ARPAT
Agenzia regionale per la protezione ambientale della Toscana

Decreto del Direttore generale nr. 59 del 27/03/2025

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. Alessandro Gignoli*

Estensore: *Silvia Cappelli*

Oggetto: Adesione all'Accordo Quadro "Servizi di sviluppo, manutenzione adozione e condizione di un ecosistema di applicazioni Target RT della GR e degli Enti del territorio regionale" CIG 98968746C a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity M1C1I1.5" - CUP E19B24000020006

ALLEGATI N.: 1

Denominazione	*Pubblicazione*	*Tipo Supporto*
Allegato "1" - relazione di acquisto	sì	digitale

Natura dell'atto: *immediatamente eseguibile*

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

Il Direttore generale

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)";

Richiamato il decreto del Presidente della Giunta Regionale n. 74 del 23.03.2021, con il quale il sottoscritto è nominato Direttore generale dell'Agenzia Regionale per la Protezione Ambientale della Toscana;

Considerata la decorrenza dell'incarico di cui sopra dal 1° maggio 2021;

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;

Vista la "Richiesta di avvio di procedura di affidamento" di cui alla PG.SG.10 avente ad oggetto "Approvvigionamento e valutazione dei fornitori", agli atti, con la quale il Responsabile della Transizione digitale dott. Alessandro Gignoli ha chiesto di aderire all'Accordo Quadro avente ad oggetto l'affidamento dei "SERVIZI DI SVILUPPO, MANUTENZIONE ADOZIONE E CONDUZIONE DI UN ECOSISTEMA DI APPLICAZIONI TARGET RT DELLA GR E DEGLI ENTI DEL TERRITORIO REGIONALE" con il R.T.I composto da Engineering Ingegneria Informatica S.p.A. (mandataria), e TD Group Italia S.r.l., e GPI S.p.A. (mandanti) per l'acquisto del servizio di sviluppo e supporto dei moduli applicativi Atti + Abilitazioni e organigramma e del servizio di manutenzione ed evoluzione dei principali applicativi di Agenzia fra i quali Freedocs, Aserf e Avatar (all'intervento 5B "Sistema XDR/EDR, reingegnerizzazione siti web e applicazioni, implementazione di un sistema CI/CD), per un importo complessivo di adesione di euro 160.606,40 oltre IVA (Euro 200.819,81 IVA compresa);

Preso atto che, come meglio declinato nella relazione (allegato "1"), dello stesso Responsabile per la Transizione Digitale:

- 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" CUP, 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.

- 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;
  - che il termine ultimo per la conclusione delle attività di progetto è il 31.12.2025.

Tenuto presente che:

- Regione Toscana, in qualità di soggetto aggregatore, in data 21.05.2024 ai sensi dell'art. 54 del D.lgs 50/2016 ha stipulato l'Accordo Quadro avente ad oggetto l'affidamento del "SERVIZI DI SVILUPPO, MANUTENZIONE ADOZIONE E CONDUZIONE DI UN ECOSISTEMA DI APPLICAZIONI TARGET RT DELLA GR E DEGLI ENTI DEL TERRITORIO REGIONALE" CIG DELL'ACCORDO QUADRO 98968746C9 con il Raggruppamento Temporaneo di Imprese composto da Engineering Ingegneria Informatica S.p.A. (mandataria), e TD Group Italia S.r.l., e GPI S.p.A. (mandanti), con scadenza 21/05/2028;
- che il suddetto Accordo Quadro ricomprende i servizi di sviluppo, supporto e manutenzione ed evoluzione dei principali applicativi di cui ARPAT ha bisogno;

Dato atto che ARPAT per l'utilizzo dell'Accordo Quadro sopra citato deve seguire la seguente procedura:

- inviare il "Piano dei fabbisogni" al Fornitore. La trasmissione al Fornitore avviene tramite PEC;
- il Fornitore invia il "Progetto dei fabbisogni" all'Amministrazione interessata all'adesione;
- inoltrare la "MANIFESTAZIONE DI INTERESSE", sulla base del modello disponibile su START (Sistema Telematico Acquisti Regionale della Toscana), con allegato il "Progetto esecutivo" validato per richiedere l'autorizzazione all'adesione– Round 0-;
- a seguito della valutazione positiva della "MANIFESTAZIONE DI INTERESSE" da parte del Responsabile Unico del Procedimento dell'Accordo Quadro, inoltrare l'"ATTO DI ADESIONE" sulla base del modello disponibile nella documentazione su START – Round 1-;
- a seguito dell'approvazione dell'ATTO DI ADESIONE da parte del Responsabile Unico del Procedimento dell'Accordo Quadro, inviare al Fornitore il documento "Data Protection Agreement". La trasmissione al Fornitore avviene tramite PEC;
- il Fornitore dovrà sottoscrivere e rinviare tramite PEC "Data Protection Agreement";
- acquisire il CIG derivato con le modalità disponibili su START con la relativa scheda di sintesi;
- predisporre l'"ORDINATIVO DI FORNITURA" allegando la scheda di sintesi del CIG derivato e inoltrarlo al Fornitore e per conoscenza al Responsabile Unico del Procedimento dell'Accordo Quadro;

