GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

"UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos"

CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

Código: IFC153_3 **NIVEL: 3**

1. ESPECIFICACIONES DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA

Dado que la evaluación de la competencia profesional se basa en la recopilación de pruebas o evidencias de competencia generadas por cada persona candidata, el referente a considerar para la valoración de estas evidencias de competencia (siempre que éstas no se obtengan por observación del desempeño en el puesto de trabajo) es el indicado en los apartados 1.1 y 1.2 de esta GEC, referente que explicita la competencia recogida en las realizaciones profesionales y criterios de realización de la UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos.

1.1. Especificaciones de evaluación relacionadas con las dimensiones de la competencia profesional.

Las especificaciones recogidas en la GEC deben ser tenidas en cuenta por el asesor o asesora para el contraste y mejora del historial formativo de la persona candidata (especificaciones sobre el saber) e historial profesional (especificaciones sobre el saber hacer y saber estar).

Lo explicitado por la persona candidata durante el asesoramiento deberá ser contrastado por el evaluador o evaluadora, empleando para ello el referente de evaluación (UC y los criterios fijados en la correspondiente GEC) y el método que la Comisión de Evaluación determine. Estos métodos pueden ser, entre otros, la observación de la persona candidata en el puesto de trabajo, entrevistas profesionales, pruebas objetivas u otros. En el punto 2.1 de esta Guía se hace referencia a los mismos.

Este apartado comprende las especificaciones del “saber” y el “saber hacer”, que configuran las “competencias técnicas”, así como el “saber estar”, que comprende las “competencias sociales”.

a) Especificaciones relacionadas con el “saber hacer”

La persona candidata demostrará el dominio práctico relacionado con las actividades profesionales principales y secundarias que intervienen en el diseño e implementación de sistemas seguros de acceso y transmisión de datos, y que se indican a continuación:

Nota: A un dígito se indican las actividades profesionales expresadas en las realizaciones profesionales de la unidad de competencia, y a dos dígitos las reflejadas en los criterios de realización.

1. Implantar políticas de seguridad y cifrado de información en operaciones de intercambio de datos para obtener conexiones seguras según las necesidades de uso y dentro de las directivas de la organización.

1.1. Las comunicaciones con otras compañías o a través de canales inseguros se realizan haciendo uso de redes privadas virtuales para garantizar la confidencialidad e integridad de dichas conexiones durante el tránsito a través de redes públicas según las especificaciones de la normativa aplicable de seguridad y el diseño de redes de la organización.

1.2. Los requerimientos para implantar la solución de red privada virtual se seleccionan y comunican al operador de telefonía para lograr soluciones adecuadas al plan de seguridad.

1.3. Las técnicas de protección de conexiones inalámbricas disponibles en el mercado se evalúan y se seleccionan aquellas más idóneas, teniendo en cuenta el principio de proporcionalidad y las normas de seguridad de la organización.

1.4. Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones se implantan según parámetros de la normativa de seguridad de la organización.

1.5. La encapsulación, o encriptación extremo a extremo se activa para aquellos servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas para garantizar la seguridad de las comunicaciones.

1.6. Los servicios que incorporan soporte para certificados digitales para identificación del servidor, se emplean para garantizar al usuario la identidad del servidor.

1.7. Las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas se documentan en el formato establecido en la organización.

1.8. Los servicios que incorporan una autenticación de doble o triple factor, validación con certificados de usuario, DNI electrónico, 'token', biométricos u otros dispositivos se implantan según las necesidades.

2. Implantar sistemas de firma digital para asegurar la autenticidad, integridad y confidencialidad de los datos que intervienen en una transferencia de información utilizando sistemas y protocolos criptográficos según las necesidades de uso y dentro de las directivas de la organización.

2.1. El acceso a servicios a través de la red telemática se implanta de forma que utilice la autenticación basada en certificados digitales de identidad personal.

2.2. El proceso de obtención y verificación de firmas se aplica en caso de ser necesario según los requerimientos del sistema informático y los procesos de negocio.

2.3. La utilización de certificados digitales para firmar y cifrar su contenido se asegura en la transmisión de mensajes de correo electrónico.

2.4. El perfil de firma digital de documentos estándar se emplea asegurando que es el más adecuado al uso que se va a realizar.

