogate dall’Agenzia per la Cybersicurezza Nazionale (ACN) nell’ambito del progetto di cui trattasi solamente i servizi svolti e le prestazioni erogate dal R.T.I. aggiudicatario della citata Convenzione che saranno concluse entro e non oltre il 31.03.2026, riservandosi di valutare successivamente l’eventuale necessità di avvalersi di ulteriori prestazioni e servizi svolti dal R.T.I. aggiudicatario, prevedendone la copertura con risorse proprie dell’Agenzia;
4. di accantonare, in via prudenziale, nelle more dell’adozione della nuova modalità di riparto degli incentivi per le funzioni tecniche, alla luce delle recenti sopracitate disposizioni, la quota massima del 2% dell’importo posto a base della procedura di affidamento di cui trattasi, pari a

euro 1.310,40, con riserva di verificare successivamente l'effettiva spettanza e il quantum;

5. di dare atto che le funzioni di “Responsabile Unico del Progetto” saranno espletate dal dirigente responsabile del Settore SIRA - Dott. Marco Chini;
6. di nominare quale “Direttore dell’esecuzione del contratto”, secondo l’art. 114 (“Direzione dei lavori e dell’esecuzione dei contratti”) del D.Lgs. n. 36/2023, Silvia Giubbilini del Settore SIRA, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto, e quali “Assistenti al Direttore dell’esecuzione del contratto” con funzioni di “Direttore operativo” Rita Gargani e Stefano Paci, assegnati al Settore SIRA, e Jacopo Cappelli e Filippo Del Campana, assegnati al Settore Provveditorato, per le attività di controllo, principalmente ma non esclusivamente, contabile ed amministrativo sulla fase di esecuzione del contratto e di verifica/certificazione della regolare esecuzione delle attività contrattuali;
7. di dare atto che il Settore Provveditorato, come da Atto di organizzazione interna, svolge funzioni di struttura stabile di supporto dei RUP ai sensi dell'art. 15 del D.Lgs. n. 36/2023 e s.m.i. in continuità con l’art. 31, comma 9, del D.Lgs. 50/2016 e s.m.i., così come stabilito, altresì, nel decreto del Direttore generale n. 41/2017;
8. di dichiarare il presente decreto immediatamente eseguibile, al fine di consentire l’adesione da parte di ARPAT e il conseguente inizio delle attività quanto prima in modo da rispettare i tempi previsti dal progetto dell’Agenzia per la Cybersicurezza Nazionale (ACN) individuato con CUP E19B24000020006.

Il Direttore amministrativo
Dott.ssa Paola Querci *

“Documento informatico sottoscritto con firma digitale ai sensi del Codice dell’amministrazione digitale, D.Lgs. 82/2005 e s.m.i, predisposto e conservato come nativo digitale e disponibile presso l’amministrazione”

Il Decreto è stato firmato elettronicamente da:

- Marta Bachechi , responsabile del settore Affari generali in data 10/03/2026
- Andrea Rossi , responsabile del settore Bilancio e Contabilità in data 10/03/2026
- Marco Chini , il proponente in data 10/03/2026
- Paola Querci , Direttore amministrativo in data 10/03/2026
- Pietro Rubellini , Direttore generale in data 10/03/2026

ARPAT - DIREZIONE TECNICA - Settore Sistema Informativo Regionale Ambientale

Via Ponte alle Mosse, 211 - 50144 - Firenze

N. Prot: Vedi segnatura informatica cl.: del 20/02/2026

Relazione di acquisto

Oggetto: Acquisto di un sistema EDR/XDR e di un sistema AGENTIC SIEM su finanziamento ACN a seguito di AVVISO PUBBLICO n. 08/2024 valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity M1C111.5, CUP: _E19B24000020006

Premesso che:

- ARPAT ha partecipato al bando ACN a seguito di AVVISO PUBBLICO n. 08/2024 valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity M1C111.5 presentando una proposta di progetto descritta nell’Allegato B1.
- ACN ha finanziato il progetto (CUP: _E19B24000020006, contributo di euro 1.494.683) con comunicazione del 25/9/2024, con responsabile del progetto Dott. Alessandro Gignoli.
- A seguito del finanziamento ARPAT si è attivata per avviare il progetto che prevede le seguenti categorie di intervento:
 - 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.
- Per ognuna di queste categorie di intervento sono state individuati una serie di interventi specifici, per un totale di complessivi 19 interventi (vedi Allegato B2).

Considerato che con decreto del Direttore generale n. 228 del 29.11.2024, ARPAT ha preso atto:

- dell’ammissione al finanziamento del progetto presentato a valere sull’avviso pubblico n. 08/2024 per la presentazione di proposte di interventi di potenziamento della resilienza cyber, approvato con la Determina di ACN (prot. n. 30550 del 23.09.2024), per un importo complessivo di euro 1.494.683,00 IVA inclusa;
- della sottoscrizione dell’atto d’obbligo di accettazione del finanziamento, sottoscritto dal legale rappresentante di ARPAT ed inviato all’Agenzia per la Cybersicurezza Nazionale (ACN) con ns. prot. 84691 del 24.10.2024;

Tenuto conto che:

