

CAPITOLATO SPECIALE

**25IST014_PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE M1C1
“DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA P.A.” – INVESTIMENTO 1.5
“CYBERSECURITY” - PROGETTO “MIGLIORAMENTO DELLA POSTURA DI SICUREZZA CYBER
NEL PERIMETRO AZIENDALE” FINANZIATO DALL’UNIONE EUROPEA -
“NEXTGENERATIONEU” – INTERVENTO “GOVERNANCE E PROGRAMMAZIONE CYBER” - CUP
E29B24000000006**

1.	Amministrazione Appaltante	3
2.	Premessa	3
3.	Normativa di riferimento	4
4.	Scopo	5
4.1	Definizioni e abbreviazioni	6
4.2	Acronimi	6
5.	Oggetto	6
5.1	Obiettivi e benefici da perseguire	7
5.2	Sedi di erogazione	8
5.3	Durata del contratto	8
6.	Descrizione della fornitura richiesta	8
6.1	Rispetto del principio DNSH	10
7.	Caratteristiche e quantità del personale richiesto	10
7.1	Gruppo di lavoro e Profili professionali richiesti	10
7.2	Orario di servizio	11
8.	Modalità di esecuzione	11
8.1	Contesto Economico–Finanziario e consuntivazione	12
8.2	Modalità di esecuzione dei servizi	13
8.3	Gestione della fornitura	13
8.4	Controllo	13
9.	Condizioni generali dell'affidatario	14

1. Amministrazione Appaltante

Azienda Regionale di Coordinamento per la Salute - ARCS

Sede legale: Via Pozzuolo, 330 – 33100 Udine

Codice fiscale e partita IVA: 02948180308

Codice IPA: arcs

Posta Elettronica Certificata (PEC): arcs@certsanita.fvg.it

Responsabile unico del progetto: dott. Nicola Bortolotti

L'Azienda Regionale di Coordinamento per la Salute (ARCS) è istituita dal 1° gennaio 2019 con Decreto del Presidente della Regione n. 0240/Pres. del 21 dicembre 2018 in attuazione alla Legge Regionale di riordino del Servizio Sanitario Regionale n. 27 del 17 dicembre 2018, quale ente dotato di personalità giuridica pubblica ed è disciplinata dalle vigenti disposizioni di legge concernenti le Aziende Unità Sanitarie Locali di cui al D.lgs. n. 502 del 30 dicembre 1992.

Le macro-attività garantite da ARCS sono:

- Coordinamento della programmazione delle aziende sanitarie e degli IRCCS e monitoraggio dei livelli di raggiungimento degli obiettivi e di consumo delle risorse assegnate
- Coordinamento delle reti cliniche, dei programmi di sicurezza delle cure, delle politiche relative a farmaci, dispositivi medici e protesica e delle attività connesse allo sviluppo e all'utilizzo delle professioni sanitarie
- Gestione delle attività amministrative, tecniche, logistiche e sanitarie centralizzate.
- Contributo tecnico alla Direzione centrale salute, politiche sociali e disabilità nella predisposizione di documenti di programmazione, nella stesura di accordi e nella partecipazione a tavoli tecnici regionali e/o nazionali.

In tale contesto, aumentare il know-how e la consapevolezza sui rischi inerenti alla propria organizzazione e ai propri servizi e infrastrutture informatiche riveste un'importanza centrale, così come programmare le azioni da attuare per mitigare i rischi e per contrastare eventi di cybercrime.

2. Premessa

L'Agenzia per la Cybersicurezza Nazionale (di seguito anche "Agenzia" o "ACN"), in qualità di Soggetto attuatore dell'Investimento 1.5 "Cybersecurity" – Missione 1, Componente 1, del PNRR, a titolarità della Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale (di seguito anche "DTD"), ha attuato una serie di interventi finanziati dall'UE mirati alla **realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione finalizzati ad irrobustire le infrastrutture e i servizi digitali del Sistema Paese nonché a migliorare le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza**, quale elemento fondante per la transizione digitale sicura della Pubblica Amministrazione.

