CUADRO DE CARACTERÍSTICAS ADMINISTRATIVAS Y TÉCNICAS
Suministro de servicio: Acción formativa en Ciberseguridad: credenciales, contraseñas, claves y vulnerabilidades (Categoría 2 del SDA)

1. Objeto del contrato. Código CPV. Plazo de entrega

Objeto:

Contratación del servicio de una acción formativa para desarrollar competencias avanzadas en ciberseguridad, con un enfoque práctico orientado a la gestión de credenciales, contraseñas, claves criptográficas y vulnerabilidades por el equipo de Tecnología del IL3-UB.

Acción formativa que tiene como objetivo capacitar a las personas participantes que son profesionales de Tecnología en los principios y buenas prácticas de la ciberseguridad relacionadas con la gestión de credenciales digitales, contraseñas, claves de acceso y la identificación de vulnerabilidades habituales. Se abordarán los riesgos asociados a una gestión inadecuada de la información de acceso, así como las medidas para protegerse ante ataques cibernéticos como el phishing, el uso de contraseñas débiles o la reutilización de credenciales.

El curso combina contenidos teóricos con casos prácticos para fomentar la conciencia y la responsabilidad digital de los usuarios y contribuir a la protección global de los sistemas de información de la organización.

El objetivo es desarrollar competencias avanzadas en seguridad informática, centrándose en el tratamiento de credenciales, la minimización del uso de contraseñas, el uso de llaves ibiometría, la explotación de vulnerabilidades, y la prevención básica de la seguridad.

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

Plazo de ejecución: a mediados del mes de noviembre de 2025 en horario mañanas.

Número de grupos: 1 grupo

Duración total: 15 horas

Modalidad: Mixta (3 sesiones presenciales + 2 sesiones virtuales)

Calendario propuesto:

Presenciales: **17, 24 de noviembre y 01 de diciembre** (de 9.30 a 12.30 h)

Virtuales (Aula virtual): **cualquiera de las marcadas en color azul en el calendario propuesto** (de 9.30 a 12.30 h)

Número de participantes: grupo único reducido, máximo 15 personas.

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. Importe y presupuesto base de la licitación

Justificación del precio: se ha realizado una consulta con diferentes empresas del sector valorando las posibilidades.

El presupuesto base de la licitación es de 4.114,00 €, IVA incluido, siendo el 3.400,00 € la base imponible y 714,00 € de IVA, teniendo en cuenta que la duración será :

Nombre	Cantidad	Precio unitario 1 grupo (máx.15 personas)	Precio total 1 grupo
Acción formativa en Ciberseguridad: credenciales, contraseñas, claves y vulnerabilidades	15 horas	226,67 €/hora	3.400,00 €

3. Plurianualidades

Se contratará un curso de 15 horas en total para todo el personal de Tecnología se hará un solo grupo de máximo 15 personas.

Año	**Importe**
2025	3.400,00 €

4. Valor estimado del contrato

El valor estimado del contrato por un año será de 3.400,00 € IVA excluido.

5. Garantía definitiva

De acuerdo con el valor estimado del contrato y el artículo 159.6.f) de la LCSP, en los contratos específicos dentro del sistema dinámico de adquisición no se requiere la constitución de garantía definitiva

6. Lugar y forma de pago

Se hará un único pago, una vez finalizada la presetación del servicio de formación, objeto de este contrato, previa presentación de la factura, y comprobadas la corrección y finalización de este servicio.