- In riferimento all'intervento 5B "Sicurezza delle applicazioni, dei dati e delle reti. Miglioramento dei processi e dell'organizzazione" ARPAT intende implementare un sistema EDR/XDR per la protezione degli endpoint e dell'infrastruttura di rete.
- In riferimento all'intervento 3D "Gestione e risposta agli incidenti di sicurezza. Progettazione e sviluppo di nuove tecnologie" ARPAT intende implementare un sistema SIEM per raccogliere, correlare e analizzare in tempo reale i log e gli eventi provenienti da tutta l'infrastruttura IT per rilevare minacce, monitorare comportamenti anomali

tutto ciò premesso per i motivi esposti, si chiede di:

- Acquisire, per l'importo complessivo di euro 79.934,40 compresa IVA, di cui euro 65.379,80 per il sistema XDR e euro 14554,60 per il sistema SIEM, tramite la PROCEDURA APERTA, SUDDIVISA IN DUE LOTTI, PER LA FORNITURA DI APPARATI INFRASTRUTTURALI E NETWORKING PER REGIONE TOSCANA, LE AZIENDE SANITARIE/OSPEDALIERE ED ENTI DEL SERVIZIO SANITARIO REGIONALE TOSCANO - SOGGETTO AGGREGATORE (CUI 2020-021-0010) i prodotti necessari all'implementazione del sistema EDR/XDR e SIEM elencati nell'allegato A, comprensivo di attività di installazione, configurazione, formazione alla gestione infrastruttura, per l'importo desunto dal relativo listino afferente alla succitata procedura di acquisto
- nominare quale "Direttore dell'esecuzione del contratto", di cui all'art. 114 comma 7 del D.Lgs 36/2023, Silvia Giubbilini del Settore SIRA, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto e, Stefano Paci e Rita Gargani come "Assistenti al Direttore dell'esecuzione del contratto";
- individuare il sottoscritto, Responsabile del SIRA, quale responsabile del presente procedimento, ai sensi dell'art. 15 del D.Lgs 36/2023 e s.m.i..

In allegato alla presente.

- Allegato 1: Proposta di progetto
- Allegato 2: Quadro finanziario e cronoprogramma.
- Allegato 3: Proposta economica fornitore per acquisizione servizi XDR e SIEM.
- Allegato 4: Codici di acquisto su convenzione ESTAR.

Il Responsabile per il Digitale/Responsabile del progetto

Dott. Alessandro Gignoli¹.

¹Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs 82/2005. L'originale informatico è stato predisposto e conservato presso ARPAT in conformità alle regole tecniche di cui all'art. 71 del D.Lgs 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'art. 3 del D.Lgs 39/1993

Responsabile del SIRA

Dott. Marco Chini²

²Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs 82/2005. L'originale informatico è stato predisposto e conservato presso ARPAT in conformità alle regole tecniche di cui all'art. 71 del D.Lgs 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'art. 3 del D.Lgs 39/1993

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: ARPAT-Interventi di potenziamento della resilienza cyber
**SOGGETTO PROPONENTE: ARPAT-Agenzia Regionale per la protezione ambientale della
Toscana**

Sezione 1 – ANAGRAFICA DEL SOGGETTO PROPONENTE

1.A Dati identificativi del Soggetto proponente	
Denominazione	Agenzia Regionale per la protezione ambientale della Toscana
Codice IPA	arpat
CF/P.IVA	04686190481
Posta elettronica certificata (PEC)	arpat.protocollo@postacert.toscana.it
1.B Dati identificativi del titolare del potere di impegnare il Soggetto proponente (come riportato nell'Allegato A)	
Nome e Cognome	Pietro Rubellini
Qualifica	Direttore Generale
Residente in (indicare Via/Piazza, n. civico e CAP)	Via Carlo Poma 7 50100, Firenze
Riferimenti di contatto	Mail: _dirgen@arpat.toscana.it _____ N. Telefono: ____05532061_____
1.C Dati identificativi del Responsabile del Progetto proposto	
Nome e Cognome	Alessandro Gignoli
Qualifica	Dirigente Analista
CF	GGNLSN66P29D612S
Nato a (indicare il luogo e la data di nascita)	Firenze 29/09/1966

Residente in (<i>indicare Via/Piazza, n. civico e CAP</i>)	
Riferimenti di contatto	Mail: <u>_a.gignoli@arpat.toscana.it</u> N. Telefono: <u>__+39-348-3968453</u>

Sezione 2 – ANAGRAFICA DEL PROGETTO PROPOSTO

2.A Codice Unico di Progetto (CUP) <i>Indicare il CUP e la tipologia</i>	CUP: _E19B24000020006_____ ☒ 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 <i>Indicare il costo complessivo del progetto proposto, inclusivo di eventuali ulteriori fonti finanziarie, come risultante dal CUP</i>	____Euro 1.494.683,00_____
2.C Importo contributo richiesto <i>Indicare l'importo del contributo richiesto a valere sul presente Avviso, come risultante dalla compilazione dell'Allegato B2</i>	____Euro 1.494.683,00_____
2.D Importi derivanti da altre fonti di finanziamento <i>Eventuale, da compilare esclusivamente se il costo del progetto (2.B) risulta maggiore dell'importo del contributo richiesto (2.C)</i>	_____, fonte: _____ _____, fonte: _____ _____, fonte: _____
2.E Interventi che si intende realizzare <i>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</i>	☒ 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

