QUADRE DE CARACTERÍSTIQUES ADMINISTRATIVES I TÈCNIQUES
Subministrament de servei: Acció formativa en Ciberseguretat: credencials, contrasenyes, claus i vulnerabilitats (Categoria 2 del SDA)

1. Objecte del contracte. Codi CPV. Termini de lliurament

Objecte:

Contractació del servei d'una acció formativa per desenvolupar competències avançades en ciberseguretat, amb un enfocament pràctic orientat a la gestió de credencials, contrasenyes, claus criptogràfiques i vulnerabilitats per l'equip de Tecnologia de l'IL3-UB.

Acció formativa que té com a objectiu capacitar les persones participants que són professionals de Tecnologia en els principis i bones pràctiques de la ciberseguretat relacionades amb la gestió de credencials digitals, contrasenyes, claus d'accés i la identificació de vulnerabilitats habituals. S'abordaran els riscos associats a una gestió inadequada de la informació d'accés, així com les mesures per protegir-se davant d'atacs cibernètics com el phishing, l'ús de contrasenyes febles o la reutilització de credencials.

El curs combina continguts teòrics amb casos pràctics per fomentar la consciència i la responsabilitat digital dels usuaris i contribuir a la protecció global dels sistemes d'informació de l'organització.

L'objectiu és desenvolupar competències avançades en seguretat informàtica, centrant-se en el tractament de credencials, la minimització de l'ús de contrasenyes, l'ús de claus ibiometria, l'explotació de vulnerabilitats, i la prevenció bàsica de la seguretat.

Codi CPV: 79632000-3 Servicios de formación de personal.

Termini d'execució: a mitjans mes de novembre de 2025 en horari matins.

Nombre de grups: 1 grup

Durada total: 15 hores

Modalitat: Mixta (3 sessions presencials + 2 sessions virtuals)

Calendari proposat:

Presencials: **17, 24 de novembre i 01 de desembre** (de 9.30 a 12.30 h)

Virtuals (Aula virtual): **qualsevol de les marcades en color blau en el calendari proposat** (de 9.30 a 12.30 h)

Nombre de participants: grup únic reduït, màxim 15 persones.

Novembre

Lu.	Ma.	Mi.	Ju.	Vi.	Sá.	Do.
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

DICIEMBRE

Lu.	Ma.	Mi.	Ju.	Vi.	Sá.	Do.
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

dates possibles formació presencial
dates possibles formació online

2. Import i pressupost base de la licitació

Justificació del preu: s'ha realitzat una consulta amb diferents empreses del sector valorant les possibilitats.

El pressupost base de la licitació es de 4.114,00 €, IVA inclòs, sent el 3.400,00 € la base imposable i 714,00 € d'IVA, tenint en compte que la durada serà :

Nom	Quantitat	Preu unitari 1 grup (màx.15 persones)	Preu total 1 grup
Acció formativa en Ciberseguretat: credencials, contrasenyes, claus i vulnerabilitats	15 hores	226,67 €/hora	3.400,00 €

3. Plurianualitats

Es contratarà un curs de 15 hores en total per tot el personal de Tecnologia es farà un sol grups de màxim 15 persones.

Any	**Import**
2025	3.400,00 €

4. Valor estimat del contracte

El valor estimat del contracte per un any serà de 3.400,00 € IVA exclòs.

5. Garantia definitiva

D'acord amb el valor estimat del contracte i l'article 159.6.f) de la LCSP, en els contractes específics dins del sistema dinàmic d'adquisició no es requereix la constitució de garantia definitiva

6. Lloc i forma de pagament

Es farà un únic pagament, un cop finalitzada la presetació del servei de formació, objecte d'aquest contracte, prèvia presentació de la factura, i comprovades la correcció i finalització d'aquest servei.

