Università degli Studi di Perugia

PNRR: consultazione per la raccolta di proposte progettuali

SCHEDA

Proponente della proposta progettuale	Stefano Bistarelli
Dipartimento/Centro del Proponente/Coordinatore	Dipartimento di Matematica e Informatica,
Dipartimenti/Centri potenzialmente coinvolti	Dipartimento di Ingegneria, Dipartimento di Economia, Dipartimento di Giurisprudenza, Dipartimento di Scienze Politiche, Dipartimento di Filosofia, Scienze Sociali, Umane e della Formazione, Dipartimento di Scienze Agrarie, Alimentari e Ambientali
Eventuali collaborazioni pubbliche e/o private (riportare eventuali partner istituzionali/imprenditoriali coinvolgibili nell'idea progettuale	Sono presenti manifestazione di interesse (oramai raccolte un po' di tempo fa) al progetto da parte di di alcune aziende (elenco non esaustivo): • CyberTechEU • Digi-One • ECSO • Umbria Digitale • Exprivia • MySecurity • Officine Meccaniche Galletti Partecipano inoltre come sponsor o docenza ad alcune delle attivita formative già in essere del progetto (Cyberchallenge): • Digi-One • Micra • Coherentia • Nexus • Tinia • Acta • TS Way • IBM • Exprivia • CyberDivision • CybertechEU • BIP
Titolo (indicativo) della proposta progettuale	Proposta per la costituzione di un Centro per la Ricerca, il Trasferimento Tecnologico e l'Alta Formazione in Cybersecurity, collegato ad un centro di Competenza ed Eccellenza regionale in cybersecurity della regione Umbria (C3U)
Tematica/tematiche di prevalente interesse (max 300 caratteri spazi inclusi)	**Missione 4** Componente 2

	T7: Cybersecurity, nuove tecnologie e tutela dei diritti
Grado di T.R.L di partenza (ove applicabile la scala TRL, descrivere il livello di maturità dell'ipotesi progettuale iniziale facendo riferimento ai gradi e alle declaratorie della scala TRL europea)	Il gruppo puo' esporre sia TRL basso come richiesto dalle azioni di partenariato esteso sia piu' alto necessario in altre iniziative del PNRR
Sintesi (estrema) degli obiettivi e delle possibili ricadute nel territorio locale e/o nazionale (descrivere i principali obiettivi, i risultati attesi e eventuali impatti di ricaduta; max 500 caratteri spazi inclusi)	A livello regionale è già stato approvata la creazione di un centro regionale di competenza per la cybersecurity. All'interno dell'ateneo esiste già un gruppo di ricercatori che afferiscono al Cyberdecurity Research Lab che operano in tale ambito. Esiste un master in Data Protection, Cybersecurity e Digital Forensics che aggrega altri soggetti in tale ambito. L'utilizzo dei fondi PNRR permetterebbero la creazione all'interno dell'ateneo di un centro per la ricerca, il trasferimento tecnologico e l'alta formazione in Cybersecurity.
Costo complessivo del progetto (riportare in k-euro l'ordine di grandezza: 100 k-e, 500 k-e, ...)	Almeno 500K euro all'anno per i primi 4 anni di intervento, oltre ai costi di esercizio per la gestione della sede (portineria, amministrazione, segreteria e spese di funzionamento)
Informazioni aggiuntive (riportare ogni informazione ritenuta utile a rappresentare l'idea progettuale: es. eventuali finanziamenti nazionali/internazionali già ottenuti, eventuali partenariati nazionali/internazionali già consolidati intorno all'ipotesi progettuale; eventuali attività di ricerca commissionata in partenariati pubblico/privati collegati all'idea progettuale; eventuali brevetti collegati; collaborazioni in atto da lunga data etc. – max 500 caratteri spazi inclusi)	Il gruppo ha attivo un laboratorio di ricerca in cybersecurity d'ateneo (anche nodo del laboratorio nazionale cybersecurity del consorzio CINI); Il gruppo ha anche attivo un master in Data Protection, Cybersecurity and Digital Forensics. Obiettivi del Centro saranno quelli di • mettere a disposizione delle imprese e delle pubbliche amministrazioni (**anche per tramite del Centro di eccellenza e Competenza regionale in Cybersecurity (C3U)**) il sistema delle competenze e delle infrastrutture di ricerca, • valorizzare anche a livello nazionale ed europeo il sistema di competenze Universitarie e regionali in materia di cybersecurity e • favorire e promuovere attività di divulgazione per accrescere la conoscenza delle problematiche e delle soluzioni connesse al tema della cybersecurity nell'ambito dei processi di digitalizzazione (awareness). Il Centro mira al raggiungimento dei propri obiettivi in particolare mediante lo svolgimento delle seguenti attività (a titolo esemplificativo e non esaustivo): - divulgazione delle problematiche e delle soluzioni sulla cybersecurity a favore delle imprese e delle pubbliche amministrazioni; - supporto tecnico scientifico alle imprese, agli organismi di ricerca, alle pubbliche amministrazioni e ai cittadini; - creazione dell'Osservatorio Umbro sulla cybersecurity, in collaborazione con la regione Umbria e le aziende del territorio con competenze in ambito cybersecurity, **anche per tramite del C3U,** per la valutazione e il potenziamento delle capacità di difesa sulla base dei fabbisogni di cybersecurity rilevati dall'osservatorio stesso; - contribuire allo sviluppo di strumenti atti a verificare l'adeguamento degli enti pubblici e privati, dei professionisti e delle imprese al Regolamento UE 2016/679 (GDPR) e fornire il supporto informativo e informatico necessario ad assicurare la sua corretta interpretazione e implementazione;