Il presente Capitolato si riferisce in particolare all'intervento 1 del bando di finanziamento approvato da ACN, denominato "Governance e pianificazione cyber".

L'intero progetto dovrà concludersi inderogabilmente entro il 31 dicembre 2025, termine ultimo entro il quale dovranno essere completate tutte le attività, erogati i servizi richiesti, consegnati i deliverable oltre che pervenire le correlate fatture.

Nello specifico, la soluzione individuata da ARCS, intercetta la Misura 14 della Strategia Nazionale di Cybersicurezza, volta a coordinare interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini.

A seguito della valutazione con esito positivo da parte dell'Agenzia del progetto presentato da ARCS, si rende necessaria l'implementazione di una serie di interventi mirati, in accordo con le regole ed i principi trasversali individuati dal framework normativo di riferimento del PNRR, finalizzati al potenziamento della resilienza cyber dell'infrastruttura di ARCS.

Al fine di descrivere l'esecuzione del servizio, si sottolinea che, a prescindere dall'organizzazione adottata dal Fornitore per l'erogazione dei diversi servizi, è richiesto un alto grado di sinergia delle risorse messe a disposizione dal Fornitore e operanti presso le sedi di ARCS e da remoto in contatto con il personale individuato dall'Amministrazione, al fine di garantire un adeguato grado di omogeneità nelle varie soluzioni adottate e uniformità di comportamento nei confronti degli utenti. L'erogazione dei servizi deve comunque prevedere un alto grado di responsabilizzazione delle risorse del Fornitore, attitudine a lavorare per obiettivi, capacità di operare in team e rispetto delle scadenze pianificate.

3. Normativa di riferimento

- il decreto legislativo 18 maggio 2018, n. 65, "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione";
- il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, "relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»);
- il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica";
- il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n.131, recante "Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133";
- il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", che prevede l'istituzione dell'Agenzia a tutela degli interessi

- nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;
- il Regolamento (UE) 2016/679 (cd. GDPR) così come il D.lgs. 101/18 relativo alle Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679;
 - la Strategia Nazionale di Cybersicurezza 2022-2026, adottata unitamente al relativo Piano di Implementazione (di seguito anche "Piano"), con decreto del Presidente del Consiglio dei ministri del 17 maggio 2022;
 - l'Accordo stipulato, in data 14 dicembre 2021, tra l'Agenzia e il Dipartimento per la trasformazione digitale, ai sensi dell'articolo 5, comma 6, del d.lgs. n. 50/2016, di cui al prot. ACN n. 896 del 15 dicembre 2021, disciplinante lo svolgimento in collaborazione delle attività di realizzazione dell'"Investimento 1.5", registrato dalla Corte dei Conti il 18 gennaio 2022 al n. 95, e modificato dall'atto aggiuntivo del 14 luglio 2023, registrato dalla Corte dei Conti il 5 settembre 2023 al n. 2425;
 - il Sistema di Gestione e Controllo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri che illustra la struttura organizzativa, gli strumenti operativi e le procedure definite per la gestione, il monitoraggio, la rendicontazione e il controllo degli interventi previsti nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) di competenza del DTD, tra cui l'investimento 1.5 "Cybersecurity";
 - le Linee guida per i Soggetti Attuatori versione 3 del 6 marzo 2023, adottate dall'Unità di Missione PNRR del Dipartimento per la trasformazione digitale, Amministrazione Centrale titolare per l'investimento 1.5;
 - la circolare AgID del 18 aprile, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015)";
 - il decreto legislativo 4 settembre 2024, n.138 "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148";
 - la Legge 28 giugno 2024, n.90 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";
 - le "Linee guida per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90" del 20 novembre 2024
 - le "Linee Guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio" del 26 novembre 2024

4. **Scopo**

Il presente Capitolato descrive gli aspetti tecnici relativi alla fornitura di servizi consulenziali specialistici finalizzati alla realizzazione di un intervento di potenziamento dei processi di governance della cyber security e dei modelli organizzativi dell'Ente relativi alle compliance a regolamenti, leggi e standard di settore (es: NIS/NIS2, GDPR).

