ARPAT
Agenzia regionale per la protezione ambientale della Toscana

Decreto del Direttore amministrativo nr. 92 del 22/12/2025

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: Alessandro Gignoli

Estensore: Filippo Del Campana - Struttura stabile di supporto ai sensi dell'art. 15 del D.Lgs. n. 36/2023 - Settore Provveditorato

Oggetto: Affidamento alla Telecom Italia Spa dell'appalto per la fornitura di servizi di formazione relativi al potenziamento della postura di cybersicurezza a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity M1C1I1.5" - CUP E19B24000020006" CIG: B97F4A771C

ALLEGATI N.: 2

Denominazione	*Pubblicazione*	*Tipo Supporto*
Allegato 1 - Quadro tipologie di intervento	sì	digitale
Allegato 2 - proposta per bando ACN	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 10.6.2021, con il quale alla sottoscritta è stato attribuito, a decorrere dal 10.6.2021, 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 5.3.2024 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 5.8.2024), successivamente adeguato alla DGRT 968/24 con decreto del Direttore generale n. 167 del 5.9.2024;

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 4.1.2013, 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” (RAP) del 04.12.2025 (prot. 2025/101623), avente ad oggetto “Acquisto di servizi di formazione, a seguito dell’acquisizione di servizi per il potenziamento della postura di cybersicurezza di ARPAT”, agli atti, con la quale il Responsabile del Settore SIRA ha chiesto di approvvigionarsi, per l’importo complessivo di euro 28.551,00 oltre IVA, dei servizi presenti nel piano formativo proposto da Telecom Italia Spa che si integra con il piano dettagliato degli interventi dei servizi di potenziamento della postura di cybersicurezza acquisito dall'ente;

Preso atto che:

- come precisato nella relazione a firma del dirigente responsabile del Settore SIRA (allegato “1”), 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 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 31.03.2026;

Tenuto presente che:

- in data 23.06.2025, con decreto del Direttore generale n. 119 ARPAT ha aderito, per il potenziamento della postura di cybersicurezza dell'ente, 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 raggruppamento temporaneo con Wetech's spa società benefit a valere sul piano nazionale di ripresa e resilienza (PNRR), missione 1 – componente 1 – investimento 1.5 "cybersecurity m1c1i1.5" - CUP E19B24000020006";
- in data 03.09.2025, ns. protocollo n° 0071963 (agli atti), Telecom Italia Spa ha inviato il piano dettagliato degli interventi previsti per l'adesione descritta precedentemente;
- si rende necessario integrare i servizi di potenziamento della postura di cybersicurezza acquisisti tramite l'adesione di cui al decreto del Direttore generale n. 119/2025 con i servizi di formazione;
- si ritiene, come indicato nella relazione di acquisto allegata alla RAP del 04/12/2025, di approvvigionarsi dei servizi di formazione della postura di cybersicurezza, affidando il servizio alla ditta Telecom Italia S.p.a., a completamento e integrazione della fornitura di apparati infrastrutturali e networking per Regione Toscana;

Preso, altresì, atto che:

- nella "Richiesta di avvio di procedura di affidamento" (Allegato "1"), sono elencate 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;
- nell'allegato 3 alla "Richiesta di avvio di procedura di affidamento" (Allegato "2"), è presente la proposta di piano formativo integrativa inviata da Telecom Italia Spa;

Dato atto che:

- in data 27.11.2025 è stato pubblicato sulla piattaforma START (procedura n. 048632) l'affidamento diretto ai sensi dell'art. 50 comma 1 lett. b) del d.lgs. n. 36/2023 dell'"Appalto per la fornitura di servizi di formazione relativi al potenziamento della postura di cybersicurezza a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) - CUP E19B2400006", con il quale si è richiesto alla ditta Telecom Italia Spa di confermare il preventivo di spesa per i servizi di formazione ad integrazione dei servizi di potenziamento della postura di cybersicurezza acquisiti tramite l'adesione di cui al decreto del Direttore generale n. 119/2025;
- entro il 05.12.2025 data di scadenza per la presentazione del preventivo è pervenuta l'offerta della ditta Telecom Italia Spa;
- l'offerta economica presentata da Telecom Italia Spa è risultata essere di euro 28.551,00 oltre IVA e pertanto è ritenuta congrua e conforme a quanto richiesto;