Team di progetto:

1. Settore Sira, RUP Dott. Marco Chini, responsabile, coordinatore e assistente RUP Dott. Alessandro Gignoli, Dirigente Analista e RTD, 6 funzionari, con competenze IT e gestionali.
2. Settori Provveditorato e Direzione Amministrativa (Dott.ssa Paola Querci): coordinamento attività amministrative forniture beni e servizi.
3. Settore Pianificazione dell'Agenzia: coordinamento e integrazione con la pianificazione dell'Agenzia (PIAO) e verifica conformità con i sistemi di gestione certificati.
4. Tecnici, specialisti e PM di fornitori esterni, esperti e manutentori dell'infrastruttura IT (contratti PdL, assistenza sistemistica e networking, database, telefonia e applicativi): supporto implementativo.
5. Tecnici e specialisti dell'infrastruttura ARPAT su SCT, Sistema Cloud Toscana: supporto implementativo.
6. Personale esterno specialistico di supporto: svolgimento delle attività implementative previste da ogni singolo progetto e relativi contratti.

Lo svolgimento del progetto prevederà le fasi di avvio, pianificazione, esecuzione, monitoraggio e controllo e conclusione mediante (a titolo di esempio) riunioni periodiche, diagrammi di Gantt, documentazione specifica. Nell'ambito dei vari task progettuali saranno definiti:

- Obiettivi.
- Risorse, budget e le tempistiche.
- Analisi dei rischi.
- Milestone e il piano di consegne.
- Piani di comunicazione.

- **Fasi di test e validazione.**
- **Formazione del personale.**
- **Metriche di valutazione e le modalità di monitoraggio.**
- **Documentazione.**

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	Migrazione posta e collaboration a O365	Acquisizione di licenze O365 e migrazione servizi di posta elettronica di ARPAT con apposito contratto aggiuntivo di supporto.	2021-2024	150.000
2	Contratto assistenza Pdl, e sistemistica	Contratto RT per la gestione e l'assistenza delle Pdl, sistemistica e telefonia.	2021-2026	400.000
3	Ivanti	Acquisizione di un sistema per la gestione e l'asset delle PdL (EPM) e per la gestione dell'helpdesk IT (ITSM).	2023-2024	80.000
4	Migrazione licenze collaboration a M365	Acquisto e implementazione licenze aggiornate (M365 E3) per piattaforma di collaboration, con implementazione di intune anche su dispositivi mobili.	2023-2024	50.000
5	SCT Cloud	Migrazione a SCT dei server, firewall e servizi erogati precedentemente tramite infrastruttura on premise.	2022-2026	200.000
6	RTRT4	Migrazione alla nuova connettività regionale RTRT4, con ampliamento di banda, attivazione di connettività ridondata e gestione della connettività delle centraline della qualità dell'aria.	2023-2024	300.000

7	Sostituzione pdl – dotazione cellulari	Sostituzione di tutte le PdL di Agenzia con portatili nuova generazione, aggiornati a Windows 11 con sistema antivirus e gestione asset. Dotazione cellulari di servizio a tutti i dipendenti per utilizzo MFA, fortitoken per VPN e sms/authenticator per 365.	2022-2024	200.000
8	Antivirus Trendmicro/Apex One	Rinnovo licenze sistema antivirus Trendmicro e collegamento al servizio in cloud di gestione	2024	20.000
9	Papercut	Attivazione sistema papercut per ritiro stampe tramite badge, nel rispetto delle norme GDPR.	2022-2025	40.000
10	Networking sede direzione	Messa in opera e attivazione infrastruttura di networking ridondata e in sicurezza presso il nuovo complesso della Direzione Generale (3 edifici) con relativo firewall per i laboratori.	2022	20.000

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	CLASTER Interreg Italia Marittimo Francia	Europeo	Il progetto CLASTER ha come obiettivo quello di migliorare il clima acustico nelle aree urbane prossime ai porti, riducendo l'impatto sonoro in-dotto dalle sorgenti sonore portuali a beneficio delle popolazioni residenti in tali zone	2024-2026	35.000

2	Progetto Salpam - Piano Nazionale per gli investimenti complementari E.1 Salute, Ambiente, Biodiversità e Clima	Nazionale	L'obiettivo generale del progetto è quello di sviluppare azioni di promozione, fornire indicazioni e supporto alle politiche e alle normative in tema di pianificazione urbana sostenibile ai fini della riduzione della pressione ambientale degli impatti sulla salute umana in contesti urbani caratterizzati dalla presenza di porti.	2023-2025	35.000
3	Progetto Horizon Europe One- Blue	Europeo	ONE-BLUE will provide an integrated assessment of contaminants of emerging concern (CECs) and their impacts, will develop new monitoring tools, and will provide an advanced understanding of the combined effects of CECs and climate change (CC) on the different marine ecosystems and their biodiversity.	2024-2026	55.000
4	Progetto REPORT Interreg Italia Marittimo Francia	Europeo	L'obiettivo generale a lungo termine di REPORT è la mitigazione delle emissioni sonore dei porti nell'area di cooperazione transfrontaliera per rendere più sostenibili le infrastrutture portuali dello Spazio Marittimo. Ciò è ottenibile attraverso la creazione di un approccio specifico per la corretta gestione del rumore.	2018-2021	38.000