Tutte le prescrizioni contenute nel presente Capitolato rappresentano requisiti minimi del servizio se non specificatamente indicati.

4.1 Definizioni e abbreviazioni

Salva diversa esplicita indicazione, ai termini seguenti viene attribuito, ai fini del presente documento, il significato successivamente indicato:

- **Capitolato speciale:** indica il presente documento;
- **Committente:** Agenzia Regionale di Coordinamento per la Salute – ARCS;
- **Data di Attivazione:** primo giorno lavorativo utile, successivo alla data di approvazione del Piano di Lavoro, da parte della Amministrazione;
- **Fornitura:** indica, nel suo complesso, l'erogazione dei servizi oggetto del presente Capitolato speciale;
- **Fornitore:** indica l'aggiudicatario della Fornitura;
- **Piano di Lavoro:** indica il documento di pianificazione dei Servizi Continuativi;
- **Resoconto Attività:** indica il documento di consuntivazione dei servizi oggetto della Fornitura.

4.2 Acronimi

- **SAL:** stato avanzamento lavori
- **GDPR:** Regolamento UE 2016 679
- **DNSH:** principio del "Do No Significant Harm" previsto per i soggetti attuatori degli investimenti a titolarità del Dipartimento per la Trasformazione Digitale

5. Oggetto

Il presente bando ha come obiettivo l'acquisto di servizi consulenziali specialistici in ambito cybersecurity e sistemi di governance, finalizzati al miglioramento dei processi dell'Ente in relazione alle nuove e più evolute esigenze di compliance, necessarie per garantire la riservatezza e l'integrità dei dati trattati, punto cardine del continuo processo di digitalizzazione dei servizi dell'ecosistema dell'Ente.

Allo scopo di innovare i servizi ed incrementare la produttività dell'Amministrazione, la Sicurezza delle informazioni e la Privacy rappresentano gli elementi di base abilitanti che consentono di raggiungere tale obiettivo con le dovute garanzie. In quest'ottica, l'eccellenza è il risultato che può essere raggiunto:

- migliorando quanto già in essere;
- innovando al fine di erogare e offrire nuovi servizi sicuri;
- attuando un adeguato processo di monitoraggio, misurazione e comunicazione della sicurezza delle informazioni.

Questo modello richiede e prevede l'adozione di un approccio di miglioramento continuo che consenta di rispondere alle mutate esigenze di contesto (normativo in primis), garantendo al contempo la continuità di quanto avviato.

Occorre quindi che sia adottato un approccio «Business & Risk Based» che coniughi le attuali esigenze di business con specifiche logiche di rischio derivanti da:

- Nuove e più evolute esigenze dovute all'evoluzione del contesto;
- Minacce alla continuità operativa;

- Mutevoli Minacce esterne (es. rischi connaturati alla digitalizzazione, attacchi sempre più sofisticati);
- Vincoli esterni (es. Regolamento Privacy Europeo («GDPR»), misure sicurezza AGID, Direttiva NIS, Direttive ENISA, ecc.).

In tale contesto ARCS si propone di attuare alcuni interventi di base finalizzati all'incremento complessivo e progressivo del livello di sicurezza e a contrastare il costante aumento delle minacce informatiche, anche in considerazione di cyber-attacchi ed accadimenti critici e dei relativi risvolti negativi sulle PA italiane.

Per l'erogazione dei servizi oggetto del presente Capitolato speciale, il Fornitore dovrà definire le seguenti figure professionali che potranno essere ricondotte anche alla stessa persona:

1. **Responsabile del contratto**, il quale ha la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del contratto (es. fatturazione, verifica del rispetto dei livelli di servizio, definizione e aggiornamento del team di cui al paragrafo 7.1); nonché la richiesta di attivazione di nuovi Servizi, tra quelli definiti;
2. **Responsabile tecnico** per l'erogazione dei servizi, avente la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente Capitolato speciale e di essere il punto di riferimento tecnico per la gestione dei Servizi, tra quelli definiti. Il Responsabile tecnico dovrà inoltre coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL di progetto;

Il Responsabile tecnico del servizio, durante i SAL bimestrali, dovrà presentare ad ARCS il "Resoconto Attività", contenente lo stato delle fasi in lavorazione. Tali informazioni e dati saranno successivamente vagliati dalla Committente in sede di verifica di conformità.

