Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | UNIVERSITÀ DEGLI STUDI DI SALERNO

ATTIVITÀ FORMATIVE RIVOLTE A STUDENTI, DOCENTI, FORMATORI E DIPENDENTI DA REALIZZARSI MEDIANTE CONFERENZE, SEMINARI, PIATTAFORME DI FORMAZIONE, CYBER-GAME PERSONALIZZATE, CONNESSE ALLO SVILUPPO DI UNO SCENARIO IMPLEMENTATIVO RELATIVO ALLA COSTITUZIONE DI UNA NATIONAL CYBERSECURITY ACADEMY NELL'AMBITO DEL PROGRAMMA DI RICERCA E INNOVAZIONE DEL PARTENARIATO ESTESO SERICS

NUMERO GARA: _____
CUP: B43C22000750006
CIG: _____

CAPITOLATO SPECIALE D'APPALTO
SCHEMA DI CONTRATTO

Sommario

PREMESSA

La Fondazione SERICS – Security and Rights in CyberSpace, è una fondazione di partecipazione, costituita per essere il soggetto attuatore del Partenariato esteso "**SERICS – Security and Rights in CyberSpace**" finanziato (con Decreto Mur nr. 1556 del 11.10.2022) a seguito della partecipazione all'Avviso Pubblico per la presentazione di Proposte di intervento per la creazione di "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU – Avviso nr. 341 del 15.3.2022.

La Fondazione non ha scopo di lucro, opera nel campo della ricerca scientifica e tecnologica e si propone di:

a. Curare le attività di avvio, attuazione e implementazione del Partenariato esteso SERICS;
b. Svolgere attività di gestione e coordinamento del Partenariato esteso, ricevere le tranche di agevolazioni concesse, verificare e trasmettere al MUR la rendicontazione delle attività svolte dagli Spoke e loro affiliati;
c. Garantire un'ampia diffusione dei risultati di tali attività anche mediante l'insegnamento, la pubblicazione e il trasferimento di conoscenze.

La Fondazione agisce nel rispetto dei limiti funzionali connessi alla sua natura di soggetto attuatore (HUB) per la realizzazione del Programma esteso. In particolare, le attività che la Fondazione intende svolgere sono le seguenti:

a. Promozione e realizzazione di attività di ricerca e sviluppo strumentali alla realizzazione del Partenariato esteso;
b. Concentrazione strutturale di ricerche strategiche attraverso la cooperazione delle istituzioni della ricerca e partner pubblici e privati;
c. Realizzazione di una efficiente coordinamento, verifica – anche scientifica – e monitoraggi delle attività progettuali e del piano degli investimenti finanziato;
d. Rendicontazione scientifica ed economica delle attività del progetto all'Ente finanziatore
e. Promozione di iniziative culturali, della ricerca scientifica e dello sviluppo tecnologico sia nella prospettiva dell'avanzamento della conoscenza sia del servizio alla società;
f. Promozione di iniziative innovative per il sapere, attente anche agli approcci multidisciplinari e alla dimensione applicativa;
g. Al trasferimento dei risultati della ricerca.

Il PROGETTO SERICS

La presente sezione è organizzata in tre parti. In una prima sotto sezione 2.1, il progetto SERICS (*Security and Rights in the Cyberspace*) è inquadrato nello scenario di riferimento, si delineano le sfide principali perseguite dal progetto e si evidenzia l'aderenza agli obiettivi e alle priorità del PNR (Piano Nazionale della Ricerca). In seguito, la Sezione 2.2, illustra gli obiettivi scientifici generali del progetto SERICS, sui quali poggia l'architettura del Partenariato Esteso. Infine, nella sezione 2.3, vengono presentati i partner della proposta (ovvero, gli Spoke e gli Enti affiliati) con l'obiettivo di descrivere le competenze di ciascuno nella gestione e nell'implementazione del progetto SERICS.

SCENARIO GENERALE E PRINCIPALI SFIDE

La sicurezza del cyberspazio è una delle massime priorità dei governi di tutto il mondo. Il blocco delle operazioni commerciali, il controllo surrettizio di servizi infrastrutturali cruciali, il furto di proprietà intellettuale o di importanti informazioni sono solo alcuni esempi di tali minacce. Le recenti campagne di ransomware e di furto di dati hanno rappresentato eventi visibili di una serie di attacchi in ogni angolo del pianeta. Gli attacchi informatici mettono in allarme la popolazione, danneggiano l'economia e compromettono la sicurezza stessa dei cittadini quando colpiscono le reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti, vale a dire le infrastrutture sensibili della società moderna. In Italia, interi settori di eccellenza, come la meccanica, la cantieristica, il Made-in-Italy, il turismo, i beni culturali, l'agroalimentare e i trasporti, potrebbero subire pesanti ricadute sul piano economico in conseguenza di attacchi perpetrati nel cyberspazio da parte di concorrenti commerciali, della criminalità organizzata, ma anche di Stati sovrani. Gli attacchi informatici possono compromettere la credibilità di un'azienda in breve tempo, ma possono anche costringerla a operare per lungo tempo in condizioni non ottimali, indebolendo lo sviluppo della sua attività e la sua capacità commerciale. Un attacco riuscito potrebbe destabilizzare il mercato azionario o obbligazionario, gettando nel caos interi Paesi, oppure agire sui componenti hardware e software delle reti di distribuzione, bloccando, ad esempio, le forniture di gas o il ciclo dei rifiuti urbani. L'industria, ma anche la democrazia può essere oggetto di attacchi nel cyberspazio. Le *fake news* costituiscono l'evoluzione degli attacchi basati sull'ingegneria sociale: confezionate, personalizzate e diffuse in modo mirato attraverso il cyberspazio, le false informazioni tendono a confondere e destabilizzare i cittadini.

Alla luce di queste considerazioni, si pone la questione di come difendere il cyberspazio dalle minacce e dagli attacchi che, attraverso azioni informatiche malevoli, perpetrano frodi, sottraggono dati aziendali sensibili e strategici e colpiscono la stabilità finanziaria, l'ordine pubblico e la vita democratica di un Paese.

Per questo motivo, è particolarmente importante coinvolgere istituzioni, università, centri di ricerca e aziende in modo sempre più esteso e integrato. Un Paese che non ponga la cybersecurity al centro delle proprie politiche di innovazione e trasformazione digitale si espone a un concreto rischio per la prosperità e l'indipendenza economica.

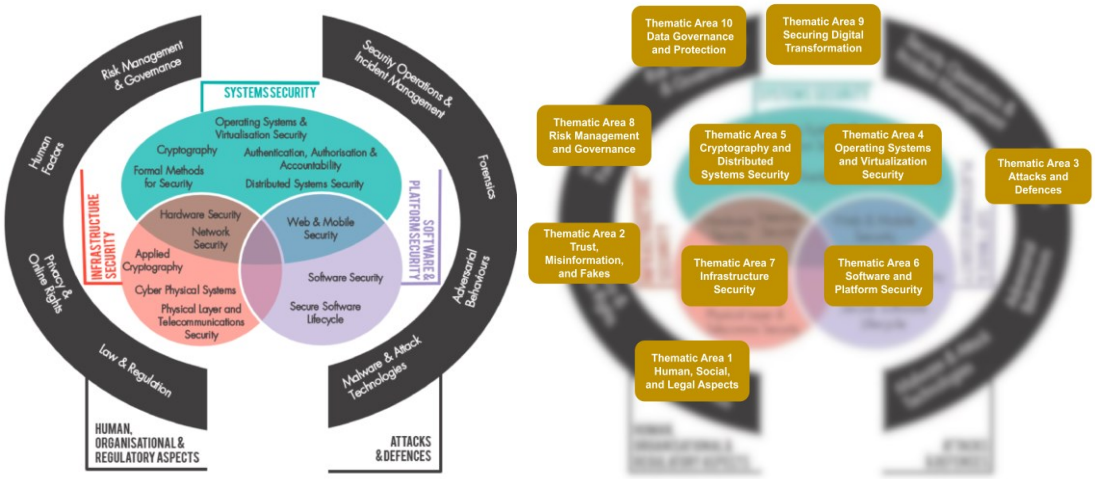
Proprio da tali riflessioni è nata la proposta del Piano Nazionale della Ricerca 2021-2027 dedicata alla Sicurezza dei Sistemi Sociali. Sulla base di queste considerazioni, si è giunti infatti alla definizione dei seguenti obiettivi fondamentali:

- *Protezione di dati e servizi sul Web*: Attraverso la certificazione delle applicazioni che trattano dati sensibili; l'analisi automatizzata delle applicazioni; l'analisi dei sistemi interoperanti.
- *Rilevamento di malware*: Attraverso la raccolta e la convalida di insiemi di dati rappresentativi di comportamenti normali o anomali; una banca dati nazionale di codici malevoli, integrata con banche dati di altri Paesi; strumenti e metodologie per l'automazione del cyberspazio.
- *Lotta alla criminalità informatica/cybercriminalità*: Attraverso una *threat intelligence* o informazione sulle minacce avanzata; l'identificazione delle vulnerabilità in ambienti complessi; l'automazione delle indagini forensi.
- *Garanzia della democrazia*: Attraverso un approccio multidisciplinare all'individuazione delle *fake news*; il monitoraggio dei social media volto ad identificare e comprendere le dinamiche delle *echo chambers*; l'allarme preventivo rispetto a messaggi che possono trasformarsi in potenziali veicoli di informazioni false, fuorvianti o strumentali.
- *Difesa dell'Intelligenza Artificiale*: Attraverso il rilevamento di dati o di immissione di codice; algoritmi di apprendimento robusti e resistenti agli attacchi, tecniche mirate a preservare l'integrità dei dati nella fase di elaborazione e di produzione; approcci alla formazione/elaborazione in grado di garantire la tutela della privacy.

- *Protezione della privacy*: Attraverso la crittografia omomorfa, che consente di elaborare direttamente i dati crittografati, e tecniche di protezione delle infrastrutture di dati federati in spazi di dati internazionali; l'anonimizzazione dei dati per garantire all'utente di non essere nuovamente identificato; una computazione *multi-party* sicura.
- *Preparazione all'eventualità di attacchi da computer quantistici*: nuovi sistemi crittografici il cui livello di sicurezza sia quantificabile in relazione alla crittoanalisi, sia per i dispositivi quantistici che quelli classici; analisi dell'utilizzabilità di sistemi crittografici basati sulla quantistica e sui metodi di generazione e distribuzione delle chiavi per i dispositivi informatici di uso generale; garanzia di interoperabilità tra i sistemi crittografici quantistici e classici.
- *Protezione dell'hardware:* Attraverso metodologie nazionali per il controllo completo dell'intera catena di fornitura hardware, dalla progettazione al processo di produzione, alla manutenzione, fino al ritiro; architetture nazionali *vulnerability-tolerant* che garantiscono livelli di sicurezza predefiniti, anche in sistemi potenzialmente vulnerabili.