7. Criteris de valoració

7.1. Criteris que dependent d'un judici de valor – 40 punts

Els licitadors hauran d'aportar una fitxa técnica descriptiva acomodada a les prescripcions tècniques especificant la informació demanada a la taula següent de criteris subjectius que depenen d'un judici de valor, el més detalladament possible, de com a màxim de 5 pàgines inclosos portada, índex i annexos amb lletra Arial 10, interlineat 1,5, que haurà d'incloure:

Criteris	Puntuació màxima
Objectius i Contingut del pla docent, breu descripció dels objectius del curs així com del contingut del mateix d'acord amb les característiques tècniques exposades en el punt 9.	Descripció complerta i que s'ajusta al que es demana .....20 Descripció incomplerta i que s'ajusta al que es demana.....10 Descripció incomplerta i que no s'ajusta al que es demana.....0
Metodologia: Breu explicació de l'enfocament pedagògic del curs d'acord amb les característiques tècniques exposades en el punt 9.	Descripció complerta i que s'ajusta al que es demana .....20 Descripció incomplerta i que s'ajusta al que es demana.....10 Descripció incomplerta i que no s'ajusta al que es demana.....0

7.2. Criteris objectius, avaluables mitjançant fórmula automàtica – 60 punts.

54 Punts.- Mitjançant preu: s'atorgarà la màxima puntuació a les proposicions que ofereixen el preu més baix. La resta serà de manera proporcional tenint en compte la següent fórmula.

FÓRMULA:

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 54\ punts$$

Millores: -6 punts

Per tal de garantir la màxima qualitat en la prestació del servei, es valoraran les següents millores:

Referències (fins a 3 punts)

Bones referències documentades amb contactes o informes d'altres clients en formació en Ciberseguretat.

Experiència acreditada	Descripció	Punts
Alta (≥ 5 referències)	Aporta referències d'altres clients en formació en Ciberseguretat.	3 punts
Mitjana (3-4 referències)	Aporta referències d'altres clients en formació en Ciberseguretat.	2 punts
Baixa (1-2 referències)	Aporta alguna referència d'altes clients en formació en Ciberseguretat.	1 punts

Experiència acreditada	Descripció	Punts
Sense referències	No aporta referències d'altres clients en formació en Ciberseguretat.	0 punts

Especialització del formador/a (fins a 3 punts)

Grau d'especialització en la temàtica concreta del curs, tant en coneixements pràctics com en competències pedagògiques per a especialistes tecnòlegs. L 'experiència del formador es demostri amb CV, certificats o informes de formació impartida.

Criteris de valoració:

Experiència acreditada	Descripció	Punts
Alta (≥ 5 accions)	Ha impartit 5 o més accions formatives centrades específicament en ciberseguretat per a tecnòlegs en els darrers 3 anys.	3 punts
Mitjana (3-4 accions)	Ha impartit entre 3 i 4 accions específica en formació sobre ciberseguretat per a tecnòlegs en els darrers 3 anys.	2 punts
Baixa (1-2 accions)	Ha impartit 1 o 2 específica en formació sobre ciberseguretat per a tecnòlegs.	1 punts
Sense experiència específica	No s'acredita experiència específica en formació sobre ciberseguretat per a tecnòlegs.	0 punts

8. Criteris per considerar l'oferta anormalment baixa

La determinació de les ofertes que presentin uns valors anormalment baixos s'ha de dur a terme en funció dels límits i els paràmetres objectius establerts a continuació.

1. Si concorre una única licitadora, es considera anormalment baixa l'oferta que sigui un 35% més baixa que el pressupost de licitació.

2. Si concorren dues empreses licitadores, es considera anormalment baixa l'oferta que compleixi els dos criteris següents:
   - Que el preu ofert per una de les empreses és inferior en més d'un 20% al preu ofert per l'altra oferta.
   - Que el sumatori de la puntuació que li correspongui en la resta de criteris d'adjudicació diferents del preu sigui superior en més d'un 20% a la puntuació de l'altra empresa.

3. Si concorren tres o més empreses licitadores, es considera anormalment baixa l'oferta que compleixi els dos criteris següent:

- Que la puntuació que li correspongui en l'oferta econòmica sigui superior en més d'un 20% a la mitjana aritmètica de les puntuacions de totes les ofertes econòmiques presentades. No obstant això, quan hi concorrin tres empreses licitadores, per al còmput de la mitjana s'ha d'excloure l'oferta econòmica que sigui d'una quantia superior en més de 15% a la mitjana.
- Que la puntuació que li correspongui en la resta de criteris d'adjudicació diferents del preu, sigui superior a la suma de la mitjana aritmètica de les puntuacions de les ofertes i la desviació mitjana d'aquestes puntuacions.