2.5. Los sistemas de sellado digital de tiempo, para garantizar la existencia de un documento en una determinada fecha, se implantan según las normas de seguridad de la organización.

2.6. Los componentes web se firman digitalmente de forma que se pueda garantizar la integridad de dichos componentes.

2.7. Los sistemas de firma digital implantados se documentan en el formato establecido en la organización.

3. Implementar infraestructuras de clave pública para garantizar la seguridad según los estándares del sistema y dentro de las directivas de la organización.

3.1. La jerarquía de certificación se diseña en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.

3.2. La declaración de prácticas de certificación y la política de certificación se redacta de forma que definen los procedimientos y derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.

3.3. El sistema de autoridad de certificación se instala siguiendo las indicaciones del fabricante.

3.4. El certificado digital de la autoridad de certificación y su política asociada se ponen a disposición de los usuarios en la forma y modo necesario, siguiendo las directrices contenidas en la declaración de prácticas de certificación.

3.5. La clave privada de la autoridad de certificación se mantiene segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.

3.6. La emisión de certificados digitales se realiza según los usos que va a

recibir el certificado y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.

3.7. El servicio de revocación de certificados mantiene accesible la información sobre validez de los certificados emitidos por la autoridad de certificación según lo indicado en la declaración de prácticas de certificación.

3.8. Las infraestructuras de clave pública implantadas se documentan en el formato establecido en la organización.

b) Especificaciones relacionadas con el "saber".

La persona candidata, en su caso, deberá demostrar que posee los conocimientos técnicos (conceptos y procedimientos) que dan soporte a las actividades profesionales implicadas en las realizaciones profesionales de la **UC0489_3 Diseñar e implementar sistemas seguros de acceso y transmisión de datos.** Estos conocimientos se presentan agrupados a partir de las actividades profesionales principales que aparecen en cursiva y negrita:

1. Criptografía.

- Seguridad de la información y criptografía.
- Conceptos básicos.
- Cifrado de clave simétrica.
- Firma digital.
- Cifrado de clave pública.
- Funciones resumen.
- Cifrado de flujo y de bloque.
- Protocolos de intercambio de clave.

2. Comunicaciones Seguras.

- Redes privadas virtuales.
- IP Security Protocol.
- Túneles cifrados.

3. Autoridades de Certificación.

- Infraestructura de clave pública (PKI).
- Política de certificado y declaración de prácticas de certificación.
- Jerarquías de autoridades de certificación.
- Infraestructuras de gestión de privilegios (PMI).

c) Especificaciones relacionadas con el "saber estar"

La persona candidata debe demostrar la posesión de actitudes de comportamiento en el trabajo y formas de actuar e interactuar, según las siguientes especificaciones:

- Demostrar interés por el conocimiento amplio de la organización y sus procesos.
- Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
- Adaptarse a la organización, a sus cambios organizativos y tecnológicos así como a situaciones o contextos nuevos.
- Demostrar flexibilidad para entender los cambios.
- Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
- Habituarse al ritmo de trabajo de la organización.

1.2. Situaciones profesionales de evaluación y criterios de evaluación

La situación profesional de evaluación define el contexto profesional en el que se tiene que desarrollar la misma. Esta situación permite al evaluador o evaluadora obtener evidencias de competencia de la persona candidata que incluyen, básicamente, todo el contexto profesional de la Unidad de Competencia implicada.

Así mismo, la situación profesional de evaluación se sustenta en actividades profesionales que permiten inferir competencia profesional respecto a la práctica totalidad de realizaciones profesionales de la Unidad de Competencia.

Por último, indicar que la situación profesional de evaluación define un contexto abierto y flexible, que puede ser completado por las CC.AA., cuando éstas decidan aplicar una prueba profesional a las personas candidatas.

En el caso de la UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos, se tiene una situación profesional de evaluación y se concreta en los siguientes términos:

1.2.1. Situación profesional de evaluación

a) Descripción de la situación profesional de evaluación.