5	Progetto MON ACUMEN Interreg Italia Marittimo Francia	Europeo	La presenza di importanti porti commerciali comporta un disturbo notevole per le città portuali circostanti, con quartieri residenziali a pochi passi da sorgenti di rumore rilevanti. MON ACUMEN affronta il tema della pianificazione e del controllo acustico nei porti commerciali dell'area di cooperazione sviluppando una comune metodologia di analisi della descrizione acustica e del rilevamento del rumore	2018-2021	102.000
6	Progetto NEMO Noise and Emissions Monitoring and radical mitigation H2020-EU.3.4. ID: 860441	Europeo	NEMO aims to create new systems to empirically measure emissions and noise emitted by individual vehicles identifying noisy and polluting vehicles in existing traffic and make this information available to tolling or access systems.	2021-2023	66.000
7	Nereide Progetto Life CONTRACT Project LIFE15 ENV/IT/000268 "Noise Efficiently REduced by recycleD pavEments	Europeo	The LIFE NEREiDE project wants to demonstrate the use of new porous asphalt pavements and low noise surfaces composed by recycled asphalt pavements and crumb rubber from scrap tires.	2017-2021	40.000
8	Progetto AER	Europeo	Il progetto promuove la riduzione delle emissioni inquinanti derivanti dalle attività	2020-2023	100.000

	NOSTRUM Interreg Italia Marittimo Francia		portuali ed in particolare, dalle navi. L'obiettivo generale del progetto è contribuire a preservare o migliorare la qualità dell'aria nelle aree prospicienti i porti dell'area di cooperazione favorendo al contempo la crescita sostenibile delle attività portuali, nel rispetto della normativa vigente e delle politiche ambientali europee. prioritarie garantendo la massima ricaduta su tutto il territorio ammissibile		
9	Turtlenest Progetto Life CONTRACT Project n. 101074584 LIFE21-NAT-IT-LIFE "Caretta caretta* nesting range expansion under climate warming: urgent actions to mitigate threats at emerging nesting sites in the Western Mediterranean - TURTLENEST"	Europeo/Nazionale	The LIFE Turtlenest project WILL IMPROVE THE STATE OF CONSERVATION OF CARETTA CARETTA, SPECIES PRIORITY OF THE DIRECTOR. HABITAT, THANKS AD AN INTERNATIONAL NETWORK, THE USE OF BEST PRACTICE PROCEDURES REVISED FOR MITIGATE THREATS TO NESTING SITES EMERGING	2023-2024	36.000

10	LIFE16 GIE/IT/000761- "SUPPORTING ENVIRONMENTAL GOVERNANCE FOR THE POSIDONIA OCEANICA SUSTAINABLE TRANSPLANTING OPERATIONS - SEPOSSO"	Europeo/Nazionale	Il progetto LIFE SEPOSSO ha l'obiettivo di implementare e diffondere sistemi e strumenti volti sia al sostegno di efficaci processi di controllo atti a valutare l'ottemperanza dei reimpianti di Posidonia oceanica realizzati come opera di compensazione sia come utili strumenti di supporto alla pianificazione di tali attività per i diversi portatori d'interesse, tecnici e amministratori, coinvolti in tale tematica, in conformità con la legislazione ambientale dell'Unione.	2023-2024	60.000
----	--	-------------------	--	-----------	--------

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 _____
2. ISO 17025 _____
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)

Attualmente in Arpat non sono presenti atti e documenti di processo riguardanti policy e governance in ambito cybersecurity. Le attività in questo ambito vengono svolte senza una effettiva formalizzazione specifica, se non per quanto richiesto da normative riguardanti altri ambiti (es. GDPR o linee guida AGID). L'attuale postura di sicurezza non è mai stata analizzata. E' necessario rivedere il modello organizzativo nel suo complesso per potere conoscere ed effettivamente migliorare la postura cyber dell'ente.

La mancanza di un team per la gestione della Cybersecurity, aggiornamento del personale IT e procedure di intervento è una reale criticità. Il personale non IT è stato formato nel 2023 con corsi generici sulla cybersicurezza ed una campagna di phishing, non più riproposta.

2. Gestione del rischio cyber e della continuità operativa

(da valorizzare solo se scelto)

I server e i servizi di Agenzia, a seguito di un progetto specifico di migrazione in cloud, sono in trasferimento presso SCT (Sistema Cloud Toscana). L'attività è in fase avanzata ma la migrazione non prevede un piano di DR. I backup vengono effettuati. Attualmente ARPAT riscontra carenze di controllo asset e la necessità di migliorare le procedure e i servizi che garantiscono la continuità operativa, in particolare a seguito di attacco cyber.