Preso, quindi, atto che:

- per l'adesione al contratto è necessario redigere il Data Protection Agreement;
- l'emissione l'ordinativo di fornitura perfeziona l'obbligazione tra Amministrazione contraente e appaltatore e in relazione a ciascun atto di adesione può essere emesso un solo contratto attuativo;

Tenuto presente che saranno finanziate 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 del citato Contratto Quadro che saranno concluse entro e non oltre il 31.12.2025;

Ritenuto di nominare:

- “Responsabile unico di progetto” Alessandro Gignoli Responsabile per la Transizione Digitale di ARPAT;
- “Direttrice dell’esecuzione del contratto” Monica Caponeri del Settore Affari Generali, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto,
- “Assistenti alla Direttrice dell’esecuzione del contratto” Silvia Cappelli assegnata alla Direzione Amministrativa,, Stefano Mignani, Marco Bazzani, Giacomo Giusti, Giacomo Zanobini assegnati al Settore SIRA, Marco Stefanelli assegnato al Settore CRTQA, Paola Pargoli assegnata al Settore Affari Generali;

Visto l’art. 45 del D.Lgs. n. 36/2023 (Incentivi alle funzioni tecniche) ed, in particolare, i commi 2 e 3 i quali stabiliscono quanto segue:

<<2. Le stazioni appaltanti e gli enti concedenti destinano risorse finanziarie per le funzioni tecniche svolte dal proprio personale specificate nell’allegato I.10 e per le finalità indicate al comma 5, a valere sugli stanziamenti di cui al comma 1, in misura non superiore al 2 per cento dell’importo dei lavori, dei servizi e delle forniture, posto a base delle procedure di affidamento. Il presente comma si applica anche agli appalti relativi a servizi o forniture nel caso in cui è nominato il direttore dell’esecuzione. È fatta salva, ai fini dell’esclusione dall’obbligo di destinazione delle risorse di cui al presente comma, la facoltà delle stazioni appaltanti e degli enti concedenti di prevedere una modalità diversa di retribuzione delle funzioni tecniche svolte dal proprio personale.
3. L’80 per cento delle risorse di cui al comma 2, è ripartito, per ogni opera, lavoro, servizio e fornitura, tra il RUP e i soggetti che svolgono le funzioni tecniche indicate al comma 2, nonché tra i loro collaboratori. Gli importi sono comprensivi anche degli oneri previdenziali e assistenziali a carico dell’amministrazione. I criteri del relativo riparto, nonché quelli di corrispondente riduzione delle risorse finanziarie connesse alla singola opera o lavoro, a fronte di eventuali incrementi ingiustificati dei tempi o dei costi previsti dal quadro economico del progetto esecutivo, sono stabiliti dalle stazioni appaltanti e dagli enti concedenti, secondo i rispettivi ordinamenti entro trenta giorni dalla data di entrata in vigore del codice>>;

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 di gestione di attrezzature informatiche per lo sviluppo di sistemi informatici CPV 72514200-3 – S;

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 3.292,13, 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;

Dato atto che il presente decreto è riconducibile alla seguente categoria della data protection: “affidamento di dati a soggetti esterni”, ai sensi dell'art 10 paragrafo 2 sottoparagrafi c.ii.c. di cui al decreto del Direttore generale n.186/2019;

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;