È opportuno precisare che gli obiettivi sopra descritti si focalizzavano sulla sicurezza informatica dal punto di vista di disciplina ingegneristica. Ma la cybersecurity non è solo questo. Una caratteristica distintiva della nostra proposta è quella di mantenere l'attenzione anche su quello che è considerato l'"anello debole" della sicurezza generale del cyberspazio: l'essere umano. Una vera ed efficace sicurezza del cyberspazio non è unicamente garantita da una tecnologia solida e robusta, ma anche da una altrettanto solida e robusta regolamentazione dei comportamenti umani. Ciò richiede un profondo coinvolgimento da parte di quanti comprendono le motivazioni, le forze e gli incentivi di natura non tecnica - economisti, sociologi, giuristi e altri esperti - per creare una prospettiva olistica che possa anticipare e guidare strategie efficaci nel mondo reale. Una realtà in grado di creare un ambiente ricco di collaborazioni, partnership e nuove forme di rapporti di lavoro commerciali e accademici, ma allo stesso tempo profondamente impegnativo per la compresenza di differenze fondamentali nella cultura, nella metodologia e nell'approccio alla ricerca. È questa un'ulteriore sfida del progetto, che è tuttavia centrale per il suo successo: a tale scopo, i seguenti obiettivi sono cruciali:

- *Diritti, Regole e Autorità per un cyberspazio sicuro*: Realizzare una rete nazionale di *tech-lawyers*, giuristi esperti di tecnologia, e di un archivio di normative sulla *cybersecurity* (che combini e armonizzi leggi, codici etici, *soft-law*, dottrina e giurisprudenza sul Cyberspazio); Contribuire alla co-regolamentazione internazionale ed europea del Cyberspazio a più livelli e alla regolamentazione della protezione transfrontaliera/sovranazionale dei diritti privati.
- *Aspetti legali ed etici della cybersicurezza:* Privacy digitale e diritti online; regolamentazione dell'E-government e dell'E-democracy; sviluppo di metodologie sicure, a "prova di privacy" e affidabili nell'ambito della sovranità digitale; criminalità informatica e diplomazia informatica.
- *Apprendimento permanente e istruzione sulla regolamentazione della sicurezza informatica:* Modelli e metodi di formazione destinati all'istruzione in tema di cyber security e *governance* dei dati; *Cyber-compliance* per la pubblica amministrazione e per le piccole e medie imprese.



OBIETTIVI SCIENTIFICI DEL PROGETTO SERICS

Punto di partenza per la configurazione del progetto SERICS è stato il CyBoK, un corpus di conoscenze complessivo, concepito con l'aiuto dei massimi esperti a livello internazionale con lo scopo di mappare lo spazio di conoscenza della Cybersecurity.

La Figura 1a riassume le 21 aree di conoscenza introdotte nel CyBoK e che hanno costituito la base per la definizione di questa proposta. In realtà, sulla base delle 10 Aree Tematiche (AT) della SERICS si è definita la struttura dei dieci Spoke della proposta. Le aree tematiche sono frutto di un lungo confronto con un ampio gruppo di ricercatori italiani che rappresentano i diversi approcci alla cybersecurity. I nomi delle aree tematiche e i loro obiettivi principali sono descritti di seguito.

La Figura 1b rappresenta graficamente le aree di conoscenza coperte dalle aree tematiche di SERICS.

Area tematica 1: Aspetti Umani, Sociali e Legali

L'obiettivo principale dell'AT 1 è studiare come creare un cyberspazio affidabile e sicuro combinando sistemi tecnologici solidi con comportamenti umani appropriati. Ciò si baserà su un ecosistema innovativo in cui esperti di tecnologia, giurisprudenza, etica, sociologia e formazione uniranno le forze per definire un processo che, attraverso una prospettiva olistica, possa definire e testare nuove politiche di cybersicurezza. In particolare, l'AT 1 contribuirà alla creazione di nuova conoscenza sugli aspetti normativi, legali ed etici del cyberspazio. Gli obiettivi dettagliati dell'AT 1 possono essere classificati in cinque macro-categorie. La prima categoria riguarda i diritti, le regole, le definizioni, le tassonomie e le autorità utili per creare nuove forme di co-regolamentazione nel cyberspazio. La seconda categoria analizza le questioni legali ed etiche della cybersicurezza, come i diritti fondamentali all'interno del nuovo ecosistema. La terza categoria comprende l'apprendimento continuo e i modelli educativi sulle questioni legali della cybersicurezza. La quarta categoria analizza criminalità informatica e diplomazia informatica come elementi importanti e cruciali di una nuova strategia nazionale, e punta a sviluppare la conoscenza su questo tema nel pubblico non solo accademico. La quinta categoria considera la sovranità digitale, anche in relazione a computazioni e tecnologie basate sull'intelligenza artificiale, il *cloud*, il fog e l'*edge computing*, e alle loro applicazioni in settori specifici, come quelli dell'energia e dei trasporti.

Area tematica 2: Disinformazione e Fake News

Questa AT mira a progettare e sviluppare soluzioni innovative per identificare e gestire le minacce al sistema informativo che si manifestano attraverso le *fake news* e la loro diffusione. Queste azioni malevole, sfruttando il *bias* cognitivi delle persone, generano sfiducia dei cittadini nei media e nelle istituzioni. Il progetto utilizzerà un approccio multidisciplinare tramite l'analisi automatica delle notizie liberamente disponibili i recenti progressi dell'Intelligenza Artificiale e le conoscenze delle scienze politiche e geopolitiche. In primo luogo, il progetto mira a verificare la veridicità dei contenuti delle notizie e l'affidabilità delle fonti. L'obiettivo è implementare metodologie di analisi dei contenuti testuali e multimediali per mettere a punto modelli da

utilizzare per individuare i tentativi di disinformazione. Inoltre, l'analisi delle comunità dei social media darà evidenza delle vulnerabilità cognitive dei partecipanti e delle minacce legate alla diffusione di *fake news*. L'obiettivo è quello di progettare un sistema di allerta precoce per mettere in guardia su informazioni false, sfruttando l'integrità sintattica dei contenuti e i modelli legati ai flussi di disinformazione. Il *framework* risultante punterà a sensibilizzare le persone sugli effetti rischiosi della condivisione di contenuti discutibili. Inoltre, il *framework* supporterà gli esperti e i responsabili della sicurezza nel processo decisionale, adottando un approccio *human-in-the-loop*.

Area tematica 3: Attacchi e Difese

L'AT 3 si propone di analizzare le metodologie di attacco emergenti e di sviluppare metodi avanzati per la rilevazione di attacchi e l'individuazione di linee guida per la progettazione di sistemi informatici che garantiscano una ridotta vulnerabilità a nuove categorie di attacco. Gli obiettivi di dettaglio possono essere suddivisi in quattro macro categorie: (i) Sviluppo di strumenti avanzati per l'analisi dei *malware* e dei software finalizzati all'identificazione delle vulnerabilità che potrebbero essere sfruttate dai *malware* stessi; (ii) Sviluppo di strumenti per l'analisi del traffico di rete per identificare le comunicazioni relative agli attacchi in corso; (iii) Sviluppo di sistemi di *machine learning* robusti agli attacchi e attraverso i quali è possibile estrarre conoscenze finalizzate alla creazione di strumenti più avanzati per l'analisi tempestiva e l'individuazione precoce degli attacchi; (iv) Analisi dei "fattori umani" coinvolti in un attacco con lo sviluppo di strumenti per l'analisi e la correlazione di informazioni provenienti da OSINT (*open sources intelligence*) e per la difesa e prevenzione di attacchi basati su tecniche di *social engineering*.

Area tematica 4: Sicurezza dei Sistemi Operativi e della Virtualizzazione

I sistemi operativi (OS) e le tecnologie di virtualizzazione (VT) sono fattori abilitanti fondamentali per i paradigmi di calcolo e di comunicazione esistenti ed emergenti, ovvero *cloud, fog, edge computing* e 5G/6G. Sfruttando i meccanismi di sicurezza di base forniti dall'hardware, i sistemi operativi e le tecnologie di virtualizzazione offrono meccanismi e servizi di sicurezza fondamentali (quali la gestione dell'identità di base e il controllo degli accessi) su cui si basa la sicurezza delle applicazioni e di conseguenza del cyberspazio. L'AT 4 si occupa di sviluppare servizi di sicurezza automatici di alto livello nonché metodologie innovative di valutazione e garanzia della sicurezza per supportare lo sviluppo *secure-by-design* e la verifica di applicazioni *cloud, edge* e 5G. L'efficacia delle tecniche proposte sarà valutata mediante stress-test in scenari di attacco simulati, ma altamente realistici, eseguiti in sicurezza all'interno di una piattaforma di *CyberRanges* federati.

Area tematica 5: Crittografia e Sicurezza dei Sistemi Distribuiti

L'AT 5 si occupa principalmente di attività di ricerca nei domini della crittografia e della sicurezza dei sistemi distribuiti. A causa della vastità di questi domini e per individuare obiettivi concreti volti a ottenere risultati a lungo termine di alto livello tecnologico con grande beneficio per il Paese, l'AT 5 vede la coesistenza di approcci diversi. Vengono considerate diverse sotto-tematiche (i) primitive e protocolli crittografici, (ii) crittografia fondazionale e crittoanalisi, (iii) crittografia post-quantistica, (iv) identità digitale, autenticazione e *accountability*, e (v) *distributed ledgers* e *blockchain*. Questo per coniugare due anime: la continua ricerca dell'approfondimento della conoscenza (in tutti i campi sopra citati), e l'obiettivo di applicare questo approccio investigativo a sistemi reali. Nel corso della presente iniziativa, ciò sarà realizzato attraverso un unico progetto unificante incentrato sulla nozione di identificazione e tracciamento digitale, interpretando tale nozione anche da prospettive non convenzionali. In base a questo obiettivo generale, le linee di ricerca dell'AT 5 si muoveranno su binari diversi, stimolando continue interazioni e applicazioni verticali dei risultati su specifici domini applicativi.