7. Criterios de valoración

7.1. Criterios que dependiente de un juicio de valor – 40 puntos

Los licitadores deberán aportar una ficha técnica descriptiva acomodada a las prescripciones técnicas especificando la información solicitada en la tabla siguiente de criterios subjetivos que dependen de un juicio de valor, lo más detalladamente posible, de como máximo de 5 páginas incluidos portada, índice y anexos con letra Arial 10, interlineado 1,5, que deberá incluir:

Criterios	**Puntuación máxima**
Objetivos y Contenido del plan docente, breve	Descripción completa y que se ajusta a lo que se pide 20

descripción de los objetivos del curso así como del contenido del mismo de acuerdo con las características técnicas expuestas en el punto 9.	Descripción incumplida y que se ajusta a lo solicitado..... 10 Descripción incumplida y que no se ajusta a lo solicitado..... 0
Metodología: Breve explicación del enfoque pedagógico del curso de acuerdo con las características técnicas expuestas en el punto 9.	Descripción completa y que se ajusta a lo que se pide ..... 20 Descripción incumplida y que se ajusta a lo solicitado..... 10 Descripción incumplida y que no se ajusta a lo solicitado..... 0

7.2. Criterios objetivos, evaluables mediante fórmula automática – 60 puntos

54 Puntos.- Mediante precio: se otorgará la máxima puntuación a las proposiciones que ofrecen el precio más bajo. El resto será de manera proporcional teniendo en cuenta la siguiente fórmula.

FÓRMULA:

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

Mejoras: -6 puntos

Con el fin de garantizar la máxima calidad en la prestación del servicio, se valorarán las siguientes mejoras:

Referencias (hasta 3 puntos)

Buenas referencias documentadas con contactos o informes de otros clientes en formación en Ciberseguridad.

Experiencia acreditada	Descripción	Puntos
Alta (≥ 5 referencias)	Aporta referencias de otros clientes en formación en Ciberseguridad.	3 puntos
Media (3-4 referencias)	Aporta referencias de otros clientes en formación en Ciberseguridad.	2 puntos
Baja (1-2 referencias)	Aporta alguna referencia de altos clientes en formación en Ciberseguridad.	1 puntos
Sin referencias	No aporta referencias de otros clientes en formación en Ciberseguridad.	0 puntos

Especialización del formador/a (hasta 3 puntos)

Grado de especialización en la temática concreta del curso, tanto en conocimientos prácticos como en competencias pedagógicas para especialistas tecnólogos. La experiencia del formador se demuestre con CV, certificados o informes de formación impartida.

Criterios de valoración:

Experiencia acreditada	Descripción	Puntos
Alta (≥ 5 acciones)	Ha impartido 5 o más acciones formativas centradas específicamente en ciberseguridad para tecnólogos en los últimos 3 años.	3 puntos
Media (3-4 acciones)	Ha impartido entre 3 y 4 acciones específica en formación sobre ciberseguridad para tecnólogos en los últimos 3 años.	2 puntos
Baja (1-2 acciones)	Ha impartido 1 o 2 específica en formación sobre ciberseguridad para tecnólogos.	1 puntos
Sin experiencia específica	No se acredita experiencia específica en formación sobre ciberseguridad para tecnólogos.	0 puntos

8. Criterios para considerar la oferta anormalmente baja

La determinación de las ofertas que presenten unos valores anormalmente bajos debe llevarse a cabo en función de los límites y parámetros objetivos establecidos a continuación.

1. Si concurre una única licitadora, se considera anormalmente baja la oferta que sea un 35% más baja que el presupuesto de licitación.

2. Si concurren dos empresas licitadoras, se considera anormalmente baja la oferta que cumpla los dos criterios siguientes:
   - Que el precio ofrecido por una de las empresas es inferior en más de un 20% al precio ofrecido por la otra oferta.
   - Que el sumatorio de la puntuación que le corresponda en el resto de criterios de adjudicación diferentes del precio sea superior en más de un 20% a la puntuación de la otra empresa.

3. Si concurren tres o más empresas licitadoras, se considera anormalmente baja la oferta que cumpla los dos criterios siguientes:
   - Que la puntuación que le corresponda en la oferta económica sea superior en más de un 20% a la media aritmética de las puntuaciones de todas las ofertas económicas presentadas. No obstante, cuando concurran tres empresas licitadoras, para el cómputo de la media se debe excluir la oferta económica que sea de una cuantía superior en más de 15% a la media.
   - Que la puntuación que le corresponda en el resto de criterios de adjudicación distintos del precio, sea superior a la suma de la media aritmética de las puntuaciones de las ofertas y la desviación media de estas puntuaciones.