Il Fornitore, al momento della stipula, dovrà comunicare ad ARCS i nominativi -comprensivi di relativi ruoli/responsabilità- il numero di recapito telefonico, l'indirizzo e-mail attraverso i quali contattare le suddette figure professionali oltre ad eventuali ulteriori soggetti preposti alla conduzione del progetto.

Per le attività svolte dalle figure di cui sopra non sarà riconosciuto nessun corrispettivo economico, ritenendosi gli stessi ricompresi nell'offerta economica presentata.

5.1 Obiettivi e benefici da perseguire

Il Progetto, composto da una serie di iniziative di cybersecurity di cui questo bando fa parte, mira ad eseguire una valutazione del livello di maturità del sistema di gestione della sicurezza e della conformità normativa dell'Ente (GDPR, NIS/NIS2) al fine di identificare le relative azioni necessarie per il rafforzamento della governance sulla cybersecurity e la capacità di difesa cyber.

Il progetto è finalizzato, quindi, alla realizzazione di interventi di potenziamento della resilienza cyber di ARCS attraverso la realizzazione di un percorso virtuoso di gestione del rischio cyber concernente:

- la realizzazione di un assesment approfondito sulla conformità normativa e sugli standard di settori ai quali l'Ente deve aderire per poter erogare ed innovare i suoi servizi offerti alle PA;

- la realizzazione di un piano programmatico di potenziamento, adeguamento e miglioramento, sia a breve che a medio-lungo termine, delle conformità normative e nuovi standard volta a supportare il percorso di trasformazione digitale sicura della PA;

Per il conseguimento degli obiettivi che ARCS vuole raggiungere è richiesta l'attuazione delle seguenti principali azioni/macro attività che sono oggetto del presente bando, ovvero:

- A. Analisi della postura di compliance dell'Ente
- B. Supporto all'adeguamento dell'Ente alla nuova postura individuata
- C. Formazione e miglioramento della consapevolezza delle persone

5.2 Sedi di erogazione

Le prestazioni oggetto del presente Capitolato dovranno essere erogate, a seconda delle esigenze specifiche di progetto, presso:

- la sede centrale di Udine;
- il magazzino centralizzato di Pordenone;
- la Sala Operativa Regionale Emergenza Sanitaria (SORES) a Palmanova;
- altre sedi che verranno eventualmente indicate in fase di esecuzione;
- la sede del Fornitore.

5.3 Durata del contratto

L'affidamento avrà decorrenza dalla data di stipula della Trattativa Diretta sul portale MEPA e la scadenza massima del contratto è fissata al 31.12.2025.

Il contratto dovrà pertanto concludersi inderogabilmente entro il 31.12.2025, termine ultimo entro il quale la soluzione dovrà essere collaudata e dovranno pervenire tutte le correlate fatture.

6. Descrizione della fornitura richiesta

Di seguito si illustrano i servizi richiesti.

Macro-attività	Attività	Deliverable
Analisi della postura di sicurezza e definizione di un piano di potenziamento	Analisi della postura di cyber security, anche a fronte delle azioni di rimedio già previste e in fase di attuazione e degli aggiornamenti normativi e prevedendo l'utilizzo del modello MOA-06 adottato dall'Agenzia e con il Framework Nazionale per la Cybersecurity e la Data Protection	1. Analisi della postura di cybersecurity <ul style="list-style-type: none"> • Report di valutazione della postura di cybersecurity (MOA-06): Documento che dettaglia il livello attuale di maturità della sicurezza informatica dell'azienda, con evidenza delle lacune rispetto ai requisiti normativi e dello stato di attuazione delle azioni di rimedio già previste. (Deliverables: N°1 MOA-06) • Matrice di conformità normativa: Tabella che mappa la conformità ai requisiti delle normative applicabili (es. Direttiva NIS2, Framework Nazionale per la Cybersecurity).-(Deliverables: N°2 Matrice di conformità normativa)