Visti i pareri espressi in calce dal Direttore amministrativo e dal Direttore tecnico;

decreta

1. di aderire, per le motivazioni precisate nella relazione del Responsabile per la Transizione Digitale (allegato “1”), presumibilmente a decorrere dal 01.05.2025 e fino al 31.12.2025, all'Accordo Quadro "Servizi di sviluppo, manutenzione adozione e condizione di un ecosistema di applicazioni Target RT della GR e degli Enti del territorio regionale" CIG 98968746C9, stipulato da Regione Toscana quale soggetto aggregatore con il Raggruppamento Temporaneo di Imprese composto da Engineering Ingegneria Informatica S.p.A. (mandataria), e TD Group Italia S.r.l., e GPI S.p.A. (mandanti), con scadenza 21/05/2028, come previsto nella procedura esposta nella parte narrativa;
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 atto che:
   - il costo dell’affidamento è di 160.606,40 oltre IVA (Euro 200.819,81 IVA compresa), e che tale importo sarà ricompreso alla voce “Acquisti di servizi” dell’anno 2025;
   - saranno finanziati 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 del citato Contratto Quadro che saranno concluse entro e non oltre il 31.12.2025;
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 3.292,13 con riserva di verificare successivamente l'effettiva spettanza e il quantum;
5. di dare atto che, a seguito dell’approvazione dell’atto di adesione parte del Responsabile Unico del Procedimento dell’Accordo Quadro, dovrà essere redatta la Data Protection Agreement (DPA) che dovrà essere firmata da titolare del trattamento dati ARPAT e inviata al fornitore per la relativa sottoscrizione;
6. di dare atto che le funzioni di “Responsabile Unico del progetto” saranno espletate dal

Responsabile per la Transizione Digitale di ARPAT, Dott. Alessandro Gignoli;

7. di nominare quale:
   - “Direttrice dell’esecuzione del contratto”, ai sensi dell’art. 114 (“Direzione dei lavori e dell’esecuzione dei contratti”) del D.Lgs. n. 36/2023, Monica Caponeri del Settore Affari Generali, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto;
   - “Assistenti alla Direttrice dell’esecuzione del contratto” Silvia Cappelli assegnata alla Direzione Amministrativa, Stefano Mignani, Marco Bazzani, Giacomo Giusti, Giacomo Zanobini assegnati al SIRA, Marco Stefanelli assegnato al CRTQA, Paola Pargoli assegnata al Settore Affari Generali;
8. di notificare il presente decreto all'Ufficio DPO per la conservazione nel dossier data protection, ai sensi del decreto del Direttore generale n. 186 del 31 dicembre 2019;
9. 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’Agezia per la Cybersicurezza Nazionale (ACN) individuato con CUP E19B24000020006.

Il Direttore generale
Dott. Pietro Rubellini*

* “Documento 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.”

Il Decreto è stato firmato elettronicamente da:

- Marta Bachechi , responsabile del settore Affari generali in data 26/03/2025
- Andrea Rossi , responsabile del settore Bilancio e Contabilità in data 26/03/2025
- Marco Chini , il proponente in data 26/03/2025
- Paola Querci , Direttore amministrativo in data 27/03/2025
- Marcello Mossa Verre , Direttore tecnico in data 27/03/2025
- Pietro Rubellini , Direttore generale in data 27/03/2025

ARPAT - DIREZIONE TECNICA - Settore Sistema Informativo Regionale Ambientale
Via Ponte alle Mosse, 211 - 50144 - Firenze

N. Prot: Vedi segnatura informatica cl.: del 27/02/2025

Relazione di acquisto

Oggetto: **Acquisto del servizio di sviluppo e supporto dei moduli applicativi Atti + Abilitazioni e organigramma e del servizio di manutenzione ed evoluzione dei principali applicativi di Agenzia fra i quali Freedocs, Aserf e Avatar.**

Premesso 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" descritta nell'allegato 1 alla presente relazione;
- l'obiettivo dell'investimento 1.5 "Cybersecurity" 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, 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 25.9.2024 (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, 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 "Sistema XDR/EDR, reingegnerizzazione siti web e applicazioni, implementazione di un sistema CI/CD" che prevede l'hardening e la reingegnerizzazione delle principali applicazioni di Agenzia, si rende necessario lo sviluppo e il conseguente supporto dei moduli applicativi Atti + Abilitazioni e organigramma, nonché la manutenzione ed evoluzione dei principali applicativi di Agenzia fra i quali Freedocs, Aserf e Avatar.

tel. 055.32061 - fax 055.3206324 - P.IVA 04686190481 - www.arpat.toscana.it - per informazioni: urp@arpat.toscana.it
per comunicazioni ufficiali PEC: arpat.protocollo@postacert.toscana.it - (accetta solo PEC),