Area tematica 6: Sicurezza del Software e delle Piattaforme

Il primo obiettivo scientifico dell'AT 6 è fornire un ecosistema in cui gli sviluppatori di software possano facilmente ragionare sulla sicurezza del software. Ciò si baserà su nuove primitive di programmazione astratte e centrate sulla sicurezza e su nuovi modelli semantici che permetteranno di formalizzare, verificare e certificare le proprietà di sicurezza puntando al *secure-by-design*. L'obiettivo è sviluppare nuove tecniche formali basate sulla compilazione sicura e sulla composizione sicura, per ridurre il divario tra i modelli formali,

essenziali per fornire piene garanzie di correttezza, e le implementazioni reali. Il secondo obiettivo scientifico è fornire soluzioni innovative per proteggere la catena di fornitura del software, compresi i processi di gestione e sviluppo del software. L'obiettivo è sviluppare nuove tecniche per eseguire test di sicurezza attraverso un'analisi dinamica continua e per proteggere il software, rilevando attività dannose e prevenendone o limitandone l'impatto, secondo un paradigma di autodifesa. Verranno utilizzati scenari di test per validare e valutare sperimentalmente le tecniche proposte.

Area tematica 7: Sicurezza delle Infrastrutture

L'AT 7 ha come obiettivo generale lo sviluppo di tecnologie di sicurezza per le infrastrutture. Questo obiettivo generale si traduce in quattro obiettivi specifici: (i) Progettare e sviluppare un'architettura informatica sicura aperta, e disponibile a livello nazionale, che sarà il punto di partenza per la costruzione di infrastrutture sicure che non soffrano dei potenziali rischi derivanti dall'uso di tecnologie proprietarie; (ii) Migliorare la sicurezza dell'infrastruttura automobilistica che, con la massiccia interconnessione ed elettrificazione delle auto, diventerà uno degli *asset* più vulnerabili del Paese; (iii) Migliorare la sicurezza, la protezione e la resilienza delle *smart power grid*, che sono una elemento fondamentale per l'ottimizzazione del consumo energetico e per raggiungere il Green deal; (iv) Contribuire al miglioramento della postura di sicurezza degli *asset* ITC (e.g., reti, sistemi e servizi IT/OT) inclusi nel "Perimetro di Sicurezza Nazionale Cibernetica", fornendo ontologie, metodologie, linee guida, *best practice* e strumenti appropriati.

Area tematica 8: Gestione del Rischio e Governance

L'AT 8 intende contribuire alla resilienza informatica dei futuri sistemi e servizi caratterizzati da componenti digitali sempre più interconnessi e intrinsecamente vulnerabili, come richiesto dall'UE attraverso NIS e NIS2, nonché dall'Agenzia Nazionale per la Cybersicurezza (ACN). A tal fine, propone un approccio olistico alla cybersicurezza basato sul rischio che deve includere anche la resilienza, la privacy, e la sicurezza delle organizzazioni, delle industrie, delle infrastrutture critiche e delle relative filiere. Questa AT richiede competenze interdisciplinari adatte ad affrontare sia le sfide scientifico-tecnologiche sia quelle legali e politiche attraverso nuovi modelli per la valutazione continua delle minacce e delle vulnerabilità, ma anche attraverso la progettazione di componenti di rete autodifensivi. L'AT 8 mira anche a promuovere la visione secondo cui un'Europa digitale evoluta richiede la protezione dei diritti e delle libertà fondamentali, la promozione della consapevolezza sociale e una formazione informatica diffusa, nonché il raggiungimento di un equilibrio di genere nella sicurezza informatica.

Area tematica 9: Mettere in sicurezza la trasformazione digitale

L'AT 9 ha l'obiettivo principale di studiare nuovi approcci, metodologie, soluzioni e strumenti in grado di fornire adeguate garanzie di sicurezza per i nuovi scenari applicativi che stanno emergendo oggi come conseguenza della forte accelerazione verso la trasformazione digitale pervasiva. In particolare, i ricercatori coinvolti nelle tematiche del TA 9 lavoreranno su quattro scenari di riferimento, considerati di interesse strategico per il prossimo futuro: (i) lo sviluppo di soluzioni di finanza decentralizzata basate su tecnologie distribuite sicure come i distributed ledger e gli smart contract; (ii) il rafforzamento delle proprietà di sicurezza dei dati e della privacy nei servizi forniti dalla pubblica amministrazione nell'ambito di programmi di e-government; (iii) la proposta di soluzioni di sanità remota basate su dispositivi personali, essenziali per una gestione più efficiente dei pazienti malati cronici o che necessitano di un monitoraggio continuo; (iv) la messa a punto di tecnologie di distribuzione di chiavi quantistiche per applicazioni critiche.

Area tematica 10: *Governance* e Protezione dei Dati

La moderna società digitale si basa, e si baserà sempre di più, sulla raccolta, la condivisione e l'analisi di grandi collezioni di dati, con evidenti vantaggi, dal punto di vista personale e aziendale, nonché con benefici della ricerca e della società. La piena realizzazione di una società digitale basata sui dati può avvenire solo se c'è fiducia nella sicurezza e nella privacy dei dati stessi, e quindi se si rendono disponibili soluzioni che ne garantiscano corretta protezione e uso. Le leggi e i regolamenti sulla protezione dei dati impongono restrizioni che ne limitano l'uso e i singoli, così come le aziende, chiedono il rispetto dei requisiti di protezione e la garanzia di un'effettiva protezione dei loro dati. TA 10 risponde a questa esigenza puntando a garantire ai vari

attori coinvolti nella condivisione dei dati e la disponibilità di strumenti e scenari per il controllo dei loro dati, per supportare la condivisione dei dati in modo selettivo e sicuro, garantendo allo stesso tempo funzionalità, efficienza e scalabilità. Le soluzioni per la protezione dei dati sviluppate nell'ambito dell'AT 10 consentiranno e incoraggeranno nuovi scenari applicativi e introdurranno nuove opportunità di condivisione dei dati, in modo controllato, nel rispetto della privacy e delle restrizioni di accesso, garantendo l'integrità dei dati e dei risultati delle analisi. L'AT 10 contribuirà quindi a una vera e piena realizzazione della sovranità digitale.

PARTNER DEL PROGETTO SERICS

In questa sezione, si espongono le esperienze pregresse e le competenze scientifiche e progettuali di ciascun partecipante in riferimento all'area di specializzazione del Partenariato Esteso (*Cybersecurity: nuove tecnologie e tutela dei diritti*) in termini di innovazione e trasferimento tecnologico. Vengono illustrate le comprovate competenze dei singoli Spoke e degli enti affiliati nella gestione e implementazione di progetti di ricerca fondamentale o applicata, con particolare riferimento all'area del partenariato. Si descrive inoltre la capacità di sviluppare il programma di ricerca basato su un approccio interdisciplinare, olistico e orientato alla soluzione dei problemi e si specificano le eventuali collaborazioni esistenti a livello nazionale e internazionale con altre istituzioni e centri di alta qualità scientifica.

- Grazie alle caratteristiche della procedura di selezione (vedi sotto, sezione B), la proposta ha riunito il segmento più rappresentativo della comunità nazionale di Cybersecurity. Le più importanti istituzioni accademiche sulla Cybersecurity sono Partner di SERICS e può essere facilmente constatato come tra i coordinatori degli Spoke e i PI del progetto, figurano numerosi scienziati di primo piano. In generale, gli accademici presenti vantano un curriculum eccellente, una comprovata esperienza nel campo della sicurezza informatica e visibilità internazionale (partecipazioni all'ECSO, agli Steering e ai Program Committees delle principali conferenze sulla Cybersecurity, all'Editorial board di riviste di spicco, esperienza come Editor in Chief di riviste di rilievo, come coordinatore di progetti di ricerca internazionali, e così via.).
- Il Partenariato è fortemente multidisciplinare, in quanto comprende un numero rilevante di settori scientifici (denominati SSD, nel sistema accademico italiano) che spaziano tra scienza, ingegneria, economia e giurisprudenza. Un fattore chiave dell'iniziativa, che consente al partenariato di adottare un approccio olistico alla cybersecurity, come intrinsecamente richiesto da quest'area di ricerca. L'analisi dei 27 progetti attraverso i quali si articola il programma generale di ricerca (descritto nella Sezione B) supporta chiaramente quanto sopra affermato, dimostrando come l'ampio e variegato insieme di competenze sia reso complementare per il raggiungimento di obiettivi di ricerca che per loro natura richiedono un approccio multiprospettico.
- La proposta coinvolge soggetti provenienti da tutte le aree geografiche del Paese, comprese le regioni del Sud. Come descritto di seguito, 3 dei 10 Spoke sono situati nel Mezzogiorno d'Italia, uno Spoke (vale a dire il Consiglio Nazionale delle Ricerche) la cui sede principale è nel Centro Italia, è distribuito su tutto il territorio nazionale, con il coinvolgimento nella proposta di molti istituti di tale Partner presenti nelle diverse aree del Paese. Un altro Spoke ha sede a Roma (ovvero, nel Centro Italia), mentre 4 Spoke si trovano nel Nord Italia. Considerando gli altri Partner (cioè i soggetti affiliati agli Spoke), l'entità della distribuzione del partenariato sull'intero territorio aumenta, data la partecipazione di un'altra università situata al Sud (nella fascia orientale del Meridione), di altri tre istituti di ricerca dislocati nel Centro Italia e un altro istituto di ricerca al Nord. Infine, tutti i partner industriali coinvolti hanno sedi distribuite su tutto il territorio nazionale.

Nella tabella sottostante sono elencati tutti i Partner del Partenariato Esteso con l'acronimo corrispondente, che verrà utilizzato nel resto del documento. La tabella riporta anche la tipologia di ente (se Università pubblica, Ente pubblico di ricerca, Istituto di istruzione superiore e di ricerca, Ente pubblico senza scopo di lucro/ non profit, Azienda).