Macro-attività	Attività	Deliverable
		<ul style="list-style-type: none"> • Piano di miglioramento della postura di sicurezza: documento di piano strategico a breve, medio e lungo termine che espone un elenco strutturato e prioritizzato delle azioni di miglioramento, comprensivo di milestone e tempistiche. (Deliverables: N°3 Piano strategico)
Miglioramento dei processi e dell'organizzazione	<p>Revisione del framework documentale in materia di cybersecurity nell'ottica di coerenza con la normativa vigente</p> <p>Supporto nell'implementazione delle misure di sicurezza o deliverables documentali previsti dalla normativa vigente</p>	<p>2. Revisione del framework documentale</p> <ul style="list-style-type: none"> • Documenti di policy aggiornati: Set di policy e procedure in materia di cybersecurity, aggiornati in base agli ultimi standard e alle normative. (Deliverables: N°4 Procedura di gestione degli accessi, N°5 Procedura di gestione degli incidenti, N°6 Procedura di gestione del rischio cyber, N°7 Procedura di gestione dei log, N°8 Politica per la cyber sicurezza, N°9 policy VPN, N°10 policy Vulnerability Management, N°11 policy IT Standard) • Matrice di tracciabilità normativa: Documento che mostra come ciascun elemento del framework documentale aziendale soddisfa i requisiti normativi e le linee guida del MOA-06. (Deliverables: N°12 Matrice di tracciabilità normativa) <p>3. Supporto all'implementazione delle misure di sicurezza</p> <ul style="list-style-type: none"> • Piano operativo per l'implementazione delle misure di sicurezza: Documenti che descrivono le attività, i responsabili, le risorse necessarie e i tempi per l'implementazione delle misure di sicurezza tecniche e organizzative. (Deliverables: N°13 Piano operativo implementazione misure di sicurezza) • Supporto nella predisposizione di richieste e comunicazioni verso gli stakeholder regionali di rilevanza (ad es. Direzione Centrale Salute, Politiche Sociali e Disabilità, società in House della Regione FVG Insiel SpA) necessarie alla raccolta delle informazioni da integrare ai deliverable previsti • Supporto nella predisposizione dei provvedimenti interni (istruttorie e proposte di decreti e determine) indispensabili all'approvazione e all'adozione delle politiche e delle procedure in materia di cybersecurity. • Rapporti di avanzamento: Report periodici che monitorano lo stato di avanzamento nell'implementazione delle misure e deliverable previsti. (Deliverables: N°14 SAL) <p>Deliverable trasversali</p> <ul style="list-style-type: none"> • Dashboard di monitoraggio: Strumento visivo e interattivo per tenere traccia delle principali metriche di sicurezza, dello stato di conformità normativa e delle azioni di miglioramento in corso. (Deliverables: N°15 Dashboard di monitoraggio) • Executive Summary per il management: Documento sintetico per presentare ai vertici aziendali lo stato

Macro-attività	Attività	Deliverable
		della cybersecurity e le principali raccomandazioni operative comprensivo di previsioni economiche per l'attuazione. (Deliverables: N°16 Executive Summary)
Formazione e miglioramento della consapevolezza delle persone	Supporto alla conduzione delle attività previste dalla normativa vigente tramite apposita formazione rivolta agli esperti IT dell'Azienda	4. Supporto alla conduzione delle attività previste dalla normativa <ul style="list-style-type: none"> Materiali di formazione: Slide, esercitazioni e test di verifica per la formazione degli esperti IT dell'azienda su normative, framework e strumenti di cybersecurity. (Deliverables: N°17 Pacchetto Slide, N°18 Test di verifica) Registro delle attività formative: Documento che attesta i corsi svolti, con evidenza dei partecipanti, dei contenuti trattati e degli obiettivi formativi raggiunti. (Deliverables: N°19 Registro) Linee guida operative: Documenti pratici che forniscono istruzioni per la gestione quotidiana delle attività in conformità normativa. (Deliverables: N°20 linee guida operative)