dal servizio cloud ma non vengono trasferiti in altra sede. Non vengono verificati eventuali presenze di password/credenziali su collection in rete o analoghi (haveibeenpowned, pastebin,

	etc) e dark web. Non è stata effettuato un asset perimetrale e una valutazione del rischio specifica.
3. Gestione e risposta agli incidenti di sicurezza <i>(da valorizzare solo se scelto)</i>	In ARPAT non sono presenti strumenti di controllo che consentano di ridurre l'impatto di un cyber attacco. Non sono inoltre mai stati attivati servizi il controllo della postura di sicurezza e processo di test e remediation in continuo. Inoltre non sono definiti e previsti processi di incident response e incident management, come procedure documentate per la gestione degli incidenti cyber, di verifica dei log e nessun tipo di playbook. Non è presente alcun tipo di sistema per la raccolta centralizzata dei log dei sistemi e degli apparati e per la loro analisi. Non è presente alcun tipo di servizio per l'intervento tempestivo in caso di attacco cyber identificato dai sistemi di analisi dei log.
4. Gestione delle identità digitali e degli accessi logici <i>(da valorizzare solo se scelto)</i>	ARPAT sta dismettendo un servizio LDAP di autenticazione oramai obsoleto ed ha attivato da circa 3 anni un servizio di autenticazione Active Directory on premise. Tale servizio viene utilizzato per l'autenticazione di tutti gli applicativi, per l'accesso VPN e per il tenant. Non è attiva una autenticazione MFA per gli applicativi, interni e in SaaS esposti all'esterno (es. contabilità, LIMS, gestione paghe/personale), e per l'accesso alla postazione di lavoro. Il sistema AD, pur ridonato, non è stato verificato dal punto di vista cyber e non risulta replicato su Cloud.

5. Sicurezza delle applicazioni, dei dati e delle reti

(da valorizzare solo se scelto)

ARPAT non ha proceduto all'ingegnerizzazione delle reti in ottica cybersecurity, non ha definito un processo di security by design, controlli del perimetro esterno e gestione delle vulnerabilità

La maggioranza delle applicazioni presenti nell'infrastrutture on premise Agenzia sono datate, sviluppate internamente da personale non specializzato, non aggiornate o aggiornabili e progettate con criteri di sicurezza moderni. Anche i siti web principali (www, sira e intranet) sono datati, sviluppati con tecnologie non aggiornabili e non sono stati progettati con criteri che garantiscano una adeguata protezione cyber.

In particolare i siti www e intranet utilizzano un cms Plone versione 3.3.5 (del 2010) non più aggiornabile e il sito Sira è costituito da una eterogeneità di applicazioni non sicure e aggiornato con modalità non controllate (semplice copia di file su server). Anche i principali applicativi interni sono stati sviluppati con tecnologie datate (PHP 5, Classic ASP, Plone 3.3.5, etc.) e spesso da personale con profilo tecnico ma non informatico senza alcun tipo di formazione specifica a riguardo della cybersecurity.

Nelle sedi periferiche di ARPAT non è presente alcun sistema di protezione e monitoraggio del traffico di rete, come firewall e sistemi di gestione degli accessi fisici delle prese di rete.

Gli endpoint, nella maggior parte portatili utilizzati anche in smartworking, hanno solo un antivirus, non sono dotati di sistemi di verifica e controllo tipo EDR e di accesso alla rete.

Non è mai stata verificata la resilienza del sistema di sicurezza perimetrale e interno.

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 di analizzare l'attuale postura di sicurezza rilevando eventuali criticità in un'ottica di compliance alle attuali norme vigenti, in particolare alla direttiva NIS2, la cui prossima adozione a livello nazionale impatterà molto probabilmente ARPAT.

Essendo ARPAT carente di policy e governance in ambito cybersecurity, il progetto prevede una consulenza per definizione di un modello organizzativo con una analisi iniziale della postura di sicurezza.

A seguito dell'analisi iniziale verrà definito un piano di miglioramento cyber di dettaglio, in cui saranno inseriti processi, la struttura organizzativa e le tecnologie cyber. Tale attività verrà affiancata da una adeguata formazione per il personale IT e la programmazione di ulteriori programmi di formazione per gli utenti con campagne di awareness incluso phishing e simulazione attacco cyber.

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

Il progetto prevede, mediante un servizio di consulenza, una analisi dell'asset aziendale e del rischio correlato, con relativa definizione della metodologia di valutazione.

Verrà inoltre valutato il perimetro classificando gli asset esposti ed individuando quelli potenzialmente critici, effettuando anche test specifici sul perimetro esterno e l'attivazione di servizi di servizi cyber threat intelligence e security rating per verificare l'esposizione di informazioni aziendali all'esterno e innalzare ulteriormente la postura di sicurezza dell'Agenzia.

Inoltre verranno analizzate le attuali procedure di backup e restore, analizzando i processi e le vulnerabilità in caso di attacco cyber.

Il progetto prevede inoltre la pianificazione e l'attivazione di un sistema di DR da implementare utilizzando il servizio cloud di Regione Toscana dove sono presenti i server di Agenzia (SCT – Sistema Cloud Toscana). A fianco del sistema di DR verrà attivato un ulteriore sistema di messa in sicurezza dei backup effettuati con copia in cloud e/o presso altra sede remota.

Verrà inoltre erogata la necessaria formazione riguardante gli aspetti di gestione dei servizi di cybersecurity, dell'asset, dei processi, del DR e del backup a tutti i soggetti IT coinvolti.

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

Il progetto prevede l'implementazione di una attività di red teaming con l'obiettivo di testare la postura di sicurezza iniziale dell'infrastruttura e definire un piano di miglioramento, al termine del quale verrà effettuata una nuova attività di red teaming per testare la crescita della postura di sicurezza, definendo un processo di test e remediation in continuo.