Tabella 1

Soggetto	Acronimo	Tipo di Ente

Consiglio Nazionale delle Ricerche	CNR	Ente pubblico di ricerca
Università degli Studi di Salerno	UNISA	Università pubblica
Università degli Studi di Cagliari	UNICA	Università pubblica
Università degli Studi di Genova	UNIGE	Università pubblica
Università degli Studi di Calabria	UNICAL	Università pubblica
Università Ca' Foscari di Venezia	UNIVE	Università pubblica
Politecnico di Torino	POLITO	Università pubblica
Università Alma Mater Studiorum di Bologna	UNIBO	Università pubblica
Università degli Studi di Roma "La Sapienza"	UNIROMA1	Università pubblica
Università degli Studi di Milano	UNIMI	Università pubblica
Consorzio Interuniversitario Nazionale per l'Informatica	CINI	Ente pubblico senza scopo di lucro
Consorzio Nazionale Interuniversitario per le Telecomunicazioni	CNIT	Ente pubblico senza scopo di lucro
Fondazione Bruno Kessler	FBK	Ente di ricerca
Fondazione Ugo Bordoni	FUB	Ente di ricerca
Scuola IMT Alti Studi Lucca	IMT	Istituto di Alta Formazione e Ricerca
Scuola Superiore Sant'Anna di Pisa	SSSA	Istituto di Istruzione Superiore e di Ricerca
Università degli Studi di Bari "Aldo Moro"	UNIBO	Università pubblica
Università degli Studi di Firenze	UNIFI	Università pubblica
Deloitte	DELOITTE	Azienda
Eni S.p.A.	Eni	Azienda
Fincantieri S.p.A.	Fincantieri	Azienda
Intesa Sanpaolo S.p.A.	ISP	Azienda
Leonardo S.p.A.	Leonardo	Azienda
TIM - Telsy	TIM	Azienda

AMBITO DEL PROGETTO SERICS

Nell'ambito delle attività progettuali (M42: Academy 1° anno; M53: Academy 2° anno; M64: Academy 3° anno), come da cronoprogramma di attuazione (allegato C del Decreto Mur nr. 1556 del 11.10.2022), del progetto ammesso a finanziamento "SERICS – Security and Rights in CyberSpace" (data di avvio del progetto 1 gennaio 2023 e data di fine 31 Dicembre 2025), la Fondazione ha il compito di curare, organizzare ed erogare attività formative rivolte a studenti, docenti, formatori, dipendenti e altri da realizzarsi mediante conferenze, seminari, piattaforme di formazione, cyber-game personalizzate, connesse allo sviluppo di uno scenario implementativo relativo alla costituzione di una National Cybersecurity Academy nell'ambito del Programma di ricerca e innovazione del Partenariato Esteso SERICS. L'attività è da completarsi entro e non oltre Dicembre 2025.

La formazione in ambito cybersecurity è divenuta elemento essa stessa di protezione e gestione del rischio cyber. La Strategia Nazionale di Cybersecurity identifica la formazione e promozione della cultura della sicurezza cibernetica come un fattore abilitante alla realizzazione degli obiettivi della strategia stessa, in quanto correlati in maniera trasversale agli obiettivi di protezione, risposta, sviluppo.

Il contesto tecnologico attuale comporta la necessità da parte di tutte le organizzazioni di costruire o aumentare la consapevolezza collettiva dei rischi derivanti dall'utilizzo di strumenti informatici.

La formazione risponde alla duplice esigenza di:

- creare consapevolezza diffusa a livello aziendale delle minacce e dei rischi cyber, fornendo le nozioni in merito ai presidi ed alle buone pratiche che ciascun utente deve mettere in pratica per prevenire o reagire ad incidenti informatici;

- rafforzare, integrare o creare in azienda nuove competenze – manageriali e specialistiche – per gestire consapevolmente la sicurezza degli asset tecnologici.

La formazione è da considerarsi parte integrante del programma di mitigazione dei rischi cyber e di gestione della sicurezza delle informazioni.

I principali obiettivi del progetto sono:

- elaborazione e condivisione di conoscenze e competenze attraverso l'utilizzo di strumenti concreti che riducano lo skill shortage nell'ambito della difesa del cyberspazio, difesa informatica, protezione e governance dei dati. Questo permetterà l'implementazione corretta dei processi e delle infrastrutture di-gitali che diventeranno più sicure e affidabili.
- cybersecurity awareness: diffondere una sempre maggiore consapevolezza dei rischi legati all'utilizzo delle tecnologie informatiche con un approccio multidisciplinare perché la sicurezza del terzo millennio non risiede soltanto nei mille prodotti hardware e software progettati per creare le migliori difese, ma trova radice principalmente nell'educazione di chi vive il contesto, nell'alfabetizzazione di chi è digiuno di questioni hi-tech e di chi utilizza strumenti informativi per lavoro e svago.

1. OGGETTO DEL SERVIZIO "ACADEMY"

L'appalto ha per oggetto l'esecuzione delle seguenti attività:

1. Attività di formazione specialistica per dipendenti/professionisti
2. Attività di promozione e supporto di scuole specialistiche di dottorato
3. Attività di promozione e supporto di master universitari
4. Corsi di imprenditorialità per laureandi, neo-laureati, dottorandi e neo-dottorati
5. Train the trainers per le seguenti categorie:
    - per studenti K0-K8
    - soggetti deboli e svantaggiati
6. Valutazione, monitoraggio, valorizzazione e condivisione dei contenuti: sviluppo di metodologie e strumenti per l'identificazione delle esigenze formative (skill gap) da parte dei dipendenti e delle organizzazioni in generale; sviluppo di metodologie e strumenti per la valutazione il monitoraggio dell'efficacia dell'attività formativa.

1.1 Attività di formazione specialistica per dipendenti/professionisti

Le attività riguarderanno la progettazione, la realizzazione ed erogazione di un catalogo di corsi avanzati su tecnologie allo stato dell'arte che dovranno contenere i seguenti contenuti minimi:

- Applied crypto
- Privacy-enhancing technologies
- Advanced Technologies for Identity and Access Management
- Advanced Hardware Security
- Post quantum cryptography
- Quantum key distribution
- Hardware security
- Legal aspects of Cybersecurity
- Secure by design su prodotti, servizi e supply chain
- Impatti, sia lato attaccanti che lato difensori, delle Artificial Intelligence, incluso trustworthiness, policy & controls

- Sicurezza OT
- Data & Cloud Security
- Zero Trust architecture, planning & implementation
- Machine Learning for CyberSecurity and Security of Machine Learning

L'attività di formazione sarà rivolta a soggetti (dipendenti/professionisti) altamente specializzati, rispondendo a un bisogno del tessuto produttivo e promuovendo l'adozione di soluzioni avanzate, che contribuiscono a migliorare la competitività del sistema paese. I contenuti formativi si integreranno, evitando sovrapposizioni, alla formazione erogata dai centri di competenza. I contenuti saranno erogati sia in presenza che a distanza e prevederanno la predisposizione e l'erogazione di attività laboratoriali (esercitazioni).

I servizi richiesti prevedono per ciascuna delle attività suindicate:

- Programmazione, pianificazione, organizzazione, valutazione e comunicazione delle attività di formazione specialistica. L'attività dovrà includere il supporto nella predisposizione di un business plan e dei ROI per la progettazione, il posizionamento strategico (evitando sovrappressioni con iniziative similari, quali ad esempio i centri di competenza), la realizzazione e l'erogazione del catalogo "altamente specializzato", rispondendo a un bisogno del tessuto produttivo e promuovendo l'adozione di soluzioni avanzate, che contribuiscono a migliorare la competitività del sistema paese.
- Selezione e arruolamento di docenti, tutor e personale esperto di supporto alla progettazione, produzione del materiale didattico (inclusivo delle attività laboratoriali) e svolgimento delle attività formative; ciò include il supporto alla predisposizione di albi di esperti per i profili utilizzando i criteri indicati in Tabella 2; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere ai formatori che contribuiranno alla realizzazione del programma.
- Progettazione formativa e realizzazione del materiale didattico per almeno 12 moduli formativi (nell'ambito dei contenuti proposti) della durata di 40 ore per ciascun modulo, impiegando i profili di Tabella 2 per almeno 300 giornate/uomo; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere agli esperti che contribuiranno alla realizzazione del programma;
- Erogazione di almeno 12 edizioni per ciascun modulo formativo (nell'ambito dei contenuti proposti), a distanza, impiegando i profili di Tabella 2 per almeno 300 giornate/uomo
- Erogazione di almeno 6 seminari di presentazione presso le sedi di università partner del progetto SERICS (2 al nord, 2 al centro, 2 al sud).
- Progettazione attività laboratoriali per almeno 12 moduli formativi (nell'ambito dei contenuti proposti) della durata di 16 ore per ciascun modulo
- Erogazione attività laboratoriali per almeno 12 moduli formativi (nell'ambito dei contenuti proposti) della durata di 16 ore per ciascun modulo
- Servizi organizzativi e logistici relativi all'organizzazione dei seminari e delle attività laboratoriali (es. selezione e affitto delle sedi necessarie, strumentazioni, catering per i partecipanti, missioni dei docenti e tutor coinvolti) per un minimo di 100 partecipanti.
- Predisposizione, realizzazione e diffusione digitale del materiale divulgativo (es. presentazione catalogo, scheda corso, ecc.), mediante sito web della Fondazione, strumenti social, canali tradizionali, ecc.

Si precisa che le competenze dei profili di docenti, tutor ed esperti (come da Tabella 2) andranno individuate in ambito accademico/universitario, nelle Academy dell'Industria e nei poli di ricerca e organizzazioni strategiche nazionali, in un'ottica di rete nazionale e di PPP.

1.2 Attività di promozione e supporto di scuole specialistiche di dottorato

Le attività riguarderanno la progettazione e realizzazione di una scuola specialistica di dottorato, intesa come iniziativa di formazione specialistica ad integrazione del corso di dottorato di ricerca, per ciascuno dei 10 spoke del PE SERICS.

I servizi richiesti prevedono per ciascuna delle attività suindicate:

- Programmazione, pianificazione, organizzazione, valutazione e comunicazione delle attività di formazione sulle tematiche progettuali inerenti ogni singolo spoke del progetto SERICS, da erogarsi nell'ambito dei corsi di dottorato già attivi presso i soggetti partner di progetto;
- Selezione e arruolamento di docenti, tutor e personale di supporto alla progettazione e svolgimento delle attività formative; ciò include il supporto alla predisposizione di albi di esperti per i profili utilizzando i criteri indicati in Tabella 2; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere ai formatori che contribuiranno alla realizzazione del programma;
- Progettazione formativa e realizzazione del materiale didattico per 10 scuole specialistiche (nell'ambito delle tematiche di ciascun spoke) della durata di 40 ore ciascuna, impiegando i profili di Tabella 2 per almeno 250 giornate/uomo; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere agli esperti che contribuiranno alla realizzazione del programma;
- Erogazione a distanza di 10 edizioni, 1 per ciascuna scuola specialistica (nell'ambito delle tematiche di ciascun spoke), impiegando i profili di Tabella 2 per almeno 50 giornate/uomo;
- Servizi organizzativi e logistici relativi all'organizzazione dei corsi (es. selezione e affitto delle sedi necessarie, strumentazioni, catering per i partecipanti, missioni dei partecipanti, docenti e tutor) per un minimo di 20 partecipanti per ogni spoke;
- Registrazione degli interventi con standard di qualità elevati e successiva messa a disposizione gratuita delle registrazioni alla comunità;
- Predisposizione, realizzazione e diffusione digitale del materiale divulgativo (es. presentazione catalogo, scheda corso, ecc.), mediante sito web della Fondazione, strumenti social, canali tradizionali, ecc.

