



TÈCNIC/A DE SUPORT A LA RECERCA 150-749-044

DADES DE L'OFERTA

Unitat Adscripció	Matemàtiques			
Perfil genèric	Tècnic/a de Grau Mig de Suport a la Recerca			
Tipologia contractual	Obra i Servei	Grup	2	CLT U
Retribució bruta anual	29.389,10 €/anuals (per jornada completa)			
Jornada 20 h./set.	Data Inici: 01/09/2020	Data fi: 31/12/2020	Durada prevista: 4 mesos	

DADES DEL PROJECTE

Nom del projecte	"CARSD, Criptografia Avanzada para afrontar Nuevos retos de la Sociedad Digital"		
Informació del projecte	https://mak.upc.edu/en		
Codi J-02258	Tipus de projecte	PID: Plan I+D (Retos y Excelencia)	

PROCÉS DE SELECCIÓ

Inscripció	Les persones interessades haureu d'omplir el formulari que trobareu a https://seuelectronica.upc.edu/ca/tramits/Convocatoria_i_concursos_personal_recerca_temporal . Les incidències que puguin sorgir durant la inscripció de la candidatura s'han de reportar al correu electrònic: concursos.psr@upc.edu
Termini de presentació de sol·licituds	13 de juliol de 2020
Composició del tribunal	Representant unitat: Javier Herranz Sotoca Suplent: Paz Morillo Bosch Representant del Servei de Personal: Lourdes Moreno de Francisco Representant del Comitè PasL: Per determinar
Data constitució del tribunal	15 de juliol de 2020 a les 13.15 hores a la sala de reunions del Servei de Personal, a la 3a. pl. de l'edifici Vèrtex.
Convocatòria a la prova i/o entrevista	En cas de que el tribunal acordi realitzar proves i/o entrevistes aquestes es realitzaran el dia 20 de juliol de 2020. La comunicació dels candidats/de les candidates preseleccionats/preseleccionades, el lloc i l'hora de realització es comunicarà mitjançant aquesta mateixa web. Les persones candidates han de tenir disponibilitat per dur a terme la prova i/o entrevista mitjançant l'eina informàtica Google-meet.



TÈCNIC/A DE SUPORT A LA RECERCA 150-749-044

Requisits:

- Titulació universitària de grau mitjà; Diplomatura (antiga titulació), Grau Universitari (nova titulació).

Descripció del lloc de treball

Missió

- Implementar i analitzar un nou protocol criptogràfic per a fer desxifrat de clau pública distribuït, amb seguretat post-quàntica.

Funcions a desenvolupar

- Entendre i acabar de detallar la idea teòrica del protocol de desxifrat distribuït (proposat en un Treball Final de Grau) que es pretén implementar.
- Implementar el protocol, utilitzant algun llenguatge de programació i alguna llibreria criptogràfica existent (de les habituals en la implementació de protocols basats en reticles).
- Testejar la implementació obtinguda.
- Escriure un article científic on es descriu i analitzi el nou protocol i la seva implementació.

2

Perfil Professional

- **Estudis :** Matemàtiques i/o Informàtica
- **Especialitat:** Criptografia

Coneixements

- Criptografia.
- Protocols criptogràfics basats en reticles.
- Llenguatges de programació utilitzats en criptografia.
- Català, castellà i anglès parlats, llegits i escrits.

Competències Tècniques

- Estudiar protocols criptogràfics detallats en articles científics.
- Capacitat d'implementar un nou protocol criptogràfic utilitzant llibreries existents especialitzades per a criptografia basada en reticles.
- Capacitat per a realitzar una prova de seguretat matemàtica d'un protocol criptogràfic nou.
- Habilitat per a l'escriptura d'articles científics.



TÈCNIC/A DE SUPORT A LA RECERCA 150-749-044

Competències Organitzatives

- Capacitat de treball en equip.

Competències Personals

- Capacitat per exposar de manera oral i escrita nous resultats científics.

Experiència Professional

- No requerida.

Etapes de la carrera professional

(s'indica amb una creu l'opció seleccionada)

<input type="checkbox"/>	Sense experiència prèvia
<input checked="" type="checkbox"/>	Etapa primerenca menys de 4 anys
<input type="checkbox"/>	Experiència entre 4 i 10 anys
<input type="checkbox"/>	Experiència de més de 10 anys

Perfil de recerca

(s'indica amb una creu l'opció seleccionada)

<input checked="" type="checkbox"/>	Primera etapa
<input type="checkbox"/>	Professional reconegut
<input type="checkbox"/>	Professional establert
<input type="checkbox"/>	Líder de projectes

Aquest contracte serà finançat pel Ministerio de Ciencia, Innovación y Universidades (MCIU), a la Agencia Estatal de Investigación (AEI) y al Fondo Europeo de Desarrollo Regional FEDER), títol del projecte: "CARSD, Criptografía Avanzada para afrontar Nuevos retos de la Sociedad Digital" - referencia MTM2016-77213-R.