6.1 Rispetto del principio DNSH

L'intervento oggetto del presente affidamento deve rispettare il principio del "Do No Significant Harm" (DNSH) previsto per i soggetti attuatori degli investimenti a titolarità del Dipartimento per la Trasformazione Digitale; la soluzione proposta non deve arrecare danni significativi agli obiettivi ambientali, inclusi mitigazione e adattamento ai cambiamenti climatici, uso sostenibile delle risorse idriche e marine, economia circolare, prevenzione dell'inquinamento e tutela della biodiversità. Tuttavia per le loro peculiarità, non contemplando alcun tipo di servizio hosting e/o cloud, trattandosi di servizio di implementazione documentale, di reportistica e di formazione, le attività previste non rientrano tra quelle elencate nelle schede 3,6,8 allegate alla circolare n.33 della Ragioneria Generale dello Stato del 13 ottobre 2022.

7. Caratteristiche e quantità del personale richiesto

Di seguito si elencano le caratteristiche e le certificazioni richieste che dovrà possedere il personale per l'erogazione dei servizi professionali indicati nel paragrafo 5 ai punti 1, 2 e **Errore. L'origine r** **iferimento non è stata trovata.** richiesti da ARCS ed una loro quantificazione in termini di gg/uomo.

7.1 Gruppo di lavoro e Profili professionali richiesti

Il Fornitore, per formare il team che si occuperà delle attività previste, dovrà avvalersi di personale specializzato nelle varie aree d'intervento descritte ai paragrafi precedenti e in possesso di competenze specifiche nonché di certificazioni funzionali al ruolo di riferimento.

Le risorse che verranno proposte dal Fornitore dovranno avere diversi profili ciascuno con una propria certificazione, a seconda del ruolo assunto nel progetto, tra:

- certificazione ITIL Foundation;
- certificazione di Lead Auditor ISO 27001 (profilo: tecnico per la gestione della sicurezza);
- certificazione CISA (Certified Information System Auditor);

Le qualifiche richieste devono essere rilasciate da un ente certificatore o da un'impresa di formazione accreditata.

Le risorse in possesso delle certificazioni specificate dovranno essere rese disponibili per l'intera durata del contratto e dovranno essere impiegate nei team di lavoro che garantiscono l'erogazione dei servizi oggetto della fornitura.

Il Fornitore sarà tenuto a garantire la disponibilità effettiva degli specialisti componenti il team di lavoro, rispettando la richiesta delle certificazioni sopra descritte, fatta salva la possibilità per ARCS di richiedere la sostituzione delle risorse ritenute non idonee ai compiti assegnati, a suo insindacabile giudizio.

7.2 Orario di servizio

I servizi professionali devono essere erogati nei giorni feriali dal lunedì al venerdì, indicativamente tra le 09.00 e le 18.00, fatte salve eventuali eccezioni concordate in anticipo con il Fornitore per permettere lo svolgimento degli stessi anche in fasce orarie/giorni differenti.

8. Modalità di esecuzione

Si evidenzia che l'intervento oggetto del presente affidamento è finanziato con Determina dell'Agenzia per la Cybersicurezza Nazionale prot. n. 30550 del 23.09.2024 così come rettificata da Determina prot. n. 33707 del 17.10.2024, che impone il rispetto dei target e delle tempistiche previsti per l'investimento di competenza, pena la revoca del finanziamento.

Il Fornitore è edotto, fin dalla fase di affidamento, dei termini imposti, della loro improrogabilità e pertanto, sin dalla presentazione del preventivo, è consapevole che i suoi eventuali ritardi possono cagionare un grave danno per il Committente che quindi oltre all'applicazione della penale potrà essere chiamato, per quanto di propria responsabilità, a rispondere dell'eventuale danno.