1.3 Attività di promozione e supporto di master universitari

Le attività riguarderanno la promozione e il supporto di master universitari svolti nell'ambito delle tematiche del PE SERICS.

I servizi richiesti prevedono per ciascuna delle attività suindicate:

- Programmazione, pianificazione, organizzazione, valutazione e comunicazione di moduli specialistici (ad es. dedicati all'imprenditorialità) che arricchiscono l'offerta formativa dei master individuati nell'ambito delle tematiche del PE SERICS, aumentando l'efficacia;
- Selezione e arruolamento di docenti, tutor e personale di supporto alla progettazione e svolgimento delle attività formative; ciò include il supporto alla predisposizione di albi di esperti per i profili utilizzando i criteri indicati in Tabella 2; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere ai formatori che contribuiranno alla realizzazione del programma;
- Progettazione formativa e realizzazione del materiale didattico per almeno 3 moduli formativi (nell'ambito dei contenuti proposti) della durata di 40 ore per ciascun modulo
- Erogazione a distanza di almeno 5 edizioni per ciascun modulo formativo (nell'ambito dei contenuti proposti)

- Servizi organizzativi e logistici relativi all'organizzazione dei corsi (es. selezione e affitto delle sedi necessarie, strumentazioni, trasferimenti, catering per i partecipanti, missioni dei docenti e tutor) per un minimo di 100 partecipanti;
- Registrazione degli interventi con standard di qualità elevati e successiva messa a disposizione gratuita delle registrazioni alla comunità;
- Predisposizione, realizzazione e diffusione digitale del materiale divulgativo (es. presentazione catalogo, scheda corso, ecc.), mediante sito web della Fondazione, strumenti social, canali tradizionali, ecc.

1.4 Corsi di imprenditorialità per laureandi, neo-laureati, dottorandi e neo-dottorati

Le attività riguarderanno la progettazione e realizzazione di una serie di lezioni (engaging!) che insegnino a scrivere "il mio primo business plan" e a confrontarsi con le opportunità e le difficoltà legate alla creazione di impresa, rivolti laureandi, neo-laureati, dottorandi e neo-dottorati, nell'ambito delle tematiche del PE SERICS.

I servizi richiesti prevedono per ciascuna delle attività suindicate:

- Programmazione, pianificazione, organizzazione, valutazione e comunicazione delle attività formative per un numero minimo di 200 partecipanti;
- Progettazione formativa e realizzazione del materiale didattico per i moduli formativi della durata complessiva di almeno 80 ore;
- Erogazione in presenza e/o a distanza di almeno 6 edizioni presso le sedi dei partner del progetto SERICS (2 al nord, 2 al centro, 2 al sud);
- Servizi organizzativi e logistici relativi all'organizzazione dei corsi (es. selezione e affitto delle sedi necessarie, strumentazioni, catering per i partecipanti, missioni dei docenti e tutor) per un minimo di 200 partecipanti;
- Registrazione degli interventi con standard di qualità elevati e successiva messa a disposizione gratuita delle registrazioni alla comunità;
- Predisposizione, realizzazione e diffusione digitale del materiale divulgativo (es. presentazione catalogo, scheda corso, ecc.), mediante sito web della Fondazione, strumenti social, canali tradizionali, ecc.

1.5 Train the trainers

Le attività si rivolgono ai docenti che erogano la formazione alle seguenti categorie:

1. studenti K0-K8[1]

2. soggetti deboli e svantaggiati

1.5.1 Categoria: Studenti K0-K8

I servizi richiesti prevedono:

- Coinvolgimento di esperti multidisciplinari per:
    - Studio delle best practice internazionali relative all'insegnamento dei concetti basilari di cybersicurezza e di uso consapevole del digitale per studenti K0-K8
    - Definizione di un percorso di formazione di professori
- Preparazione e realizzazione del materiale didattico per i percorsi individuati della durata complessiva di 80 ore, impiegando i profili di Tabella 2 per almeno 50 giornate/uomo; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere agli esperti che contribuiranno alla realizzazione del programma;
- Erogazione a distanza di almeno 10 edizioni per ciascun modulo formativo, impiegando i profili di Tabella 2 per almeno 100 giornate/uomo, erogabili tramite la piattaforma SOFIA del Ministero dell'Istruzione e del Merito per la formazione di docenti di studenti K0-K8 in grado di insegnare in modo efficace i concetti basilari di cybersicurezza e di uso consapevole del digitale;
- Predisposizione, realizzazione e diffusione digitale del materiale divulgativo (es. presentazione catalogo, scheda corso, ecc.), mediante sito web della Fondazione, strumenti social, canali tradizionali, ecc.

1.5.2 Categoria: Soggetti deboli e svantaggiati

I servizi richiesti I servizi richiesti prevedono:

- Coinvolgimento di esperti multidisciplinari per:
    - Studio delle best practice internazionali relative all'insegnamento dei concetti basilari di cybersicurezza e di uso consapevole del digitale per soggetti deboli e svantaggiati (e.g., Neets, carcerati, immigrati, portatori di handicap)
    - Definizione di un percorso di formazione di trainer.
- Preparazione e realizzazione del materiale didattico per i percorsi individuati della durata complessiva di 80 ore, impiegando i profili di Tabella 2 per almeno 50 giornate/uomo; in Tabella 2 è anche riportata la retribuzione lorda da corrispondere agli esperti che contribuiranno alla realizzazione del programma;
- Erogazione a distanza di almeno 10 edizioni per ciascun modulo formativo, impiegando i profili di Tabella 2 per almeno 100 giornate/uomo, per la formazione di docenti in grado di insegnare in modo efficace i concetti basilari di cybersicurezza e di uso consapevole del digitale ai soggetti deboli e svantaggiati di cui sopra;
- Predisposizione, realizzazione e diffusione digitale del materiale divulgativo (es. presentazione catalogo, scheda corso, ecc.), mediante sito web della Fondazione, strumenti social, canali tradizionali, ecc.

Tabella 2

Profilo	Criteri	Compenso lordo minimo orario
Esperto	Esperto con comprovata esperienza nella preparazione di test di ammissione a competizioni tipo olimpiadi di cybersicurezza, di informatica, etc	€ 100,00

Esperto	Esperto a supporto della progettazione alla realizzazione delle attività formative	€ 100,00
Esperto	Esperto con comprovata esperienza nello svolgimento di attività di preparazione del relativo materiale didattico in percorsi di formazione su varie tematiche di cybersicurezza	€ 100,00
Esperto	Esperto con comprovata esperienza nello sviluppo e nella gestione di piattaforme per la gestione di competizioni CFT a livello sia nazionale sia internazionale	€ 100,00
Docente	Docente universitario afferente ad uno dei Settori Scientifici Disciplinari congruenti coi temi della Cybersecurity e la Tutela dei diritti nel CyberSpaceoppure, ricercatore di centri di ricerca accreditati dall'ANVUR. In ogni caso deve è richiesta comprovata e pluriennale esperienza di attività di ricerca e insegnamento su temi inerenti alla Cybersecurity	€ 100,00
Tutor	Esperto con comprovata esperienza nello svolgimento di attività di tutoraggio in percorsi di formazione su varie tematiche di cybersicurezza	€ 80,00

N.B.: le spese di missione di tali figure dovranno essere incluse nei servizi organizzativi e logistici relativi all'organizzazione dei corsi

1.6 Valutazione, monitoraggio, valorizzazione e condivisione dei contenuti

Per ogni attività formativa, occorre definire, pianificare e realizzare un'azione di valutazione adeguata e personalizzata, volta a misurare l'efficacia e l'efficienza attraverso la somministrazione di questionari in ingresso e in uscita (erogabili ON LINE), l'individuazione di specifici KPI per il monitoraggio delle attività, ecc.

A completamento delle attività erogate (ed incluso nell'importo a base d'asta) si richiede la valorizzazione e la condivisione dei contenuti, del materiale e delle esperienze attraverso:

- Progettazione e realizzazione di un sito internet ad hoc, accessibile tramite il sito istituzionale della Fondazione SERICS, per la presentazione e valorizzazione dell'offerta formativa, dei target, degli obiettivi e dei contenuti formativi offerti
- Progettazione, realizzazione e manutenzione di un Content Management System (CMS) per l'organizzazione e accessibilità, sulla base di specifici ruoli e profili di autenticazione, dei contenuti e del materiale prodotto e utilizzato a supporto della formazione. Il CMS dovrà mettere a disposizione un ambiente di collaborazione e/o condivisione tra i discenti e canali di interazione sincrona e/o asincrona con i docenti/tutor
- Organizzazione, gestione e pubblicazione dei contenuti e del materiale prodotto e utilizzato a supporto della formazione sul CMS. Il CMS dovrà consentire anche la fruizione del materiale in modalità remota, attraverso la gestione di percorsi modulari e processi di assesment e autovalutazione, garantendo la tracciabilità
- Supporto, assistenza e formazione sull'utilizzo del CMS

L'infrastruttura sarà ospitata presso l'architettura cloud messa a disposizione da Fondazione SERICS.

PROFILI PROFESSIONALI

Il team di lavoro è articolato nei seguenti profili professionali:

Il **Project Manager** è referente verso il Process Owner dell'Academy avrà il compito di recepire le esigenze dell'Università degli Sudi di Salerno e di fare da interfaccia per la gestione delle attività di progettazione, organizzazione, erogazione, valutazione. Fornirà, inoltre, un aggiornamento sistematico relativo allo svolgimento del progetto e dovrà essere in possesso dei seguenti requisiti minimi:

- piena padronanza della lingua italiana, parlata e scritta;
- adeguata preparazione e formazione professionale, anche in relazione alle competenze informatiche necessarie per l'esecuzione del servizio;
- possesso dei poteri necessari per l'esecuzione del servizio e delle prestazioni accessorie;
- reperibilità almeno dalle ore 9.00 alle ore 17.00 (gmt + 1h) dei giorni lavorativi;

L'Università degli Studi di Salerno si rivolgerà direttamente al Project Manager dell'impresa affidataria per ogni problema che dovesse insorgere durante l'esecuzione del contratto. Le comunicazioni formali che saranno trasmesse al Project Manager dell'impresa affidataria si intenderanno come validamente effettuate all'Appaltatore ai sensi e per gli effetti di legge.