Para calcular la desviación media de las puntuaciones se obtendrá, para cada oferta, el valor absoluto de la diferencia entre su puntuación y la media aritmética de las puntuaciones de todas las ofertas. La desviación media de las puntuaciones es igual a la media aritmética de estos valores absolutos.

4. Del mismo modo, cuando concurran cuatro empresas licitadoras o más, si hay ofertas económicas superiores a la media en más de 15%, se calculará una nueva media sólo con las ofertas que no estén en el caso indicado. En todo caso, si el número de las otras ofertas es inferior a tres, la nueva media debe calcularse sobre las tres ofertas de menor cuantía.

9. Características técnicas

Objetivos del curso:

- ✓ Aplicar buenas prácticas en la gestión segura de credenciales y claves.
- ✓ Minimizar el uso inseguro de contraseñas y fomentar alternativas robustas.
- ✓ Detectar y explotar vulnerabilidades con herramientas de pentesting (Kali Linux).
- ✓ Configurar sistemas de doble autenticación con claves FIDO2 y biometría.
- ✓ Desarrollar planes básicos de seguridad, recuperación y contingencia.

Estamos pensando en una formación para el equipo de Tecnològia, equipo de SAU-Sistemas, Desarrollo y Calidad- programación e infraestructuras TIC de IL3-UB, Tecnología .

Total horas curso: 15 horas. Diferentes sesiones
Modalidad: Mixta
Número de participantes: máximo 15.

Temario propuesto:

Bloque 1: Tratamiento de credenciales

- Tiempo necesario para romper una credencial: CPU, GPU, ASIC's.
- Métodos mnemotécnicos para generar un password seguro.
- Tiempo de vida, políticas, Levenshtein.
- Group Policy Management
- **Práctica:** creación de políticas de contraseñas

Bloque 2: Minimización del uso de contraseñas

- La caja fuerte en la nube.
- Acceso desde PC y móvil.
- Principales fuentes de problemas graves y cómo solucionarlos
- Exportación de contraseñas con JSON y posterior cifrado con GPG AES-256.
- Creación de espacios con Veracrypt
- Utilización de 7-Zip con AES-256
- **Práctica:** creación de espacios cifrados (USB, ficheros y particiones)

Bloque 3: Explotación de vulnerabilidades

- Hardware específico
- Técnicas de vulnerabilidad
- Ataques y Captura de tráfico
- **Práctica:** configuración de laboratorio con antenas, GPU, handshake capture, diccionarios
- Hardware específico para montar laboratorio de penetración WiFi: Antenas, GPU.
- Sacar contraseña de un sistema por vulnerabilidad (con técnicas de Pixie Dust)
- Ataque con man-in-the-middle desautorizando estación víctima.
- Ataque silencioso occulto con captura del handshake, verificación del mismo, uso de las GPU's por fuerza bruta
- Diccionarios y Tunning de los mismos

Bloque 4: Claves criptográficas FIDO2 y biometría

- Diferencias entre FIDO U2F (antiguo) y FIDO2 (moderno)
- El doble factor mediante Device-Smartphone (no SMS, no e-mail...)
- ¿Cuáles son las tendencias actuales y hacia dónde apunta el futuro de la autenticación?
- **Práctica:** configuración práctica con claves FIDO2

Bloque 5: Prevención básica de la seguridad

- Disaster recovery
- Plan de contingencia
- Plan de recuperación
- Volver a la normalidad
- Failover y Switchover
- **Gestión de incidencias de seguridad informática** como actuar ante una sospecha en una infección en un equipo, cómo identificar las causas más comunes, y con qué herramientas pueden contar para detección y análisis, protocolos de actuación, medidas iniciales necesarias para contener y resolver el incidente de manera correcta y segura.