Al fine di descrivere l'esecuzione della Fornitura, si sottolinea che, a prescindere dall'organizzazione adottata dal Fornitore per l'erogazione dei diversi servizi, è richiesto un alto grado di sinergia delle risorse messe a disposizione dal Fornitore e operanti presso le sedi di ARCS in contatto con il personale individuato dall'Amministrazione, al fine di garantire un adeguato grado di omogeneità nelle varie soluzioni adottate e uniformità di comportamento nei confronti degli utenti.

L'erogazione dei servizi deve comunque prevedere un alto grado di responsabilizzazione delle risorse del Fornitore, attitudine a lavorare per obiettivi, capacità di operare in team e rispetto delle scadenze pianificate.

8.1 Contesto Economico-Finanziario e consuntivazione

La consuntivazione delle attività è predisposta periodicamente, su base bimestrale, attraverso una documentazione di rendicontazione, sia in termini di volumi sia di andamento dei servizi e delle attività. Le eventuali osservazioni dell'Amministrazione sui contenuti di tali documenti saranno effettuate in forma scritta, attraverso e-mail nonché attraverso lettere di rilievo, fermo restando che le informazioni e i dati di cui al Resoconto Attività saranno successivamente vagliati dalla Committente in sede di verifica di conformità.

Le fatture elettroniche emesse dovranno obbligatoriamente riportare i seguenti riferimenti:

- CIG (Codice Identificativo Gara): (trasMESSO successivamente)
- CUP (Codice Unico di Progetto): E29B24000000006
- ID Progetto: 43_WP9_A8_Azienda Regionale di Coordinamento per la Salute – ARCS
- Titolo del progetto: Miglioramento della postura di sicurezza cyber nel perimetro aziendale – investimento 1.5 "cybersecurity", intervento "Governance e Programmazione Cyber"

La fattura deve essere emessa in forma elettronica e, ove applicabile, deve essere emessa secondo le modalità di attuazione dell'art. 1, co. 629 della L. 190/2014, in materia di scissione dei pagamenti ai fini dell'IVA.

Il pagamento delle fatture avverrà ai sensi del D.Lgs. n. 231/2002 e s.m.i., con decorrenza dalla data di consegna in SDI della fattura elettronica (DM 55/2013).

Il pagamento avverrà previa verifica di conformità della fornitura, di presenza di DURC regolare e di regolarità rispetto alla posizione di adempienza presso l'Agenzia delle Entrate - Riscossione.

Nell'ipotesi di DURC irregolare i termini di pagamento sono sospesi fino alla regolarizzazione della posizione con l'emissione di un DURC positivo o con il pagamento sostitutivo disposto dall'ente previdenziale/assicurativo creditore.

Nell'ipotesi di irregolarità segnalata dall'Agenzia delle Entrate il pagamento viene sospeso fino alla definizione della posizione da parte dell'Agenzia delle Entrate competente.

I Fornitori non potranno eccepire eventuali arrotondamenti effettuati in fase di liquidazione delle fatture da ARCS con l'utilizzo dei gestionali in uso dalla P.A., nel limite di € 3,00.

Nel caso la richiesta di nota di accredito circostanziata, formulata da ARCS, non venga evasa entro 90 gg ARCS si riserva la possibilità di "compensazione finanziaria" dell'importo dovuto come nota di credito sul primo pagamento utile nei confronti del fornitore inadempiente. Di tale compensazione finanziaria sarà data formale comunicazione al fornitore.

Il pagamento si intende effettuato alla data di emissione dell'ordinativo di pagamento. Per "emissione dell'ordinativo di pagamento" si intende l'invio con esito positivo dell'ordinativo di pagamento al sistema informatico Siope+.

In merito alle modalità di fatturazione, conformemente a quanto richiesto dalle "LINEE GUIDA PER I SOGGETTI ATTUATORI INDIVIDUATI TRAMITE AVVISI PUBBLICI - Manuale Operativo" si allega un format recante specifiche istruzioni operative per la fatturazione dei fornitori (**Allegato MOA-13**).

Al fine della rendicontazione e dell'accesso all'erogazione del finanziamento PNRR i termini entro i quali le attività devono essere completate sono improrogabili e perentori.