Quanto sarà dichiarato e sottoscritto dal Referente dell'Appaltatore sarà considerato dall'Università degli Studi di Salerno dichiarato e sottoscritto in nome e per conto dell'Appaltatore.

In caso di impedimento o assenza del Project Manager dell'impresa affidataria, l'Appaltatore dovrà darne tempestiva notizia al Process Owner dell'Academy indicando contestualmente il nominativo del sostituto.

L'Università degli Studi di Salerno si riserva di chiedere la sostituzione del Project Manager dell'impresa affidataria senza che l'Appaltatore possa sollevare obiezioni, in caso di documentata inadeguatezza alle esigenze del servizio del nominativo designato.

- il **Senior Account** avrà il compito di trasferire le esigenze dell'Università degli Studi di Salerno al team interno del soggetto assegnatario del bando e di raccordarsi con il project manager. Egli garantirà l'uniformità di rappresentazione e di messaggio, fornirà tutto il materiale utile al project manager dell'impresa affidataria per opportuna condivisione con il Process Owner dell'Academy e dovrà essere in possesso dei seguenti requisiti minimi:
  - piena padronanza della lingua italiana, parlata e scritta;
  - adeguata preparazione e formazione professionale, anche in relazione alle competenze informatiche necessarie per l'esecuzione del servizio;
  - possesso dei poteri necessari per l'esecuzione del servizio e delle prestazioni accessorie;
  - reperibilità almeno dalle ore 9.00 alle ore 17.00 (gmt + 1h) dei giorni lavorativi;
- il **Responsabile delle attività di valutazione e monitoraggio** avrà il compito di monitorare i risultati di tutte le attività e raccordarli in un cruscotto di lettura che tenga in opportuna considerazione i KPI definiti alla partenza del progetto. Egli dovrà essere in possesso dei seguenti requisiti minimi:
  - piena padronanza della lingua italiana, parlata e scritta;

- adeguata preparazione e formazione professionale, anche in relazione alle competenze informatiche necessarie per l'esecuzione del servizio;
- possesso dei poteri necessari per l'esecuzione del servizio e delle prestazioni accessorie;
- reperibilità almeno dalle ore 9.00 alle ore 17.00 (gmt + 1h) dei giorni lavorativi;

PROPRIETÀ DEI RISULTATI

- Ogni materiale prodotto è di proprietà della Fondazione SERICS e, per quanto di competenza, dell'Università degli Studi di Salerno, e non potrà essere utilizzato o divulgato da terzi senza autorizzazione scritta
- Non potranno essere utilizzati brand e loghi differenti da quelli della Fondazione SERICS, se non espressamente autorizzati

2. AMMONTARE DELL'APPALTO

L'ammontare complessivo posto a base di gara è di € 2.960.000,00 (IVA esclusa) con oneri della sicurezza pari a € 0,00 per l'assenza di rischi da interferenza.

3. DURATA DELL'APPALTO

Il presente appalto ha la durata di mesi 15 (quindici) senza possibilità di proroga o rinnovo, con decorrenza dalla stipula del contratto.

4. VARIAZIONE PRESTAZIONI CONTRATTUALI

L'ammontare dell'appalto potrà variare sia in aumento sia in diminuzione nel limite del 20% (venti), ai sensi della vigente normativa, art. 120 – comma 9 del D. Lgs. 36/2023, senza mutamenti delle condizioni contrattuali. L'appaltatore, senza necessità di alcuna accettazione, è tenuto ad eseguire il servizio agli stessi patti, prezzi e condizioni del contratto originario senza diritto ad alcuna indennità ad eccezione del corrispettivo relativo alle nuove prestazioni.

Per l'intera durata dell'appalto non è prevista alcuna modifica delle condizioni offerte in sede di gara.

Nessun onere aggiuntivo, salvo ove espressamente previsto nel presente capitolato, può essere richiesto dall'Appaltatore all'Università degli Studi di Salerno.

5. REVISIONE PREZZI

Qualora nel corso di esecuzione del contratto si verifica una variazione, in aumento o in diminuzione, del costo dei servizi superiore al cinque per cento, dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione, in relazione alla prestazione principale. Ai fini del calcolo della variazione dei prezzi si utilizza l'indice dei prezzi al consumo per le famiglie di operai e impiegati come previsto dall'articolo 60, comma 3, lettera b del D. Lgs. 36/2023, pubblicato dall'Istat.

6. MODALITÀ DI FATTURAZIONE E PAGAMENTO

A far data dall'inizio del servizio saranno redatti dal Direttore dell'Esecuzione con cadenza trimestrale.

Sul valore del contratto di appalto sarà corrisposto, su richiesta dell'appaltatore ed entro quindici giorni dall'effettivo inizio della prestazione, l'importo dell'anticipazione del prezzo pari al 20 per cento dell'ammontare complessivo del contratto con le modalità ed i termini di cui all'art.125 del d.lgs.36/2023 s.m.i. .

Il pagamento delle rate di cui trattasi avverrà entro 30 gg. dalla data di ricezione fattura, previa attestazione della regolare esecuzione del servizio da parte del direttore dell'esecuzione. Sull'importo da pagare sarà operata una ritenuta dello 0,50% ai sensi dell'art. 11, comma 6, del D. Lgs. 36/2023. Le ritenute saranno svincolate soltanto in sede di liquidazione finale.

L'Appaltatore, ai fini dei pagamenti, dovrà emettere fatture intestate a:

Università degli Studi di Salerno

Ufficio di Coordinamento attività per il Piano Nazionale Ripresa e Resilienza (PNRR)

Via Giovanni Paolo II, 132 - 84084 - Fisciano (SA)

P. IVA 00851300657 – C.F. 80018670655

Le fatture dovranno riportare, oltre a quanto previsto per legge:

- il codice univoco IPA
- il CIG
- il CUP: B43C22000750006
- la dicitura: Per l'attuazione del Progetto SERICS PE 14 M4 C2 – Investimento 1.3

In caso di ingiustificato ritardo nei pagamenti del corrispettivo, il creditore ha diritto a chiedere la corresponsione degli interessi moratori dal giorno successivo alla scadenza del termine di pagamento. Il saggio degli interessi è determinato ai sensi del D. Lgs. n. 192 del 9 novembre 2012. Eventuali commissioni bancarie connesse all'esecuzione dei pagamenti sono a carico dell'Appaltatore e sono detratte dalle somme ad esso dovute. I mandati di pagamento saranno evasi con le modalità previste dalla L. 136/2010 e s.m.i. sul conto corrente dedicato alle commesse pubbliche indicato dall'impresa ai sensi della medesima legge.

Inoltre, ogni fattura dovrà riportare l'importo complessivo delle ritenute che l'Università degli Studi di Salerno applicherà ai sensi dell'art. 11 del D. Lgs. 36/2023 e l'importo della fattura al netto di tali ritenute.

7. PENALI

In caso di mancato rispetto delle prescrizioni previste dal presente Capitolato, ai sensi dell'art. 126 del D. Lgs. 36/2023 saranno applicate le penali per il ritardato adempimento calcolate in misura giornaliera dell'1 per mille dell'ammontare netto contrattuale.

L'ammontare delle penalità sarà addebitato sui crediti dell'Appaltatore nei confronti dell'Università degli Studi di Salerno; qualora tali crediti risultassero insufficienti, l'ammontare delle penalità sarà portato in detrazione sulla cauzione definitiva.

Si conviene che unica formalità preliminare all'irrogazione delle penali è la contestazione degli addebiti in via amministrativa a mezzo PEC inviata dall'Università degli Studi di Salerno all'Appaltatore, il quale potrà, nei **20 (venti) giorni** successivi, produrre, a mezzo PEC inviata all'Università degli Studi di Salerno eventuali contestazioni all'addebito.

Qualora l'ammontare delle penalità addebitate superi il 10% dell'importo complessivo contrattuale, dell'importo globale netto dell'accordo quadro, il contratto è risolto di diritto.

8. OBBLIGHI E ONERI A CARICO DELL'APPALTATORE

Sono a carico dell'Appaltatore tutti gli oneri e rischi relativi alle prestazioni oggetto del presente appalto, nonché ogni attività si rendesse necessaria al corretto e completo adempimento delle stesse. L'Appaltatore si impegna ad eseguire le prestazioni a perfetta regola d'arte e nel rispetto delle norme vigenti e delle modalità e termini indicati dall'Università degli Studi di Salerno. Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula del contratto, resteranno a carico dell'Appaltatore intendendosi remunerati dal corrispettivo

contrattualmente definito.

In ordine agli obblighi previsti in capo all'aggiudicatario di procedure afferenti agli investimenti pubblici finanziati, in tutto o in parte, con le risorse del Piano Nazionale di Ripresa e Resilienza – PNRR l'appaltatore con la stipula del presente contratto dichiara:

- di aver assolto agli obblighi di cui alla legge 12 marzo 1999, n. 68;
- (qualora operatore economico che occupa un numero pari o superiore a quindici dipendenti e non tenuto alla redazione del rapporto sulla situazione del personale, ai sensi dell'articolo 46 del decreto legislativo 11 aprile 2006, n. 198) di impegnarsi a consegnare alla stazione appaltante, entro sei mesi dalla conclusione del contratto, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta corredata dalla ricevuta di trasmissione della relazione stessa alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità;
- (qualora operatore economico che occupa un numero pari o superiore a quindici dipendenti) di impegnarsi a consegnare alla stazione appaltante, entro sei mesi dalla conclusione del contratto la certificazione di cui all'art. 17 L. 68/99 e una relazione che chiarisca l'avvenuto assolvimento degli obblighi previsti a carico delle imprese dalla legge 12 marzo 1999, n. 68, e illustri eventuali sanzioni e provvedimenti imposti a proprio carico nel triennio precedente la data di scadenza della presentazione delle offerte corredata dalla ricevuta di trasmissione della relazione stessa alle rappresentanze sindacali aziendali;
- (in caso di necessità di effettuare nuove assunzioni per l'esecuzione dello specifico contratto o per la realizzazione di attività ad esso connesse o strumentali) di impegnarsi a destinare almeno la quota del 30% di nuove assunzioni all'occupazione giovanile (persone di età inferiore ai 36 anni);
- (in caso di necessità di effettuare nuove assunzioni per l'esecuzione dello specifico contratto o per la realizzazione di attività ad esso connesse o strumentali) di impegnarsi a destinare almeno la quota del 30% di occupazione femminile;
- di impegnarsi ad assumere l'obbligo di rispettare ogni disposizione impartita in attuazione del PNRR per la gestione, controllo e valutazione della misura, ivi incluso l'obbligo del rispetto del principio di non arrecare un danno significativo all'ambiente (DNSH, "Do no significant harm") incardinato all'art. 17 del Regolamento (UE) 2020/852.