Metodología

- Sesiones demostrativas y participativas
- Enfoque práctico con resolución de casos reales y simulaciones
- Aprendizaje por descubrimiento, con acceso a recursos multimedia (vídeos, tutoriales, etc.)
- Tutoría asíncrona

Material y recursos

La empresa pondrá a disposición del alumnado ordenadores portátiles con **Windows 11** y las siguientes características:

- Procesador **CPU de 10ª generación o superior**
- **16 GB de memoria RAM**
- **Disco duro de 512 GB**

Por su parte, la **empresa proveedora** deberá aportar todo el material adicional necesario para el correcto desarrollo de la formación, garantizando que los participantes dispongan de los recursos adecuados para realizar las actividades y alcanzar los objetivos establecidos.

Además de otro material para completar la formación como :

- Ascensos digital
- Videotutoriales y manuales
- Guías para prácticas técnicas

Sesiones prácticas con ejercicios en directo.

✔ Explicaciones claras con ejemplos del día a día laboral.

✔ Materiales de soporte (guías PDF y videotutoriales).

✔ Resolución de dudas en directo con los participantes.

Formador/a

- Titulación en informática, telecomunicaciones, ingeniería o campos afines.
- Experiencia demostrable en ciberseguridad (mínimo 3 años).
- Experiencia en formación de adultos (preferentemente en el ámbito público o empresarial).

Formato: Sesiones presenciales mixtas , presencial y online para facilitar la participación, se podría combinar formación teórica online con formación práctica presencial en los grupos híbridos y online.

Duración: 15 horas en total, la modalidad híbrida que combine con práctica presencial para prácticar ejercicios, la sesión online que también combine con práctica.

Participantes: Grupos reducidos (máximo 15 personas) para favorecer un aprendizaje interactivo y personalizado. Número total de participantes:15.

10. Obligaciones del adjudicatario.

Cumplimiento del calendario y adaptabilidad:

- El adjudicatario deberá adaptarse a las fechas propuestas por la organización dentro del periodo de **la segunda de noviembre y diciembre**, por un solo grupo.
- En caso de que, por causas justificadas, no sea posible impartir la formación en las fechas convenidas, deberá proponer **fechas alternativas antes del 20 de diciembre de 2025.**

Formación personalizada y adaptada a las necesidades de la organización:

- El contenido y la metodología de la formación deben estar **adaptados al perfil de los participantes** y **a las necesidades específicas de la empresa**.
- **Formato flexible e interactivo:**

- La formación debe tener un **formato de impartición mixta, presencial y online**, según lo que se concrete, pero garantizando siempre un **enfoque práctico y participativo**.
- Se valorará que la formación esté estructurada en **módulos cortos**, con posibilidad de combinar teoría y práctica.

Materiales de apoyo:

- Se deben proporcionar **materiales formativos** como guías en PDF, videotutoriales u otros recursos útiles para la consulta posterior, simuladores, entornos virtuales, acceso a plataformas.

Calidad técnica y pedagógica:

- El/la formador/a debe tener **experiencia demostrable en el ámbito de ciberseguridad para profesionales de la tecnología** y en formación a profesionales.

Grupos reducidos para facilitar el aprendizaje:

- La formación se realizará en un solo **grupo de máximo 15 personas**, tal y como se prevé.

Evaluación y seguimiento:

- El adjudicatario deberá incluir mecanismos de valoración de **la satisfacción** y **seguimiento de los resultados de la formación**.

Sustituciones e incidencias:

El adjudicatario deberá sustituir al formador/a en caso de fuerza mayor con una persona con igual o superior calificación, con autorización previa del organismo contratante.

En caso de incumplimiento reiterado, el organismo podrá rescindir el contrato sin derecho a indemnización.

Barcelona, 19 de septiembre de 2025

Sra. Silvia Estela
Técnica que promueve la necesidad
Técnica de RRH
Fundación Instituto de Formación Continua de la Universidad de Barcelona (IL3-UB)

D. David Martínez
Responsable del presupuesto
Responsable RRHH
Fundación Instituto de Formación Continua (IL3-UB)