8.2 Modalità di esecuzione dei servizi

I servizi richiesti dovranno essere definiti, concordati e attivati a partire dalla Data di Attivazione che corrisponde alla data della riunione di Kick Off del progetto e sempre a fronte di una pianificazione approvata da parte dell'Amministrazione che verrà trasmessa al Responsabile del Contratto del Fornitore, attraverso un incontro programmatico in cui verranno definite le seguenti informazioni di riferimento per ogni attività e relativo piano di lavoro:

- data prevista di inizio attività;
- data prevista di fine attività;
- eventuali date vincolo (ad esempio legate a date di esercizio);
- tipologia di servizio richiesto;
- obiettivi e ambito di intervento;
- eventuali riferimenti a documentazione esistente;
- risultati attesi;
- modalità operativa di intervento (on-site, entità interne ed esterne da coinvolgere e modalità di interazione con le stesse, frequenza di aggiornamento dei SAL, ecc.);
- milestone dell'intervento e tempistiche richieste per il rilascio dei vari piani di lavoro,
- personale e figure professionali del Committente e del Fornitore coinvolte.

8.3 Gestione della fornitura

L'esecuzione ed il governo della Fornitura dovranno avvenire con un'attività continua di pianificazione, consuntivazione e controllo. All'inizio della Fornitura, ARCS illustrerà le attività da svolgere, indicando le informazioni e le scadenze note, i piani di evoluzione e ogni altra informazione utile ad una corretta pianificazione (per le attività cui la pianificazione sia applicabile).

In ogni caso sarà cura del Fornitore predisporre e aggiornare tempestivamente le proprie attività, in funzione delle variazioni intervenute, in modo da riflettere il reale stato delle attività, a preventivo e a consuntivo.

La Committente si riserva di accedere in ogni momento a tali pianificazioni o a richiederne opportuna documentazione, al fine di condividere in tempo reale con il Fornitore lo stato delle attività della Fornitura.

A tal proposito, il Fornitore dovrà mantenere aggiornato bimestralmente lo stato di avanzamento dei lavori (SAL), fornendo tempestivamente indicazioni sulle attività concluse ed in corso, esplicitandone la percentuale di avanzamento, su eventuali criticità/ritardi, su azioni di recupero e razionali dello scostamento.

8.4 Controllo

È richiesto che il Fornitore operi il controllo costante e diretto delle condizioni e dei processi di erogazione dei servizi, supportando l'Amministrazione nel governo e nell'evoluzione dei servizi stessi. Il Fornitore, inoltre, deve fornire all'Amministrazione gli elementi per il costante miglioramento dei servizi nonché comunicare tempestivamente eventuali elementi di criticità e/o situazioni fuori linea.

9. Condizioni generali dell'affidatario

Sono a carico del Fornitore, intendendosi remunerati con i corrispettivi contrattuali, tutti gli oneri ed i rischi relativi alla fornitura in oggetto, nonché ogni attività si rendesse necessaria per l'espletamento della stessa. Il Fornitore si obbliga altresì ad eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nella presente richiesta. Il Fornitore si impegna ad avvalersi di personale qualificato, in relazione alle diverse prestazioni contrattuali. Il subappalto, se previsto in sede di offerta, è ammesso nei limiti ed alle condizioni di cui alla vigente normativa. Il Fornitore assume gli obblighi derivanti dalle disposizioni normative per l'affidamento e l'esecuzione dei contratti pubblici finanziati con le risorse del PNRR, compresi quelli in materia di informazione e pubblicità di cui all'art. 34 del Regolamento (UE) 2021/241. Il Fornitore assume inoltre gli obblighi specifici del PNRR relativamente al non arrecare un danno significativo agli obiettivi ambientali cd. "Do No Significant Harm" (DNSH), ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio del 18 giugno 2020, e, ove applicabili, agli obblighi trasversali, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (cd. Tagging), della parità di genere (Gender Equality), della protezione e valorizzazione dei giovani e del superamento dei divari territoriali.