Per calcular la desviació mitjana de les puntuacions s'obtindrà, per a cada oferta, el valor absolut de la diferència entre la seva puntuació i la mitjana aritmètica de les puntuacions de totes les ofertes. La desviació mitjana de les puntuacions és igual a la mitjana aritmètica d'aquests valors absoluts.

4. De la mateixa manera, quan hi concorrin quatre empreses licitadores o més, si hi ha ofertes econòmiques superiors a la mitjana en més de 15%, s'ha de calcular una nova mitjana només amb les ofertes que no estiguin en el cas indicat. En tot cas, si el nombre de les altres ofertes és inferior a tres, la nova mitjana s'ha de calcular sobre les tres ofertes de menor quantia.

9. Característiques tècniques

Objectius del curs:

- ✓ Aplicar bones pràctiques en la gestió segura de credencials i claus.
- ✓ Minimitzar l'ús insegur de contrasenyes i fomentar alternatives robustes.
- ✓ Detectar i explotar vulnerabilitats amb eines de pentesting (Kali Linux).
- ✓ Configurar sistemes de doble autenticació amb claus FIDO2 i biometria.
- ✓ Desenvolupar plans bàsics de seguretat, recuperació i contingència.

Estem pensant en una formació per l'equip de Tecnològia, equip de SAU-Sistemes, Desenvolupament i Qualitat- programació i infraestructures TIC d'IL3-UB, Tecnologia .

Total hores curs: 15 hores. Diferents sessions
Modalitat: Mixta
Número de participants: màxim 15.

Temari proposat:

Bloc 1: Tractament de credencials

- Temps necessari per trencar una credencial: CPU, GPU, ASIC's.
- Mètodes mnemotècnics per generar una password segura.
- Temps de vida, polítiques, Levenshtein.
- Group Policy Management
- **Pràctica:** creació de polítiques de contrasenyes

Bloc 2: Minimització de l'ús de contrasenyes

- La caixa forta al núvol.
- Accés des de PC i mòbil.
- Principals fonts de problemes greus i com solucionar-los
- Exportació de contrasenyes amb JSON i posterior xifrat amb GPG AES-256.
- Creació d'espais amb Veracrypt
- Utilització de 7-Zip amb AES-256
- **Pràctica:** creació d'espais xifrats (USB, fitxers i particions)

Bloc 3: Explotació de vulnerabilitats

- Hardware específic
- Tècniques de vulnerabilitat
- Atacs i Captura de trànsit
- **Pràctica:** configuració de laboratori amb antenes, GPU, handshake capture, diccionaris
- Hardware específic per muntar laboratori de penetració WiFi: Antenes, GPU.
- Treure contrasenya d'un sistema per vulnerabilitat (amb tècniques de Pixie Dust)
- Atac amb man-in-the-middle desautoritzant estació víctima.
- Atac silenciós occult amb captura del handshake, verificación del mateix, ús de les GPU's per força bruta
- Diccionaris i Tunning dels mateixos

Bloc 4: Claus criptogràfiques FIDO2 i biometria

- Diferències entre FIDO U2F (antic) i FIDO2 (modern)
- El doble factor mitjançant Device-Smartphone (no SMS, no e-mail...)
- Quines son les tendències actuals i cap a on apunta el futur de l'autenticació?
- **Pràctica:** configuració pràctica amb claus FIDO2

Bloc 5: Prevenció bàsica de la seguretat

- Disaster recovery
- Pla de contingència
- Pla de recuperació
- Tornar a la normalitat
- Failover y Switchover
- **Gestió d'incidències de seguretat informàtica** com actuar davant d'una sospita en una infecció en un equip, com identificar les causes més comuns, i amb quines eines poden comptar per detecció i anàlisis, protocols d'actuació, mesures inicials necessàries per contenir i resoldre l'incident de manera correcta i segura.