Ritenuto di affidare, ai sensi dell'art. 50, comma 1, lett. b) del D.Lgs. n. 36/2023, alla società Telcom Italia Spa l'appalto di cui trattasi, per l'importo di € 28.551,00 oltre IVA, a seguito dell'esito positivo dei controlli, attivati presso la piattaforma ANAC (FVOE), sul possesso da parte della società affidataria dei requisiti di ordine generale e di ordine speciale;

Ritenuto inoltre:

- di individuare quale “Responsabile unico del progetto (RUP)” ai sensi dell’art. 15 del D.Lgs. n. 36/2023, il Dott. Alessandro Gignoli, in qualità di Responsabile della transizione digitale;
- di nominare quale “Direttore dell’esecuzione del contratto”, di cui all’art. 114 comma 7 del D. Lgs. 36/2023, Rita Gargani del Settore SIRA, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto, Silvia Giubbilini, Valentina Pestelli, Gloria Chiarini del Settore SIRA, come “Assistenti al Direttore dell’esecuzione del contratto” 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, come “Assistenti al Direttore dell’esecuzione del contratto”;

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. 26;

Dato atto che il presente decreto è riconducibile alla seguente categoria della data protection: “25 – Gestione delle risorse strumentali”, 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;

decreta

1. di disporre, per le motivazioni espresse in narrativa, l’affidamento diretto ai sensi dell’art. 50 comma 1 lett. b) del D.Lgs. n. 36/2023 a Telecom Italia Spa di Milano (partita IVA 00488410010) “Servizi di formazione della postura di cybersicurezza” previsti nel piano formativo allegato (All. “1”) (CIG B97F4A771C – CUP E19B24000020006), che si integra con il piano dettagliato degli interventi dei servizi di potenziamento della postura di cybersicurezza acquisito dall'ente, per un importo di € 28.551,00 oltre IVA (euro 34.832,22 IVA compresa);
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 € 28.551,00 oltre IVA (euro 34.832,22 IVA compresa) come indicati nella proposta di piano formativo integrativa (All. “2”) inviata da Telecom Italia Spa e che tale importo sarà ricompreso alla voce “Acquisti di servizi” del budget 2025/2026;

- il costo dell’affidamento sarà finanziato con le risorse erogate dall’Agenzia per la Cybersicurezza Nazionale (ACN) nell’ambito del progetto di cui trattasi;

4. di dare atto che le funzioni di “Responsabile Unico del progetto” saranno espletate dal Responsabile della transazione digitale, Dott. Alessandro Gignoli;

5. di nominare quale:
   - quale “Direttore dell’esecuzione del contratto”, di cui all’art. 114 comma 7 del D. Lgs. 36/2023, Rita Gargani del Settore SIRA, in ragione della competenza ed esperienza specifica nella materia oggetto di appalto,
   - quali “Assistenti al Direttore dell’esecuzione del contratto” Silvia Giubbilini, Valentina Pestelli, Gloria Chiarini del 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, come “Assistenti al Direttore dell’esecuzione del contratto”;

6. 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., così come stabilito nel decreto del Direttore generale n. 41/2017;

7. di dichiarare il presente decreto immediatamente eseguibile, al fine di consentire il conseguente inizio delle attività finalizzato a 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 smi, 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 19/12/2025
- Andrea Rossi , responsabile del settore Bilancio e Contabilità in data 19/12/2025
- Marco Chini , il proponente in data 19/12/2025
- Paola Querci , Direttore amministrativo in data 19/12/2025
- Pietro Rubellini , Direttore generale in data 19/12/2025