- nell'allegato 1 alla presente sono elencati tutte le tipologie di intervento nonché la descrizione delle attività facenti parte del progetto approvato dall'Agenzia per la Cybersicurezza Nazionale (ACN) di cui ai precedenti paragrafi;
- in detto elenco è ricompresa l'intervento denominato "5B" che prevede l'implementazione di un sistema XDR/EDR, reingegnerizzazione siti web e applicazioni, implementazione di un sistema CI/CD tramite container e sistemi di controllo del codice applicativo, così come descritto nell'allegato 2 alla presente relazione;
- è attivo su START Negozio elettronico di Regione Toscana un Accordo Quadro "Servizi di sviluppo, manutenzione adozione e conduzione di un ecosistema di applicazioni Target RT della GR e degli Enti del territorio regionale CIG: 98968746C9" con scadenza il 21/5/2028;
- ARPAT ha avviato le procedure per l'adesione al sopra citato Accordo Quadro;

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

- approvvigionarsi, per l'importo complessivo di euro 164.606,40 oltre IVA, dei servizi di sviluppo e supporto dei moduli applicativi Atti + Abilitazioni e organigramma e del servizio di manutenzione ed evoluzione dei sistemi Freedocs, Aserf e Avatar, così come descritto nell'allegato 4 Piano dei fabbisogni;
- nominare quale Responsabile unico di progetto ai sensi dell'art.15 del D.lgs 36/2023 il dott. Alessandro Gignoli, Responsabile della transizione digitale
- nominare quale "Direttore dell'esecuzione del contratto", di cui all'art. 114 comma 7 del D.Lgs 36/2023, Monica Caponeri del Settore Affari generali, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto e come "Assistenti al Direttore dell'esecuzione del contratto" Silvia Cappelli, Stefano Mignani, Marco Bazzani, Giacomo Giusti, Marco Stefanelli, Giacomo Zanobini, Paola Pargoli.
- individuare il sottoscritto, Responsabile del Settore SIRA, quale responsabile del presente procedimento, ai sensi dell'art. 15 del D.lgs. 36/2023 e s.m.i.

Il Responsabile del progetto/RTD
Dott. Alessandro Gignoli

Il Responsabile del Settore SIRA
Dott. Marco Chini

Elenco allegati:

1. Scheda di progetto presentato ad ACN
2. Quadro finanziario
3. Cronoprogramma
4. Piano dei fabbisogni

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - P.IVA 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

AVVISO PUBBLICO n. 08/2024

per la presentazione di proposte di interventi di potenziamentxo 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 (*indicare Via/Piazza, n. civico e CAP)*	
Riferimenti di contatto	Mail: _a.gignoli@arpat.toscana.it_____ N. Telefono: __+39-348-3968453_____

Sezione 2 – ANAGRAFICA DEL PROGETTO PROPOSTO

2.A Codice Unico di Progetto (CUP) *Indicare il CUP e la tipologia*	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 *Indicare il costo complessivo del progetto proposto, inclusivo di eventuali ulteriori fonti finanziarie, come risultante dal CUP*	____Euro 1.494.683,00_____
2.C Importo contributo richiesto *Indicare l'importo del contributo richiesto a valere sul presente Avviso, come risultante dalla compilazione dell'**Allegato B2***	_____Euro 1.494.683,00_____
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*	☒ 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

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	☒ 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	Acquisto e implementazione licenze aggiornate (M365 E3) per piattaforma di collaboration, con	2023-2024	50.000

	collaboration a M365	**implementazione di intune anche su dispositivi mobili.**		
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**	**2024-2026**	**35.000**

			l'impatto sonoro in-dotto dalle sorgenti sonore portuali a beneficio delle popolazioni residenti in tali zone		
2	Progetto Salpiam - 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	2018-2021	38.000

			creazione di un approccio specifico per la corretta gestione del rumore.		
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 identiying 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 NOSTRUM Interreg Italia Marittimo Francia	Europeo	Il progetto promuove la riduzione delle emissioni inquinanti derivanti dalle attività portuali ed in particolare, dalle navi. L'obiettivo generale del progetto è contribuire a preservare o migliorare la qualità dell'aria nelle aree prospicenti 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	2020-2023	100.000
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	Europeo/Nazionale	Il progetto LIFE SEPOSSO ha l'obiettivo di implementare e diffondere	2023-2024	60.000

	ENVIRONMENTAL GOVERNANCE FOR THE POSIDONIA OCEANICA SUSTAINABLE TRANSPLANTI NG OPERATIONS - SEPOSSO”		**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.**		

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 *(da valorizzare solo se scelto)*	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 *(da valorizzare solo se scelto)*	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 ridondato, 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 e 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 incident e playbook standard per la gestione degli incidenti noti. Verrà erogata la relativa formazione IT sula 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** *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**	

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 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
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.