Con l'ausilio di una consulenza esterna verranno predisposte le procedure riguardanti la gestione e la risposta a incidenti cyber, ad esempio un processo di gestione degli incidenti, un registro degli incidenti e playbook standard per la gestione degli incidenti noti. Verrà erogata la relativa formazione IT sulla gestione e organizzazione per la risposta a incidenti di sicurezza.

Verranno implementate tecnologie abilitanti che consentano una migliore visione e consapevolezza degli eventi che si manifestano nella rete, in particolare SIEM e SOAR. L'inserimento di queste tecnologie permetterà un innalzamento rilevante della postura di sicurezza iniziale.

I servizi SIEM e SOAR verranno affiancati da un servizio SOC per garantire un intervento tempestivo in caso di attacco cyber.

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

Il progetto prevede, per quanto riguarda la gestione delle identità digitali e gli accessi logici, una consulenza per hardening del dominio AD, comprendente anche l'attivazione in cloud del dominio stesso, per aumentarne la resilienza e renderlo utilizzabile anche a servizi esterni in SaaS e ai dispositivi collegati al di fuori della rete ARPAT.

Inoltre verrà avviata una consulenza per la definizione e la formalizzazione delle politiche di accesso applicativo e sistemi, comprendendo anche l'implementazione di un sistema di autenticazione MFA su tutti i sistemi (pdl, applicativi, etc.).

Per quanto riguarda gli accessi amministrativi si prevede di attivare un sistema IAM/PAM di gestione e controllo di tali accessi.

Per tutti questi servizi verrà erogata al settore IT una adeguata formazione.

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
Il progetto prevede l'implementazione di test di vulnerability assessment per misurare la postura di sicurezza iniziale, effettuando un successivo test finale per verificare l'innalzamento della postura. Verrà anche pianificato analogamente un penetration test per la verifica delle configurazioni perimetrali di Agenzia, definendo un processo di continuous VA/PT ed attivando un sistema di vulnerability management Per innalzare la postura di sicurezza del networking il progetto prevede l'implementazione di un sistema NAC per il controllo dell'accesso fisico, che potrebbe comprendere anche un sistema ZTNA per il controllo esterno, l'implementazione di un sistema EDR/XDR per la protezione degli endpoint e dell'infrastruttura di rete, l'introduzione di un firewall perimetrale in ogni sede. Il progetto prevede inoltre nell'ottica di miglioramento dei processi e dell'organizzazione consulenza e hardening e reingegnerizzazione dei principali applicativi di Agenzia, siti web e applicativi infrastrutturali (es. protocollo, gestione del sistema di monitoraggio della qualità dell'aria, gestione delle attività, rendicontazione, gestione degli atti interni, etc.). Per rendere gli applicativi sicuri verrà anche progettato e implementato un sistema di CI/CD e una infrastruttura container dedicata protetta che permetta anche di verificare il controllo del codice applicativo prima del deploy. I siti e i principali applicativi verranno inoltre protetti da WAF appositamente progettati e implementati. Su tutti gli aspetti implementati nel progetto verrà formato il personale IT, in particolare sui nuovi processi e sulle tecnologie inserite.	

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 <i>Max 300 parole</i>
☐ energia ☐ trasporti ☐ banche ☐ mercati finanziari ☐ sanità ☐ fornitura e distribuzione di acqua potabile ☐ infrastrutture digitali ☐ motori di ricerca ☐ servizi cloud ☐ piattaforme di commercio elettronico	

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 <i>Max 300 parole</i>
☒ Identify ☒ Protect ☒ Detect ☒ Respond ☒ Recover	Il progetto impatterà positivamente su tutti i punti del framework Identify: sarà possibile avere una visione chiara del perimetro, degli asset aziendali e del relativo rischio, dell'attuale livello di sicurezza e quello desiderato. Saranno inoltre definiti i ruoli e le funzioni preposti alla messa in sicurezza dell'infrastruttura Protect: attraverso l'inserimento di nuove tecnologie, processi e formazione del personale sarà possibile avere un innalzamento del livello di protezione di tutto l'asset aziendale. Detect: attraverso l'inserimento di nuove tecnologie, processi e formazione del personale sarà possibile avere un innalzamento del livello di detection di eventuali malware e di attacchi cyber. Response attraverso l'inserimento di nuove tecnologie, processi e formazione del personale sarà possibile avere un innalzamento del livello di Response a un eventuale attacco informatico Recover: attraverso l'inserimento di nuove tecnologie, processi e formazione del personale sarà possibile avere un innalzamento del livello di Recover

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

Il progetto proposto persegue le seguenti finalità:

- *Realizzare un censimento dei livelli di maturità della postura di sicurezza dell'Agenzia sia a livello perimetrale, endpoint e interno, mediante consulenze e assessment delle criticità presenti.*
- *Implementazione di un piano programmatico di potenziamento delle capacità cyber a breve termine (con sistemi di protezione perimetrale, applicativa, networking, strutturale e di formazione) e a medio lungo termine (con riprogettazione e hardening dei sistemi utilizzati e delle procedure), per supportare il percorso di trasformazione digitale sicura dei servizi erogati dall'Agenzia e più in generale della PA.*

Con questo progetto l'Agenzia intende dotarsi di strumenti e processi per la gestione del rischio cyber in linea con le migliori pratiche nazionali e internazionali (processi, sistemi di protezione, servizi e procedure di intervento, aggiornamento dei sistemi e delle applicazioni, formazione degli utenti e degli specialisti coinvolti).