En esta situación profesional, la persona candidata demostrará la competencia requerida para diseñar e implementar sistemas seguros de acceso y transmisión de datos utilizando un entorno de red en funcionamiento

que incluya como mínimo un router, un firewall o “appliance”, un servidor y dos equipos de cliente, con conexión al exterior por medio de un acceso a Internet. Esta situación comprenderá al menos las siguientes actividades:

1. Implantar la utilización de técnicas criptográficas.

2. Implantar la utilización de la firma digital.

3. Crear una infraestructura de clave pública (PKI).

Condiciones adicionales:

- Se dispondrá de equipamientos, software específico y ayudas técnicas requeridas para el desarrollo de la situación profesional de evaluación.

- Se asignará un tiempo total para que el candidato o la candidata demuestre su competencia en condiciones de estrés profesional.

- Se planteará alguna contingencia o situación imprevista que sea relevante para la demostración de la competencia relacionada con la respuesta a contingencias.

b) Criterios de evaluación asociados a la situación de evaluación.

Con el objeto de optimizar la validez y fiabilidad del resultado de la evaluación, esta Guía incluye unos criterios de evaluación integrados y, por tanto, reducidos en número. Cada criterio de evaluación está formado por un criterio de mérito significativo, así como por los indicadores y escalas de desempeño competente asociados a cada uno de dichos criterios.

En la situación profesional de evaluación, los criterios se especifican en el cuadro siguiente:

Criterios de mérito	***Indicadores, escalas y umbrales de desempeño competente***
Implantación de técnicas criptográficas.	- Elección de protocolos seguros. - Utilización de certificados digitales. - Configuración de VPN. - Protección en conexiones inalámbricas. *El umbral de desempeño competente está explicitado en la escala A.*

Aplicación de la firma digital.	- Firma de los mensajes de correo. - Cifrado de los mensajes de correo. - Firma de los documentos digitales. - Utilización del sellado digital en los documentos. *El umbral de desempeño competente está explicitado en la escala B.*
Creación de una infraestructura de clave pública.	- Redacta las políticas de certificación según las directrices recibidas. - Ofrece la petición y emisión de certificados como Autoridad de Certificación de manera eficiente siguiendo las directivas otorgadas. - Crea copias de seguridad de la clave privada de la autoridad de certificación manteniendo ésta segura en todo momento. - Posibilita la revocación de certificados y la consulta de validez en todos los casos. *El umbral de desempeño competente requiere el cumplimiento total de los indicadores del criterio de mérito.*

Escala A

5 *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido siempre preferentemente protocolos seguros y se ha garantizado la identidad de los servidores mediante certificados digitales en todos los casos. La configuración de la VPN entre distintas sedes ha sido correcta y las conexiones inalámbricas se han protegido de la manera más eficaz posible.*

4 ***La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido siempre preferentemente protocolos seguros y se ha garantizado la identidad de los servidores mediante certificados digitales en todos los casos. La configuración de la VPN entre distintas sedes ha sido correcta y las conexiones inalámbricas se han protegido.***

3 *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido siempre preferentemente protocolos seguros y se ha garantizado la identidad de los servidores mediante certificados digitales en todos los casos. La configuración de la VPN entre distintas sedes ha sido defectuosa y las conexiones inalámbricas no se han protegido completamente.*

2 *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido protocolos seguros solo en algunos casos y no se ha garantizado la identidad de los servidores mediante certificados digitales. La configuración de la VPN entre distintas sedes ha sido incorrecta y las conexiones inalámbricas no se han protegido.*

1 *La implantación de técnicas criptográficas en las conexiones de red no se ha realizado según las directivas recibidas. No se ha elegido protocolos seguros y no se ha garantizado la identidad de los*

	servidores mediante certificados digitales. No se ha configurado VPN y las conexiones inalámbricas no se han protegido.

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

Escala B

4	*La aplicación de la firma digital se ha ejecutado de manera correcta. Se ha seguido todas las directivas recibidas fielmente. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización de la mejor manera posible. Se ha permitido la posibilidad de firmar y sellar digitalmente todos los documentos de la organización de forma eficaz.*
3	***La aplicación de la firma digital se ha ejecutado de manera correcta. Se ha seguido las directivas recibidas. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización. Se ha permitido la posibilidad de firmar y sellar digitalmente todos los documentos de la organización.***
2	*La aplicación de la firma digital se ha ejecutado de manera correcta. No se ha seguido todas las directivas recibidas. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización. No se ha permitido la posibilidad de firmar ni la de sellar digitalmente todos los documentos de la organización.*
1	*La aplicación de la firma digital no se ha ejecutado de manera correcta. No se ha seguido todas las directivas recibidas. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización de manera incorrecta. No se ha permitido la posibilidad de firmar ni la de sellar digitalmente todos los documentos de la organización.*

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 3 de la escala.