	- fornire consulenza in merito ai servizi di certificazione del software, uno strumento indispensabile per garantire affidabilità e competitività; - contribuire alla predisposizione di progetti di ricerca e trasferimento tecnologico da presentare su bandi regionali, nazionali e europei; - supportare la Regione Umbria nella definizione dei programmi di finanziamento partendo dall'analisi dei fabbisogni di cybersecurity delle Pubbliche Amministrazioni e delle PMI, anche per tramite del C3U; - collaborare con la Regione Umbria nella predisposizione di programmi di formazione ed educazione in materia di cybersecurity, individuando anche possibili percorsi di alta formazione, di formazione ed educazione in materia; - offrire le proprie competenze in ogni altro settore che rientri nell'ambito della CyberSecurity. Il gruppo di lavoro si è già messo in evidenza anche a livello nazionale per alcune attività intraprese e che saranno perseguite e sviluppate all'interno del centro. In particolare • UniPG è coordinatore di un *gruppo nazionale in Distributed Ledger Technology* che oltre a studiare gli aspetti applicativi della blockchain ne studia le implicazioni in ambito security e privacy. Per questo il gruppo organizza dal 2018 sia un workshop sugli aspetti multidisciplinary della blockchain (primo convegno a Perugia nel febbraio 2018) e un workshop tagliato invece sugli aspetti di Security and Privacy, colocato dal febbraio 2019 con la conferenza italiana di Cybersecurity ITASEC, che ha nello steering commitee il coordinatore (Prof. Stefano Bistarelli) di questa proposta. • UniPG partecipa dal 2019 all'attività *formativa nazionale Cyberchallenge.it* che nei mesi marzo-maggio forma 20 selezionati studenti negli aspetti du cybersecurity. Nell'edizioni dello scorso anno una selezione dei 20 ha formato due squadre selezionate a Roma per partecipare a dei giochi svoltosi a Singapore, classificandosi 2^ e 3^ nella competizione Capture the Flag (CTF). Nella CTF nazionale inoltre UniPG si è qualificata a livello nazionale settima. • Dal 2020 è stato organizzato un *master di primo livello in Data protection, cybersecurity e digital forensics*, diretto da uno dei proponenti di questo centro (Prof.ssa Stefania Stefanelli) che prevede insegnamenti multidisciplinari in ambito cybersecurity, approfondendone i profili sia legali che informatici. • Dal 2020 è stata attivata la *Huawei ICT Academy* presso l'Università degli Studi di Perugia, nella quale è attualmente erogata attività didattica certificata in materia di Switching and Routing. I corsi di certificazione potranno estendersi anche ad altri settori dell'ICT, inclusa la cybersecurity. • La proposta conta più di 20 ricercatori/docenti aderenti da vari dipartimenti.