L'Appaltatore deve altresì provvedere, a sua cura e spese e senza diritto di compenso alcuno, ai seguenti adempimenti:

- l'utilizzo di tutte le attrezzature e di personale munito di preparazione professionale e di conoscenza tecnica necessaria per l'esecuzione delle prestazioni oggetto del presente appalto;
- il pagamento delle imposte, tasse, diritti e contributi di qualunque genere inerenti o conseguenti alla stipula del contratto ed all'esecuzione del servizio
- il trasporto e consegna del materiale;
- l'osservanza delle vigenti disposizioni di legge per la prevenzione degli infortuni, l'assistenza e la previdenza dei lavoratori impiegati, nonché la fornitura del materiale di protezione individuale contro gli infortuni, previsto dalle normative vigenti, in particolare dal D. Lgs. n. 81/2008 e s. m. i.;
- l'applicazione nei confronti dei lavoratori dipendenti delle condizioni normative e retributive non inferiori a quelle prescritte dai vigenti contratti collettivi di lavoro applicabili;
- il rispetto degli obblighi in materia di salute e di sicurezza sul lavoro nonché agli obblighi in materia

ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali elencate nell'allegato X alla direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014

Il corrispettivo di tutti i sopra richiamati e specificati obblighi e oneri si intende compreso nella quotazione offerta.

L'Appaltatore sarà in ogni caso tenuto a rifondere gli eventuali danni che, in dipendenza dell'esecuzione della fornitura, fossero arrecati all'Università degli Studi di Salerno.

9. OSSERVANZA DI NORME E PRESCRIZIONI

Il presente appalto è soggetto all'osservanza della normativa vigente in materia di contratti pubblici, delle norme di comportamento dei dipendenti pubblici ex D.P.R. 62/2013 e di tutte le condizioni stabilite nel presente Capitolato e/o in esso richiamate. L'Appaltatore si impegna a osservare e a fare osservare ai propri collaboratori, per quanto compatibili, gli obblighi contenuti nel Codice Etico e di Comportamento dell'Università degli Studi di Salerno (di seguito Codice), emanato con D.R. del 25 ottobre 2017. A tal fine l'Appaltatore di impegna a portare a conoscenza dei propri collaboratori il succitato Codice reperibile nella sezione "Normativa" dei sito web di Ateneo al link: https://web.unisa.it/ateneo/normativa/codice-etico.

10. OBBLIGHI RELATIVI ALLA PREVENZIONE DELLA CORRUZIONE

L'aggiudicatario dovrà attenersi a tutti gli obblighi relativi alla prevenzione della corruzione ed in particolare ai seguenti:

a. Comunicare un proprio indirizzo e-mail o PEC e un proprio recapito telefonico;
b. Non offrire, accettare o richiedere somme di denaro o qualsiasi altro ricompensa vantaggio o beneficio sia direttamente che indirettamente tramite intermediari al fine del rilascio del provvedimento, o al fine di distorcere l'espletamento corretto della successiva attività o valutazione da parte dell'amministrazione;
c. Denunciare immediatamente alle Forze di Polizia ogni illecita richiesta di denaro o altra utilità ovvero offerta di protezione o estorsione di qualsiasi natura che venga avanzata nei confronti di propri rappresentanti o dipendenti, di familiari dell'imprenditore o di eventuali soggetti legati all'impresa da rapporti professionali;
d. Comunicare ogni variazione delle informazioni riportate nei certificati camerali concernenti la compagine sociale;
e. Indicare eventuali relazioni di parentela o affinità sussistenti tra i titolari, gli amministratori, i soci e i dipendenti degli stessi soggetti e dirigenti e i dipendenti dell'amministrazione.

La violazione degli obblighi di cui alle lettere b), c), d) ed e) può costituire causa di risoluzione dell'affidamento, previa contestazione per iscritto assegnando un termine non superiore a dieci giorni per la presentazione di eventuali controdeduzioni. Ove queste non fossero presentate o risultassero non accoglibili, l'Amministrazione procederà alla risoluzione del contratto, fatto salvo il risarcimento dei danni.

11. ESTENSIONE OBBLIGHI DI CONDOTTA PREVISTI DAL CODICE DI COMPORTAMENTO DEI DIPENDENTI PUBBLICI – CLAUSOLA DI RISOLUZIONE.

Ai sensi del comma 3, dell'articolo 2 del D.P.R. 16 aprile 2013, n. 62, gli obblighi di condotta previsti dal "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del d.lgs. 30 marzo 2001, n. 165", in quanto compatibili, sono estesi nei confronti dei collaboratori a qualsiasi titolo dell'Aggiudicatario e delle eventuali imprese subappaltatrici.

La violazione degli obblighi derivanti dal suddetto codice, se ed in quanto compatibili e quindi applicabili, può costituire causa di risoluzione dell'affidamento, previa controdeduzione per iscritto assegnando un termine non superiore a dieci giorni per la presentazione di eventuali controdeduzioni. Ove queste non fossero presentate o risultassero non accoglibili, l'Amministrazione procederà alla risoluzione del contratto, fatto salvo il risarcimento danni.

12. ESTENSIONE OBBLIGHI DI CONDOTTA PREVISTI DAL CODICE ETICO DI COMPORTAMENTO DELL'UNIVERSITÀ DEGLI STUDI DI SALERNO – CLAUSOLA DI RISOLUZIONE.

L'impresa è tenuta ad uniformarsi ai principi contenuti nel Codice Etico e di Comportamento dell'Università degli Studi di Salerno, emanato con D.R. del 25 ottobre 2017, consultabile nella sezione "normativa" del sito web di Ateneo al link: http://web.unisa.it/ateneo/normativa/codice-etico.

Costituisce causa di risoluzione del contratto l'inosservanza degli obblighi previsti dal Codice Etico e di Comportamento dell'Università degli Studi di Salerno, accertata dall'autorità disciplinare competente.

13. TRACCIABILITÀ DEI FLUSSI FINANZIARI – L. 136/2010 E S.M.I.

Il presente appalto è assoggettato agli obblighi di tracciabilità dei flussi finanziari di cui alla L. 136/2010, pertanto tutte le transazioni identificate dalla medesima Legge saranno eseguite esclusivamente nel rispetto del predetto disposto normativo.

L'impresa, pertanto, assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della L. 13 agosto 2010, n. 136 e s.m.i., impegnandosi, altresì, a dare immediata comunicazione all'Università e alla Prefettura – Ufficio Territoriale del Governo della Provincia di Salerno della notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria.

L'Impresa ha, altresì, l'obbligo esplicito, pena la risoluzione immediata di diritto dell'affidamento in parola, di inserire negli atti contrattuali sottoscritti con tutti i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, servizi e forniture derivanti dall'esecuzione del servizio in oggetto un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 136/2010.

L'affidamento dell'appalto sarà risolto di diritto in tutti i casi in cui i relativi movimenti finanziari attivati saranno eseguiti in difformità di quanto previsto dall'art. 3 della Legge 136/2010.

14. DIVIETO DI CESSIONE DEL CONTRATTO DISCIPLINA DEI SUBAPPALTI E SUBAFFIDAMENTI

Il subappalto è disciplinato dall'art. 119 del D. Lgs.36/2023 e normativa correlata.

Il concorrente indica le prestazioni che intende subappaltare o concedere in cottimo. In caso di mancata indicazione il subappalto è vietato.

Fatto salvo quanto previsto dall'articolo 120, comma 1, lettera d), la cessione del contratto è nulla. È altresì nullo l'accordo con cui a terzi sia affidata l'integrale esecuzione delle prestazioni o lavorazioni appaltate.

Non si configurano come attività affidate in subappalto quelle di cui all'art. 119, comma 3 del Codice.

In considerazione del disposto di cui all'art. 119, comma 2 del D. Lgs. 31 marzo 2023, n. 36, tenuto conto dell'esigenza di garantire la corretta esecuzione delle prestazioni oggetto dell'appalto, atteso che un eccessivo frazionamento della commessa non assicurerebbe adeguate garanzie di funzionalità, fruibilità e fattibilità degli obiettivi perseguiti, l'affidatario dovrà eseguire direttamente tutte le prestazioni contrattualizzate residuando ai subaffidamenti le prestazioni riconducibili alla logistica

L'aggiudicatario e il subappaltatore sono responsabili in solido nei confronti della stazione appaltante dell'esecuzione delle prestazioni oggetto del contratto di subappalto.

A carico del subappaltatore non devono sussistere le cause di esclusione di cui al Libro II, Parte V, Titolo IV, Capo II del Codice.

15. GARANZIA DEFINITIVA

L'impresa, a garanzia dell'adempimento di tutte le obbligazioni assunte contrattualmente e del risarcimento di eventuali danni derivanti dall'inadempimento delle obbligazioni stesse presta la garanzia definitiva con le modalità ed i termini indicati dall'art. 107 del D. Lgs. 36/2023 e s.m.i.

Detta garanzia, prodotta con firma digitale è allegata in copia al presente atto, per farne parte integrante e sostanziale. L'eventuale incameramento della garanzia avverrà con atto unilaterale dell'Amministrazione senza necessità di dichiarazione giudiziale. L'impresa assume l'obbligo di reintegrare immediatamente la garanzia di cui l'Università abbia dovuto avvalersi in tutto o in parte, durante l'esecuzione del contratto.

16. RECESSO

Fermo restando quanto previsto dagli articoli 88, comma 4-ter e 92, comma 4, del codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n. 159, è in facoltà dell'Università recedere dal contratto con le modalità previste dalla normativa vigente, in qualunque momento previa notifica, fermo il diritto della Impresa al pagamento di quanto prodotto oltre al decimo delle forniture non eseguite, calcolato secondo quanto previsto nell'allegato II.14 del Codice, escluso ogni altro compenso.

L'Amministrazione, inoltre, si riserva la facoltà di recedere dal contratto nell'ipotesi di attivazione ed adesione da parte dell'Ateneo a convenzioni stipulate da Consip S.p.A., nel cui ambito è ricompresa la fornitura in argomento. In tal caso l'amministrazione comunicherà formalmente all'Impresa l'avvenuta adesione alla convenzione stipulata da Consip S.p.A. con un preavviso non inferiore a 20 giorni.