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 miglioramento	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 processi di backup e restore	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 SCT 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, pdl e sistemi e di un sistema sistema IAM/PAM per accesso amministrativo 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	siti web e delle principali applicazioni di ARPAT e implementazione di un sistema di CI/CD tramite container e sistemi di controllo del	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	controllo dell'accesso fisico, sistemi per il controllo dell'accesso remoto, firewall per sedi periferiche per controllo traffico e	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 €**

Cronoprogramma

Note

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

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

						Q1 2021	Q2 2021	Q3 2021	Q4 2021	Q1 2022	Q2 2022	Q3 2022	Q4 2022	Q1 2023	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024	Q3 2024	Q4 2024	Q1 2025	Q2 2025	Q3 2025	Q4 2025
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*	**Quarter di inizio pianificato [obbligatorio]** *Q1: 1 gennaio-31 marzo* *Q2: 1 aprile-30 giugno* *Q3: 1 luglio-30 settembre* *Q4: 1 ottobre-31 dicembre*	**Quarter di fine pianificato [obbligatorio]** *Q1: 1 gennaio-31 marzo* *Q2: 1 aprile-30 giugno* *Q3: 1 luglio-30 settembre* *Q4: 1 ottobre-31 dicembre* *N.B.: il quarter di fine deve essere uguale o successivo al quarter di inizio selezionato*	**Durata espressa in giorni [non compilare]** *Calcolata automaticamente*																				
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 miglioramento	Q4 2024	Q3 2025	364																				
1. Governance e programmazione cyber	C. Formazione e miglioramento della consapevolezza delle persone	Formazione per IT, programmazione corsi e campagne phishing per utente.	Q2 2025	Q4 2025	274																				
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 processi di backup e restore	Q4 2024	Q2 2025	272																				
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.	Q1 2025	Q2 2025	180																				
2. Gestione del rischio cyber e della continuità operativa	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Attivazione DR su servizio cloud SCT con relative procedure e di un ulteriore backup offload su altro sito	Q1 2025	Q3 2025	272																				
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.	Q4 2024	Q2 2025	272																				
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	Q2 2025	Q4 2025	274																				
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.	Q1 2025	Q3 2025	272																				
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	Q4 2024	Q3 2025	364																				
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	Q1 2025	Q4 2025	364																				
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.	Q2 2025	Q4 2025	274																				
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.	Q3 2025	Q4 2025	183																				
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.	Q1 2025	Q3 2025	272																				
4. Gestione delle identità digitali e degli accessi logici	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Attivazione autenticazione MFA su applicativi, pdl e sistemi e di un sistema sistema IAM/PAM per accesso amministrativo a sistemi	Q2 2025	Q4 2025	274																				
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.	Q3 2025	Q4 2025	183																				
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.	Q1 2025	Q4 2025	364																				
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	siti web e delle principali applicazioni di ARPAT e implementazione di un sistema di CI/CD tramite container e sistemi di controllo del	Q4 2024	Q4 2025	456																				
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.	Q1 2025	Q3 2025	272																				
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	controllo dell'accesso fisico, sistemi per il controllo dell'accesso remoto, firewall per sedi periferiche per controllo traffico e	Q4 2024	Q3 2025	364																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				
					#NOME?																				

Quarter	Data inizio	Data fine
Q1 2021	2021-01-01	2021-03-31
Q2 2021	2021-04-01	2021-06-30
Q3 2021	2021-07-01	2021-09-30
Q4 2021	2021-10-01	2021-12-31
Q1 2022	2022-01-01	2022-03-31
Q2 2022	2022-04-01	2022-06-30
Q3 2022	2022-07-01	2022-09-30
Q4 2022	2022-10-01	2022-12-31
Q1 2023	2023-01-01	2023-03-31
Q2 2023	2023-04-01	2023-06-30
Q3 2023	2023-07-01	2023-09-30
Q4 2023	2023-10-01	2023-12-31
Q1 2024	2024-01-01	2024-03-31
Q2 2024	2024-04-01	2024-06-30
Q3 2024	2024-07-01	2024-09-30
Q4 2024	2024-10-01	2024-12-31
Q1 2025	2025-01-01	2025-03-31
Q2 2025	2025-04-01	2025-06-30
Q3 2025	2025-07-01	2025-09-30
Q4 2025	2025-10-01	2025-12-31
Q1 2026	2026-01-01	2026-03-31
Q2 2026	2026-04-01	2026-06-30
Q3 2026	2026-07-01	2026-09-30
Q4 2026	2026-10-01	2026-12-31