Accordo Quadro fra Regione Toscana - Soggetto Aggregatore e il Raggruppamento Temporaneo di Imprese composto da Engineering Ingegneria Informatica S.p.A. (mandataria), e TD Group Italia S.r.l., e GPI S.p.A. (mandanti) avente ad oggetto ˝Servizi di sviluppo, manutenzione adozione e conduzione di un ecosistema di applicazioni Target RT della GR e degli Enti del territorio regionale" CIG: 98968746C9

MAC (Servizio di manutenzione correttiva)
SVI (Sviluppo e manutenzione evolutiva)

Attività	Importo in Euro	Tipo di servizio	Tariffa SVI	Trasformazione in gg/uu SVI
Sviluppo modulo abilitazioni e organigramma	30.543,00	SVI	251,12	122
Modulo atti (Phylum, Linneo)	39.261,00			156
Manutenzione FreeDocs Avatar AseRF	37.668,00			150
Analisi progettazione nuova architettura	30.134,40			120
TOT.	**137.606,40**			

Supporti	Canone al mese	Numero mensilità	Totale mensilità	Tipo di servizio
Modulo atti	1.000,00	9	9.000,00	MAC - Classe C
Abilitazioni e organigramma	2.000,00	9	18.000,00	MAC - Classe B
TOT.			**27.000,00**	

Totale sviluppo e supporti	**164.606,40**

Attività	Importo	Tipo di servizio
Manutenzione evolutiva AVATAR, ASERF, FreeDocs		SVI

ARPAT - Piano di lavoro

Corrisponde a una settimana lavorativa

FASE	DETTAGLI	MESI							
		1	2	3	4	5	6	7	8
1	Sviluppo organigramma e sistema delle abilitazioni - Rilascio in ambiente di staging								
2	Sviluppo modulo atti - Rilascio in ambiente di staging								
3	Presa in carico degli applicativi e manutenzione								
4	Avvio delle attività piano di analisi per la progettazione e la reingegnerizzazione dei nuovi flussi di lavoro di ARPAT e dei relativi sistemi								

ARPAT - Agenzia regionale per la protezione ambientale della Toscana

Direzione Tecnica

Piano dei fabbisogni

Progetto *ARPAT-Interventi di potenziamento della resilienza cyber. Intervento 5B, sistema XDR/EDR, reingegnerizzazione siti web e applicazioni, implementazione di un sistema CI/CD*.

Proposta presentata da ARPAT ad 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 M1C1I1.5, CUP E19B24000020006.

Adesione all'Accordo Quadro per l'affidamento dei "Servizi di sviluppo, manutenzione adozione e conduzione di un ecosistema di applicazioni Target RT - Giunta Regionale e degli Enti del Territorio regionale" - CIG 98968746C9

tel. 055.32061 - fax 055.3206324 - p.iva 04686190481 - www.arpat.toscana.it - per informazioni: urp@arpat.toscana.it
per comunicazioni ufficiali PEC: arpat.protocollo@postacert.toscana.it - (accetta solo PEC),

Dati anagrafici Ente	
Ragione sociale Ente	ARPAT – Agenzia regionale per la protezione ambientale della Toscana
Indirizzo	Via del Ponte alle Mosse, 211
CAP	50144
Comune	Firenze
Provincia	FI
Regione	Toscana
Codice Fiscale	04686190481
PEC	arpat.protocollo@postacert.toscana.it
Codice IPA	arpat

Dati anagrafici RUP	
Nome	Alessandro
Cognome	Gignoli
CAP	50144
Struttura	Settore SIRA
Telefono	3483968453
Indirizzo email	a.gignoli@arpat.toscana.it

Dati anagrafici Referente	
Nome	Alessandro
Cognome	Gignoli
CAP	50144
Struttura	Settore SIRA
Telefono	3483968453
Indirizzo email	a.gignoli@arpat.toscana.it

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it -
urp@arpat.toscana.it

Introduzione

All'interno di ARPAT si è dato avvio a un'attenta analisi dell'attuale postura di sicurezza per rilevare eventuali criticità in un'ottica di compliance alle attuali norme vigenti, in particolare alla direttiva NIS2. Sempre in quest'ottica si sta cercando di dare avvio a una radicale trasformazione delle modalità di sviluppo delle applicazioni ad uso interno e non solo.