In caso di recesso, l'aggiudicatario ha diritto al pagamento di quanto correttamente eseguito a regola d'arte secondo il corrispettivo e le condizioni di contratto. Si precisa che, indipendentemente dalla percentuale di attività eseguite rispetto all'importo contrattuale, nessun indennizzo sarà dovuto all'Impresa che rinuncia a qualsiasi pretesa risarcitoria, ad ogni ulteriore compenso o indennizzo e/o rimborso.

L'Impresa è tenuta, a non sospendere l'esecuzione del contratto fino alla effettiva attivazione dello stesso in capo all'Impresa aggiudicataria della convenzione Consip, fornendo la collaborazione necessaria al fine di non causare interruzioni della fornitura.

In ogni caso, trova applicazione l'art. 123 del D. Lgs. n. 36/2023.

17. RISOLUZIONE DEL CONTRATTO – CLAUSOLA RISOLUTIVA ESPRESSA

La risoluzione del contratto è disciplinata dall'art. 122 del D. Lgs. 36/2023 e s.m.i.

L'Università si riserva, inoltre, l'insindacabile facoltà di risolvere il contratto, con provvedimento amministrativo, ai sensi e per gli effetti di cui all'art. 1456 c.c., per inosservanze di particolare gravità e/o reiterata violazione delle disposizioni del contratto, del capitolato speciale di appalto, di leggi o regolamenti. La valutazione della gravità dell'inadempimento è di esclusiva competenza dell'Università, che procederà alla risoluzione del contratto qualora:

1. l'impresa, diffidata due volte per iscritto, persista nell'inadempienza contrattuale contestata;
2. l'applicazione delle penali raggiunga un importo superiore al 10% dell'importo contrattuale al netto di IVA;
3. l'impresa, in caso di escussione della fideiussione definitiva, non provveda al reintegro del deposito cauzionale entro il termine di 15 giorni naturali, successivi e continui dalla richiesta dell'Università;
4. il documento unico di regolarità contributiva dell'impresa risulti negativo per due volte consecutive;
5. l'impresa reiteri l'inadempimento, commettendo più di tre infrazioni di qualsiasi gravità;
6. l'impresa ceda il medesimo contratto;
7. annullamento dell'aggiudicazione a seguito di provvedimento giudiziale;
8. nell'ipotesi in cui sia intervenuto un provvedimento definitivo che dispone, a carico dell'impresa affidataria, l'applicazione di una o più misure di prevenzione di cui al codice delle leggi antimafia e delle relative misure di prevenzione, ovvero sia intervenuta sentenza di condanna passata in giudicato per i reati di cui all'articolo 80 del D. Lgs. 50/2016 e s.m.i.;
9. Per manifesta incapacità, cattivo andamento ed inefficienze gravi nell'esecuzione della fornitura;

Costituisce, altresì, causa di risoluzione del contratto l'inosservanza degli obblighi previsti dal Codice Etico e di Comportamento dell'Università degli Studi di Salerno, accertata dall'autorità disciplinare competente.

Trova, inoltre, applicazione la clausola risolutiva espressa in tutti i casi in cui i movimenti finanziari attivati per il presente appalto saranno eseguiti in difformità a quanto previsto dall'art. 3 della legge 136/2010. L'appaltatore ha l'obbligo esplicito, pena la risoluzione immediata di diritto del presente contratto, di inserire nei contratti sottoscritti con tutti i subcontraenti della filiera delle imprese a qualsiasi titolo interessare al presente appalto un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla L. 136/2010.

L'Università, verificata l'eventuale violazione, contesta per iscritto il fatto all'impresa assegnandogli un termine non superiore a dieci giorni per la presentazione di eventuali controdeduzioni. Ove queste non fossero presentate o risultassero non accogliibili, l'Università procederà alla risoluzione del contratto senza che all'impresa spetti alcun indennizzo o compenso aggiuntivo.

La risoluzione del contratto produrrà i propri effetti dalla ricezione, da parte dell'impresa della comunicazione di risoluzione, inviata tramite PEC.

In tutte le ipotesi l'Università procederà ad incamerare l'intero importo della garanzia definitiva, a titolo di risarcimento forfettario dei danni, fatta salva la facoltà di procedere nei confronti dell'affidatario per tutti gli oneri conseguenti e derivanti dalla risoluzione contrattuale, compresi i maggiori oneri contrattuali eventualmente sostenuti dall'Università e conseguenti a quelli derivanti dal nuovo rapporto contrattuale.

Si darà luogo alla risoluzione del contratto con le modalità e le procedure previste dal D. Lgs.50/2016 e s.m.i.

18. PREVIDENZA E SICUREZZA SUL LAVORO

L'Appaltatore è tenuto ad osservare integralmente, a favore del proprio personale dipendente, le disposizioni previste dal contratto collettivo di lavoro, nonché la normativa in materia di sicurezza sul lavoro, assicurazione e previdenza sociale.

L'Università potrà in qualsiasi momento – per tutto il periodo contrattuale – chiedere copia dei versamenti contributivi, previdenziali ed assicurativi, senza che l'Appaltatore possa sollevare eccezione alcuna.

Resta stabilito che l'inadempienza a ciascuno di tali obblighi comporterà la decadenza immediata dall'aggiudicazione dell'appalto e ciò senza pregiudizio del risarcimento di tutti i danni che potranno derivare all'Università degli Studi di Salerno per la ritardata o mancata esecuzione della fornitura.

19. RUP E DIRETTORE DELL'ESECUZIONE

L'esecuzione del contratto è diretta dal RUP (Responsabile Unico del Progetto), il quale si avvale del Direttore dell'esecuzione del contratto per la verifica del regolare andamento dell'esecuzione del contratto da parte dell'Appaltatore.

Il Direttore dell'esecuzione del contratto provvede al coordinamento, alla direzione e al controllo tecnico-contabile dell'esecuzione del contratto stipulato dall'Università degli Studi di Salerno. Inoltre, assicura la regolare esecuzione del contratto da parte dell'Appaltatore, verificando che le attività e le prestazioni contrattuali siano eseguite in conformità ai documenti contrattuali. A tale fine, il Direttore dell'esecuzione del contratto svolge tutte le attività allo stesso espressamente demandate dal presente Capitolato, nonché tutte le attività che si rendano opportune per assicurare il perseguimento dei compiti a questo assegnati.

20. VERIFICA DI CONFORMITA'

La verifica di conformità sarà effettuata dal Responsabile Unico del Progetto secondo le disposizioni dell'art. 116 del D. Lgs. 36/2023 e dell'allegato II.14 "Direzione dei lavori e direzione dell'esecuzione dei contratti. Modalità di svolgimento delle attività della fase esecutiva. Collaudo e verifica di conformità"

21. GIURISDIZIONE ORDINARIA

Qualsiasi controversia insorgesse che non risulti composta in contraddittorio, sarà deferita alla competenza dell'Autorità giudiziaria del Foro di competenza della Stazione Appaltante rimanendo esclusa la competenza arbitrale.

22. NORME FINALI

Per tutto quanto non specificato dal presente Capitolato speciale di appalto, si fa espresso rinvio a quanto previsto dalle norme e disposizioni vigenti in materia, e degli altri documenti di gara.

23. TRATTAMENTO DEI DATI PERSONALI E TUTELA DELLA RISERVATEZZA

Il trattamento dei dati è disciplinato dal Regolamento UE 2016/679 – Regolamento Generale sulla Protezione dei Dati. Secondo la normativa indicata, il trattamento dei dati personali sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti riconosciuti dal predetto disposto normativo. Il "Titolare" del trattamento è il Rettore p. t. dell'Università degli Studi di Salerno domiciliato per la carica in via Giovanni Paolo II, 132 Fisciano (SA); e-mail: rettore@unisa.it PEC: ammicent@pec.unisa.it. Il Responsabile del trattamento, nominato ai sensi dell'art. 37 del Regolamento UE 2016/679, è il dott. Attilio Riggio, dirigente dell'Area II "Affari Generali" dell'Università degli Studi di Salerno, e può essere contattato ai seguenti indirizzi mail: protezionedati@unisa.it, protezionedati@pec.unisa.it. Il trattamento dei dati personali forniti per la presente procedura è finalizzato esclusivamente a:

- svolgimento di tutte le attività necessarie per consentire la partecipazione alla procedura e per le finalità connesse all'aggiudicazione della presente procedura;
- adempimento degli obblighi di legge e contrattuali;
- adempimento di tutte le attività necessarie alla conclusione del Contratto;
- gestione di eventuali reclami e o contenziosi;
- prevenzione/repressione di frodi e di qualsiasi attività illecita.

I destinatari dei dati forniti sono il Titolare del trattamento e gli eventuali Responsabili del trattamento nominati dal Titolare. I dati personali potranno essere comunicati a tutti i soggetti cui la comunicazione sia necessaria per il corretto adempimento delle finalità innanzi indicate e non saranno soggetti a diffusione.

La determinazione del periodo di conservazione dei dati personali risponde al principio di necessità del trattamento. I dati personali verranno quindi conservati per tutto il periodo necessario allo svolgimento degli scopi innanzi indicati e verranno cancellati e distrutti non appena si renderanno superflui in relazione alle finalità di cui sopra.

Si precisa che in riferimento ai dati personali conferiti, l'interessato è detentore dei seguenti diritti:

1. di accedere ai propri dati personali;
2. di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento;
3. di opporsi al trattamento;
4. alla portabilità dei dati (diritto applicabile ai soli dati in formato elettronico), così come disciplinato dall'art. 20 del Regolamento UE 2016/679;
5. di proporre reclamo all'autorità di controllo (Garante per la protezione dei dati personali).

Per esercitare i diritti sopra riportanti l'interessato potrà rivolgersi al Titolare del trattamento al seguente indirizzo e-mail protezionedati@unisa.it o PEC protezionedati@pec.unisa.it che è tenuto a fornire una risposta entro un mese dalla richiesta.

24. RESPONSABILE UNICO DEL PROGETTO

Ai sensi e per gli effetti dell'art. 15 del D. Lgs. n.36/2023 viene individuato, quale Responsabile Unico del Progetto, Massimo Castaldo Capo dell'Ufficio di coordinamento didattica tel. 089 966140, e-mail mcastaldo@unisa.it

IL RESPONSABILE UNICO DEL PROGETTO
(MASSIMO CASTALDO)