L'impatto sulle risoluzioni delle criticità dichiarate sui sistemi informativi permetterà:

- *Acquisire consapevolezza dell'asset da proteggere identificando i principali fattori di rischio e le possibili contromisure.*
- *Definire piani di intervento in caso di attacco cyber.*
- *Monitorare l'infrastruttura e implementare la resilienza del sistema informatico eliminando le principali cause di vulnerabilità.*
- *Aumentare la consapevolezza del rischio cyber e istruire l'utenza, anche specialistica, sulle best practice per contrastare le problematiche cyber e gestire le contromisure in caso di attacco.*

- *Dotarsi di strumenti aggiornati per l'intercettazione degli attacchi in tempi brevi che implementino anche contromisure rapide ed efficaci.*
- *Proteggere in modalità più efficace i dati e garantire tempistiche di ripristino dei servizi in caso di attacco cyber compatibili con il mandato istituzionale dell'Agenzia.*
- *Predisporre l'Agenzia alla compliance della direttiva Nis2.*

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

Glossario

Termini	Descrizione esemplificativa
<i>Identify (Identificazione)</i>	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.
<i>Protect (Protezione)</i>	Implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
<i>Detect (Rilevamento)</i>	Definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
<i>Respond (Risposta)</i>	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.
<i>Recover (Ripristino)</i>	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.



**Finanziato
dall'Unione europea**
NextGenerationEU



**DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE**

***PNRR Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity"
Allegato B2 "Quadro finanziario e cronoprogramma"***

Avviso	Avviso Pubblico n. 08/2024
Denominazione Avviso	Avviso Pubblico 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

Quadro finanziario

Tabella 1 - Dettaglio dei costi preventivati per le attività di progetto

Compilare la tabella sottostante con il dettaglio dei costi preventivati per le attività progettuali, indicando per ciascuna di esse intervento e tipologia di intervento (rif. Paragrafo 4.1 dell'Avviso), categoria di costo e importo contributo richiesto (netto e IVA - laddove applicabile)