Tali nuovi modalità prevedono principalmente la netta divisione tra interfaccia grafica (di seguito anche UI: User Interface) e Logica Applicativa (di seguito anche BL: Business Logic).

Pertanto, al posto del tradizionale metodo di sviluppo "monolitico", l'Amministrazione si sta orientando verso implementazioni che prevedano da una parte delle UI in modalità SPA (Single Page Application), PWA (Progressive Web App) e/o Native Mobile e dall'altra la realizzazione di microservizi containerizzati.

All'interno del progetto, ARPAT-Interventi di potenziamento della resilienza cyber, finanziato da ACN a seguito di AVVISO PUBBLICO n. 08/2024 a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity M1C1I1.5, CUP E19B24000020006, è presente l'intervento 5B, "sistema XDR/EDR, reingegnerizzazione siti web e applicazioni, implementazione di un sistema CI/CD". In tale contesto verrà sviluppata l'architettura a microservizi e avviato l'hardening e la reingegnerizzazione dei principali applicativi di ARPAT.

L'utilizzo di un'architettura a microservizi non solo consente una maggiore flessibilità nello sviluppo e nel rilascio delle applicazioni, ma introduce anche significativi vantaggi dal punto di vista della sicurezza. In primo luogo, l'isolamento dei singoli servizi riduce la superficie d'attacco, limitando l'impatto di eventuali vulnerabilità. Inoltre, l'approccio modulare consente di applicare controlli di accesso e meccanismi di autenticazione personalizzati per ogni servizio, garantendo una protezione mirata e una migliore gestione dei dati.

Un altro aspetto rilevante è la possibilità di effettuare aggiornamenti e applicare patch di sicurezza in modo rapido e mirato, senza compromettere la disponibilità dell'intero sistema. Inoltre, ogni microservizio può essere sviluppato utilizzando un framework minimale che permette la riduzione al massimo della superficie d'attacco, migliorando così la resilienza complessiva.

.

Obiettivi

Mediante l'Accordo Quadro "Servizi di sviluppo, manutenzione adozione e conduzione di un ecosistema di applicazioni Target RT della GR e degli Enti del territorio regionale - CIG: 98968746C9", che costituisce la base per il presente Piano Dei Fabbisogni, gli obiettivi da raggiungere possono essere così sintetizzati:

- verifica e miglioramento della postura di sicurezza;
- reingegnerizzazione dei sistemi alle nuove tecnologie che permettono un maggiore controllo in tema di cyber security;
- maggiore integrazione tra i vari sistemi informativi.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it -
urp@arpat.toscana.it

Intervento richiesto

Gli interventi richiesti dal presente Piano Dei Fabbisogni riguardano:

- progettazione e sviluppo del nuovo sistema di gestione degli atti amministrativi di ARPAT, mediante lo sviluppo di un apposito modulo abilitazioni e organigramma e modulo atti;
- presa in carico, analisi, hardening e manutenzione dei principali software in uso presso ARPAT quali: AVATAR, ASERF, Freedocs, Status, Siwenna;
- Implementazione di API per l'interoperabilità fra i sistemi di ARPAT, in particolare Aserf e Freedocs, verso i sistemi di RT e di altri soggetti;
- stesura di un piano di analisi per la reingegnerizzazione dei sistemi di gestione dei flussi documentali e delle attività di ARPAT, in un'ottica di integrazione e di ottimizzazione della postura di sicurezza applicativa, definendo un progetto di evoluzione dei sistemi applicativi di ARPAT, legato alle modifiche infrastrutturali previste dall'intervento 5B del progetto ACN.

Macro pianificazione del servizio

I servizi fino ad ora descritti dovranno essere completati nell'arco temporale definito dal termine del progetto ACN dalla data di sottoscrizione del contratto e comunque non oltre il 31/12/2025

Service level Agreement e protezione dei dati

Per tutto quello che riguarda il rispetto degli SLA (Service Level Agreement), il modello di sviluppo, dispiegamento, privacy e compliance GDPR e tutto quello che non è stato esplicitamente trattato nel presente piano, si rimanda al capitolato tecnico relativo alla procedura di gara (Procedura aperta per l'affidamento dei "Servizi di sviluppo, manutenzione adozione e conduzione di un ecosistema di applicazioni Target RT - Giunta Regionale e degli Enti del Territorio regionale").

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it -
urp@arpat.toscana.it