2. MÉTODOS DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA Y ORIENTACIONES PARA LAS COMISIONES DE EVALUACIÓN Y EVALUADORES/AS

La selección de métodos de evaluación que deben realizar las Comisiones de Evaluación será específica para cada persona candidata, y dependerá fundamentalmente de tres factores: nivel de cualificación de la unidad de competencia, características personales de la persona candidata y evidencias de competencia indirectas aportadas por la misma.

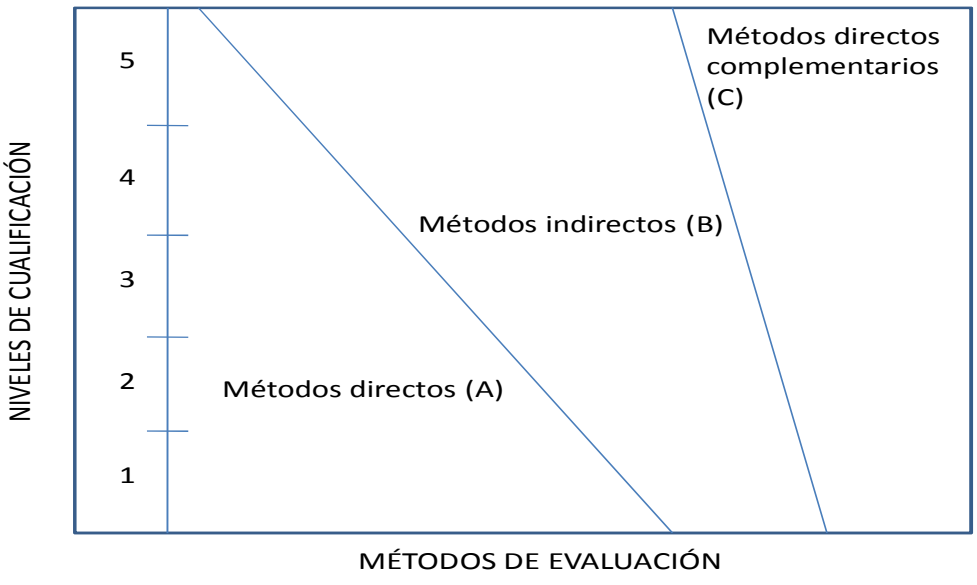
2.1. Métodos de evaluación y criterios generales de elección

Los métodos que pueden ser empleados en la evaluación de la competencia profesional adquirida por las personas a través de la experiencia laboral, y vías no formales de formación son los que a continuación se relacionan:

a) **Métodos indirectos**: Consisten en la valoración del historial profesional y formativo de la persona candidata; así como en la valoración de muestras sobre productos de su trabajo o de proyectos realizados. Proporcionan evidencias de competencia inferidas de actividades realizadas en el pasado.

b) **Métodos directos**: Proporcionan evidencias de competencia en el mismo momento de realizar la evaluación. Los métodos directos susceptibles de ser utilizados son los siguientes:

- Observación en el puesto de trabajo (A).
- Observación de una situación de trabajo simulada (A).
- Pruebas de competencia profesional basadas en las situaciones profesionales de evaluación (C).
- Pruebas de habilidades (C).
- Ejecución de un proyecto (C).
- Entrevista profesional estructurada (C).
- Preguntas orales (C).
- Pruebas objetivas (C).



Fuente: Leonard Mertens (elaboración propia)

Como puede observarse en la figura anterior, en un proceso de evaluación que debe ser integrado ("holístico"), uno de los criterios de elección depende del nivel de cualificación de la UC. Como puede observarse, a menor nivel, deben priorizarse los métodos de

observación en una situación de trabajo real o simulada, mientras que, a niveles superiores, debe priorizarse la utilización de métodos indirectos acompañados de entrevista profesional estructurada.