Intervento [obbligatorio] Indicare l'intervento oggetto dell'attività, in coerenza con quanto selezionato nella Sezione 2.E "Interventi che si intende realizzare" dell'Allegato B1 (rif. paragrafo 4.1 "Progetti finanziabili e ammissibilità - Caratteristiche delle attività" dell'Avviso)	Tipologia di intervento [obbligatorio] Indicare la tipologia di intervento oggetto dell'attività, in coerenza con quanto selezionato nella Sezione 4.B "Indicazione e descrizione delle tipologie di intervento che si intende realizzare per ciascun intervento" dell'Allegato B1 (rif. paragrafo 4.1 "Progetti finanziabili e ammissibilità - Caratteristiche delle attività" dell'Avviso)	Attività [obbligatorio] Inserire breve descrizione	Categorie di costo [obbligatorio] Indicare ad esempio: acquisizione di beni, acquisizione di servizi, ecc.	Importo contributo richiesto (al netto di IVA) [obbligatorio]	Valore IVA [obbligatorio] 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 dovrà essere compilata per essere computata nella colonna "Importo contributo richiesto" esclusivamente al verificarsi di tale fattispecie	Importo contributo richiesto (IVA inclusa) [non compilare] Calcolato automaticamente come somma delle precedenti due colonne
1. Governance e programmazione cyber	B. Miglioramento dei processi e dell'organizzazione	Consulenza per definizione modello organizzativo, analisi iniziale della postura di sicurezza e per la definizione di un piano di di	acquisizione di servizi	30.000,00 €	6.600,00 €	36.600,00 €
1. Governance e programmazione cyber	C. Formazione e miglioramento della consapevolezza delle persone	Formazione per IT, programmazione corsi e campagne phishing per utente.	acquisizione di servizi	10.000,00 €	2.200,00 €	12.200,00 €
2. Gestione del rischio cyber e della continuità operativa	B. Miglioramento dei processi e dell'organizzazione	Consulenza specifica per definizione asset aziendale, valutazione del rischio e definizione metodologia valutazione e per definizione	acquisizione di servizi	40.000,00 €	8.800,00 €	48.800,00 €
2. Gestione del rischio cyber e della continuità operativa	C. Formazione e miglioramento della consapevolezza delle persone	Formazione specialistica IT su sistemi backup, DR e servizi cyber.	acquisizione di servizi	5.000,00 €	1.100,00 €	6.100,00 €
2. Gestione del rischio cyber e della continuità operativa	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Attivazione DR su servizio cloud S.C.I. con relative procedure e di un ulteriore backup offload su altro sito.	acquisizione di servizi	180.000,00 €	39.600,00 €	219.600,00 €
2. Gestione del rischio cyber e della continuità operativa	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Attivazione servizi cyber threat intelligence e security rating.	acquisizione di servizi	15.000,00 €	3.300,00 €	18.300,00 €
3. Gestione e risposta agli incidenti di sicurezza	A. Analisi della postura di sicurezza e definizione di un piano di potenziamento	Attività di red teaming per test postura di sicurezza e piano di miglioramento	acquisizione di servizi	15.000,00 €	3.300,00 €	18.300,00 €
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Consulenza per la predisposizione di procedure riguardanti la gestione e la risposta a incidenti cyber.	acquisizione di servizi	20.000,00 €	4.400,00 €	24.400,00 €
3. Gestione e risposta agli incidenti di sicurezza	C. Formazione e miglioramento della consapevolezza delle persone	Formazione IT su gestione e organizzazione per la risposta a incidenti di sicurezza	acquisizione di servizi	5.000,00 €	1.100,00 €	6.100,00 €
3. Gestione e risposta agli incidenti di sicurezza	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementazione di sistemi SIEM e SOAR e di un servizio SOC	acquisizione di servizi	150.000,00 €	33.000,00 €	183.000,00 €
4. Gestione delle identità digitali e degli accessi logici	A. Analisi della postura di sicurezza e definizione di un piano di potenziamento	Consulenza per hardening AD e attivazione dominio in cloud.	acquisizione di servizi	20.000,00 €	4.400,00 €	24.400,00 €
4. Gestione delle identità digitali e degli accessi logici	B. Miglioramento dei processi e dell'organizzazione	Consulenza per definizione politiche di accesso applicativo e sistemi.	acquisizione di servizi	10.000,00 €	2.200,00 €	12.200,00 €
4. Gestione delle identità digitali e degli accessi logici	C. Formazione e miglioramento della consapevolezza delle persone	Formazione IT su Active Directory e sistemi di autenticazione.	acquisizione di servizi	5.000,00 €	1.100,00 €	6.100,00 €
4. Gestione delle identità digitali e degli accessi logici	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Attivazione autenticazione MFA su applicativi, pdi e sistemi e di un sistema sistema IAM/PAM per accessi amministrativi a sistemi	acquisizione di servizi/acquisizione di beni	50.000,00 €	11.000,00 €	61.000,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	A. Analisi della postura di sicurezza e definizione di un piano di potenziamento	Consulenza per verifica configurazioni perimetrali con VA/PT.	acquisizione di servizi	20.000,00 €	4.400,00 €	24.400,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Implementazione di un sistema EDR/XDR per la protezione degli endpoint e dell'infrastruttura di rete.	acquisizione di servizi/acquisizione di beni	60.000,00 €	13.200,00 €	73.200,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Consulenza, hardening reingegnerizzazione dei siti web e delle principali applicazioni di ARPAT e implementazione di un sistema di CI/CD.	acquisizione di servizi/acquisizione di beni	300.000,00 €	66.000,00 €	366.000,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	C. Formazione e miglioramento della consapevolezza delle persone	Formazione del personale per gli aspetti di sicurezza e di rete.	acquisizione di servizi	10.000,00 €	2.200,00 €	12.200,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementazione di un sistema NAC per il controllo dell'accesso fisico, sistemi per il controllo dell'accesso remoto, firewall per sedi	acquisizione di servizi/acquisizione di beni	200.000,00 €	44.000,00 €	244.000,00 €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
					- €	- €
a) TOTALE COSTI DIRETTI (somma importo contributo richiesto (IVA inclusa)) [non compilare] Calcolato automaticamente						1.396.900,00 €
b) SPESE GENERALI MAX 7% DEI COSTI DIRETTI AMMISSIBILI (a*7%) [obbligatorio] Compilare con l'importo di spese generali (al massimo pari al 7% dei costi diretti) a copertura dei costi indiretti delle attività						97.783,00 €
c) TOTALE RICHIESTO A FINANZIAMENTO (a+b) [non compilare] Calcolato automaticamente - Importo da riportare nella Sezione 2, punto 2.C dell'Allegato B1 "Scheda Progetto"						1.494.683,00 €

Tabella 2 - Panoramica contributi richiesti per ciascun intervento, come contrassegnati nella sezione 2.E dell'Allegato B1 "Scheda Progetto"

La tabella sottostante - da non compilare - fornisce una vista di sintesi dei contributi richiesti per ciascun intervento indicato

Intervento [non compilare]	Importo contributo richiesto (al netto di IVA) [non compilare] Calcolato automaticamente	Valore IVA [non compilare] Calcolato automaticamente	Importo totale contributo richiesto (IVA inclusa) [non compilare] Calcolato automaticamente
1. Governance e programmazione cyber	40.000,00 €	8.800,00 €	48.800,00 €
2. Gestione del rischio cyber e della continuità operativa	240.000,00 €	52.800,00 €	292.800,00 €
3. Gestione e risposta agli incidenti di sicurezza	190.000,00 €	41.800,00 €	231.800,00 €
4. Gestione delle identità digitali e degli accessi logici	85.000,00 €	18.700,00 €	103.700,00 €
5. Sicurezza delle applicazioni, dei dati e delle reti	590.000,00 €	129.800,00 €	719.800,00 €
TOTALE COSTI DIRETTI		1.396.900,00 €	
SPESE GENERALI		97.783,00 €	
TOTALE RICHIESTO A FINANZIAMENTO		1.494.683,00 €	

Tabella 1 - Indicazione e descrizione del cronoprogramma delle attività del progetto
Compilare la tabella sottostante con l'elenco delle attività progettuali, indicando per ciascuna intervento, tipologia di intervento e i quarter pianificati di inizio e fine

Compilare con eventuali specifiche riguardo la pianificazione temporale, lasciare vuoto altrimenti

[illegible]