Metodologia

- Sessions demostratives i participatives
- Enfocament pràctic amb resolució de casos reals i simulacions
- Aprenentatge per descobriment, amb accés a recursos multimèdia (vídeos, tutorials, etc.)
- Tutoria asíncrona

Material i recursos

L'empresa posarà a disposició de l'alumnat ordinadors portàtils amb **Windows 11** i les característiques següents:

- Processador **CPU de 10a generació o superior**
- **16 GB de memòria RAM**
- **Disc dur de 512 GB**

Per la seva part, l'**empresa proveïdora** haurà d'aportar tot el material addicional necessari per al correcte desenvolupament de la formació, garantint que els participants disposin dels recursos adequats per realitzar les activitats i assolir els objectius establerts.

A més de altre material per completar la formació com :

- Dossier digital
- Videotutorials i manuals
- Guies per pràctiques tècniques

Sessions pràctiques amb exercicis en directe.

✔ Explicacions clares amb exemples del dia a dia laboral.

✔ Materials de suport (guies PDF i videotutorials).

✔ Resolució de dubtes en directe amb els participants.

Formador/a

- Titulació en informàtica, telecomunicacions, enginyeria o camps afins.
- Experiència demostrable en ciberseguretat (mínim 3 anys).
- Experiència en formació d'adults (preferentment en l'àmbit públic o empresarial).

Format: Sessions presencials mixtes , presencial i online per facilitar la participació, es podría combinar formació teórica online amb formació práctica presencial en els grups híbrits i online.

Durada: 15 hores en total, la modalitat híbrida que combini teoría amb práctica presencial per pràcticar exercicis, la sessió online que també combini teoría amb práctica.

Participants: Grups reduïts (màxim 15 persones) per afavorir un aprenentatge interactiu i personalitzat. Número total de participants:15.

10. Obligacions de l'adjudicatari.

Compliment del calendari i adaptabilitat:

- L'adjudicatari haurà d'adaptar-se a les dates proposades per l'organització dins del període de **la segona de noviembre i desembre**, per un sol grup.
- En cas que, per causes justificades, no sigui possible impartir la formació en les dates convingudes, haurà de proposar **dates alternatives abans del 20 de desembre de 2025.**

Formació personalitzada i adaptada a les necessitats de l'organització:

- El contingut i la metodologia de la formació han d'estar **adaptats al perfil dels participants** i **a les necessitats específiques de l'empresa**.
- **Format flexible i interactiu:**

- La formació ha de tenir un **format d'impartició mixta, presencial i online**, segons el que es concreti, però garantint sempre un **enfocament pràctic i participatiu**.
- Es valorarà que la formació estigui estructurada en **mòduls curts**, amb possibilitat de combinar teoria i pràctica.

Materials de suport:

- S'han de proporcionar **materials formatius** com ara guies en PDF, videotutorials o altres recursos útils per a la consulta posterior, simuladors, entorns virtuals, accés a plataformes.

Qualitat tècnica i pedagògica:

- El/la formador/a ha de tenir **experiència demostrable en l'àmbit de ciberseguretat per a professionals de la tecnologia** i en formació a professionals.

Grups reduïts per facilitar l'aprenentatge:

- La formació s'ha de fer en un sol **grup de màxim 15 persones**, tal com es preveu.

Avaluació i seguiment:

- L'adjudicatari haurà d'incloure mecanismes de **valoració de la satisfacció** i **seguiment dels resultats de la formació**.

Substitucions i incidències:

L'adjudicatari haurà de substituir el formador/a en cas de força major amb una persona amb igual o superior qualificació, amb autorització prèvia de l'organisme contractant.

En cas d'incompliment reiterat, l'organisme podrà rescindir el contracte sense dret a indemnització.

Barcelona, 19 de setembre de 2025

Sra. Silvia Estela
Tècnica que promou la necessitat
Tècnica de RRH
Fundació Institut de Formació Contínua de la Universitat de Barcelona (IL3-UB)

Sr. David Martínez
Responsable del pressupost
Responsable RRHH
Fundació Institut de Formació Contínua (IL3-UB)