La consideración de las características personales de la persona candidata, debe basarse en el principio de equidad. Así, por este principio, debe priorizarse la selección de aquellos métodos de carácter complementario que faciliten la generación de evidencias válidas. En este orden de ideas, nunca debe aplicarse una prueba de conocimientos de carácter escrito a un candidato de bajo nivel cultural al que se le aprecien dificultades de expresión escrita. Una conversación profesional que genere confianza sería el método adecuado.

Por último, indicar que las evidencias de competencia indirectas debidamente contrastadas y valoradas, pueden incidir decisivamente, en cada caso particular, en la elección de otros métodos de evaluación para obtener evidencias de competencia complementarias.

2.2. Orientaciones para las Comisiones de Evaluación y Evaluadores.

a) Cuando la persona candidata justifique sólo formación no formal y no tenga experiencia en el diseño e implementación de sistemas seguros de acceso y transmisión de datos, se le someterá, al menos, a una prueba profesional de evaluación y a una entrevista profesional estructurada sobre la dimensión relacionada con el “saber” y “saber estar” de la competencia profesional.

b) En la fase de evaluación siempre se deben contrastar las evidencias indirectas de competencia presentadas por la persona candidata. Deberá tomarse como referente la UC, el contexto que incluye la situación profesional de evaluación, y las especificaciones de los “saberes” incluidos en las dimensiones de la competencia. Se recomienda utilizar una entrevista profesional estructurada.

c) Si se evalúa a la persona candidata a través de la observación en el puesto de trabajo, se recomienda tomar como referente los logros expresados en las realizaciones profesionales considerando el contexto expresado en la situación profesional de evaluación.

d) Si se aplica una prueba práctica, se recomienda establecer un tiempo para su realización, considerando el que emplearía un/a profesional competente, para que el evaluado trabaje en condiciones de estrés profesional.

e) Por la importancia del “saber estar” recogido en la letra c) del apartado 1.1 de esta Guía, en la fase de evaluación se debe comprobar la competencia

de la persona candidata en esta dimensión particular, en los aspectos considerados.

f) Esta Unidad de Competencia es de nivel 3 y en sus competencias más significativas tienen mayor relevancia las destrezas cognitivas y actitudinales. Por las características de estas competencias, la persona candidata ha de movilizar principalmente las destrezas cognitivas aplicándolas de forma competente en múltiples situaciones y contextos profesionales. Por esta razón, se recomienda que la comprobación de lo explicitado por la persona candidata se complemente con una prueba de desarrollo práctico, que tome como referente las actividades de la situación profesional de evaluación, todo ello con independencia del método de evaluación utilizado. Esta prueba se planteará sobre un contexto definido que permita evidenciar las citadas competencias, minimizando los recursos y el tiempo necesario para su realización, e implique el cumplimiento de las normas de seguridad, prevención de riesgos laborales y medioambientales, en su caso, requeridas.

g) Si se utiliza la entrevista profesional para comprobar lo explicitado por la persona candidata se tendrán en cuenta las siguientes recomendaciones:

   Se estructurará la entrevista a partir del análisis previo de toda la documentación presentada por la persona candidata, así como de la información obtenida en la fase de asesoramiento y/o en otras fases de la evaluación.

   La entrevista se concretará en una lista de cuestiones claras, que generen respuestas concretas, sobre aspectos que han de ser explorados a lo largo de la misma, teniendo en cuenta el referente de evaluación y el perfil de la persona candidata. Se debe evitar la improvisación.

   El evaluador o evaluadora debe formular solamente una pregunta a la vez dando el tiempo suficiente de respuesta, poniendo la máxima atención y neutralidad en el contenido de las mismas, sin enjuiciarlas en ningún momento. Se deben evitar las interrupciones y dejar que la persona candidata se comunique con confianza, respetando su propio ritmo y solventando sus posibles dificultades de expresión.

   Para el desarrollo de la entrevista se recomienda disponer de un lugar que respete la privacidad. Se recomienda que la entrevista sea grabada mediante un sistema de audio vídeo previa autorización de la persona implicada, cumpliéndose la ley de protección de datos.

h) En el desarrollo de la SPE se recomienda proporcionar indicaciones sobre directivas y las necesidades de uso de la organización.

i) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con el sistemas operativo elegido para la implantación de la Autoridad de Certificación, un cambio en el software con el que cifrar los documentos o en el de gestión del correo electrónico mediante clave pública, que tendrá que resolver de forma que plantee la solución más adecuada.