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

Tipologia 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

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.*	**Proposta**	**Dettaglio attività**	**Prezzo Offerta Complementare IVA ESCLUSA**
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	L'ente si prefigge l'obiettivo incrementare la consapevolezza e formazione del proprio personale sulle tematiche di cybersecurity e data protection. Gli interventi e le iniziative trainanti verso il suddetto obbiettivo sono: • Definizione di piani di formazione sulla base di obiettivi e requisiti di apprendimento emersi dall'assessment della postura di sicurezza dell'Ente. • Erogazione di attività di formazione specifica, anche attraverso attività di simulazione di attacchi (es. campagne di phishing) per rendere il personale consapevole sui rischi e promuovere comportamenti sicuri.	Svolgimento di un corso di formazione con contenuti concordati con l'Agenzia, in particolare su tematiche di compliance a normative che riguardano l'area IT (data protection; IA Act - sistemi interni; NIS2) e di rischio cybersecurity. La formazione sarà erogata online con 2 incontri di 2 ore (tot. 4 ore). Tale formazione è arricchita da un approccio training on the job proponendo simulazioni phishing durante lo svolgimento dell'attività lavorativa in modo da promuovere comportamenti sicuri. Verranno eseguite campagne che saranno progettate per testare la prontezza e la consapevolezza dei dipendenti nel riconoscere e-mail sospette e tentativi di attività malevole.	4.748,00 €
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	Questo tipo di formazione è erogato a conclusione della documentazione interna alla popolazione dipendente coinvolta nei processi definiti all'interno del SGS (come Pentaqo)I e riguarda anche tematiche di vulnerabilità oggetto di VA; come le famiglie delle vulnerabilità e i rimedi per fare eventualmente un focus sui riport del VA interno (come Matic).	Formazione operativa sul SGSI : un incontro formativo di una durata di 2 ore Formazione sui VA : corso specialistico in aula di 4 ore per 2 sessioni ciascuno.	5.365,00 €
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	Sarà erogata formazione specifica in merito alle procedure redatte e relativie alla gestione, tracciamento e segnalazione degli incidenti di sicurezza e ai PlayBook Remediation, oltre che l'organizzazione di table top exercises.	Formazione specifica in base ai ruoli interni sulla gestione degli incidenti. Un incontro formativo di una durata di 2 ore	1.233,00 €
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	Erogazione di formazione verso utenti della piattaforma in SaaS Logiquo (sw che ha la funzione di gestire e monitorare tutti controlli relativi alla sicurezza delle informazioni e di normative cogenti valutandone sia lo stato di maturità sia il relativo rischio) nonchè alle metriche di valutazione dei sistemi di sicurezza	Incontri formativi verso utenti assegnatari di utenze logiquo per maturare la sensibilità verso le normative selezionate dall'agenzia per la propria postura di sicurezza e conformnità nonchè per il correttoutilizzo della piattaforma. Fornitura di licenze senza limiti di utenti della piattaforma GRC SaaS Logiquo comprensive dei Set di Controlli ISO27001, GDPR e 9001, set up organizzativo e avvio in produzione.	13.875,00 €
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	Formazione specialistica IT su sistemi backup, DR e servizi cyber. Formazione IT su Active Directory e sistemi di autenticazione. Formazione del personale per gli aspetti di sicurezza e di rete	2 mezze giornate di Formazione specialistica sulle tematiche : sistemi backup, DR e servizi cyber; Active Directory e sistemi di autenticazione, sicurezza di rete	3.330,00 €
						28.551,00 €