GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

"UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos"

CUALIFICACIÓN PROFESIONAL: OPERACIÓN DE SISTEMAS INFORMÁTICOS

Código: IFC300_2 **NIVEL: 2**

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 UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.

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 mantenimiento de la seguridad de los subsistemas físicos y lógicos en sistemas informáticos 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. ***Realizar la copia de seguridad, para garantizar la integridad de los datos, según los procedimientos establecidos y el plan de seguridad.***

   1.1. Las copias de seguridad se realizan, para proteger los datos del sistema, según la periodicidad, soporte y procedimiento establecidos en el plan de seguridad del sistema.

   1.2. Las copias de seguridad se verifican, para asegurar la utilización de las mismas, según los procedimientos establecidos en el plan de seguridad del sistema.

   1.3. El almacenamiento de las copias de seguridad, para evitar pérdidas de la información, se realiza en las condiciones y según el procedimiento indicado en el plan de seguridad del sistema y las recomendaciones del fabricante del soporte.

   1.4. Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

2. ***Revisar los accesos al sistema informático, para asegurar la aplicación de los procedimientos establecidos y el plan de seguridad, informando de las anomalías detectadas.***

   2.1. Las herramientas de monitorización, para trazar los accesos y la actividad del sistema se comprueban para asegurar su funcionamiento, según el plan de seguridad del sistema.

   2.2. Los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema se recopilan para localizar la existencia de accesos o actividades no deseados.

   2.3. Las incidencias de acceso al sistema detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

   2.4. Los cambios detectados en la configuración del acceso de usuarios al sistema se documentan, para mantener el inventario actualizado, según procedimientos establecidos.

3. ***Comprobar el funcionamiento de los mecanismos de seguridad establecidos informando de las anomalías detectadas a personas de responsabilidad superior.***

   3.1. Los permisos de acceso de los usuarios al sistema se comprueban, para asegurar su validez, según el plan de seguridad del sistema.

   3.2. Las políticas de seguridad de usuario se comprueban, para cerciorar su validez, según el plan de seguridad del sistema.

   3.3. Los sistemas de protección antivirus y de programas maliciosos se revisan, en lo que respecta a su actualización y configuración funcional,

para garantizar la seguridad del equipo, según los procedimientos establecidos por la organización.

3.4. Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

3.5. Los procesos de diagnóstico se realizan en los equipos en los que se han detectado incidencias utilizando herramientas específicas y de gestión remota con el fin de solucionarlas o escalarlas siguiendo los procedimientos establecidos.

4. Verificar que las condiciones ambientales y de seguridad se mantienen según los planes establecidos, informando de posibles anomalías.

4.1. Las especificaciones técnicas de los dispositivos se comprueban para asegurar que se cumplen las recomendaciones de los fabricantes en cuanto a condiciones ambientales y de seguridad.

4.2. La ubicación de los equipos y dispositivos físicos se revisa para asegurar que se cumplen los requisitos en cuanto a seguridad, espacio y ergonomía establecidos por la organización.

4.3. Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

4.4. Las acciones correctivas establecidas para solucionar determinadas incidencias detectadas se realizan según procedimientos establecidos.

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 **UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.** Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Gestión de la seguridad informática.

- Objetivo de la seguridad.
- Procesos de gestión de la seguridad.
- Métodos de identificación de amenazas: atacante externo e interno.

2. Seguridad lógica del sistema.

- Sistemas de ficheros y control de acceso.
- Permisos y derechos de usuarios.
- Registros de usuarios: sistemas de autenticación débiles; sistemas de autenticación fuertes; sistemas de autenticación biométricos y otros sistemas.

- Herramientas para la gestión de usuarios.
- Software de detección de virus y programas maliciosos, técnicas de recuperación y desinfección de datos afectados.
- Herramientas de gestión remota de incidencias.

3. Copias de seguridad.

- Tipos de copias.
- Arquitectura del servicio de copias de respaldo.
- Medios de almacenamiento para copias de seguridad.
- Herramientas para la realización de copias de seguridad.
- Restauración de copias y verificación de la integridad de la información.

4. Procedimientos de monitorización de los accesos y la actividad del sistema.

- Objetivos de la monitorización.
- Procedimientos de monitorización de trazas: aspectos monitorizables o auditables; clasificación de eventos e incidencias: de sistema, de aplicación, de seguridad; mecanismos de monitorización de trazas: alarmas y acciones correctivas; información de los registros de trazas.
- Técnicas y herramientas de monitorización.
- Informes de monitorización.

5. Entorno físico de un sistema informático.

- Los equipos y el entorno: adecuación del espacio físico.
- Reglamentos y normativas aplicables.
- Agentes externos y su influencia en el sistema.
- Efectos negativos sobre el sistema.
- Creación del entorno adecuado: control de las condiciones ambientales: humedad y temperatura; factores industriales: polvo, humo, interferencias, ruidos y vibraciones; factores humanos: funcionalidad, ergonomía y calidad de la instalación; otros factores.
- Factores de riesgo: conceptos de seguridad eléctrica; requisitos eléctricos de la instalación; perturbaciones eléctricas y electromagnéticas; electricidad estática; otros factores de riesgo.
- Los aparatos de medición.
- Acciones correctivas para asegurar requisitos de seguridad y ambientales.

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:

- Actuar con rapidez en situaciones problemáticas y no limitarse a esperar.
- Demostrar un buen hacer profesional.
- Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
- Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.

- Adaptarse a situaciones o contextos nuevos.
- Respetar los procedimientos y normas internas de la organización.
- Mantener una actitud proactiva orientada a la mejora de procesos.

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 UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos, 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 las competencias requeridas para mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos, utilizando una red local de ordenadores compuesta al menos por dos equipos de usuario, en el que uno actuará como servidor. Esta situación comprenderá al menos las siguientes actividades:

1. Revisar el acceso a los sistemas informáticos.

2. Comprobar los mecanismos de seguridad.

3. Realizar una copia de seguridad.

Condiciones adicionales:

- Se dispondrá de los equipos, material y documentación necesaria para el desarrollo de la situación profesional de evaluación.

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

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

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***
Revisión del acceso a los sistemas informáticos.	- Comprobación del funcionamiento de las herramientas de monitorización. - Recopilación de los ficheros de trazas de conexión de usuario. - Localización de accesos no deseados en las trazas. - Registro de la incidencia de seguridad. - Documentación del proceso. *El umbral de desempeño competente está explicitado en la Escala A.*
Comprobación de los mecanismos de seguridad.	- Detección de la incidencia. - Diagnóstico y localización del origen de la incidencia. - Solución de la incidencia. - Documentación del proceso. *El umbral de desempeño competente está explicitado en la Escala B.*
Comprobación del estado del dispositivo de impresión.	- Comprobación de la validez de los permisos de usuario. - Comprobación de la validez de las políticas de seguridad de usuario. - Revisión de los sistemas de protección como el estado del software como antivirus y spyware y de su configuración de seguridad. - Registro de incidencias completa y clara. - Uso de herramientas remotas de diagnóstico con fluidez.

	El umbral de desempeño competente requiere el cumplimiento total de este criterio de mérito.
Realización de copia de seguridad.	- Protección de datos de usuario. - Verificación de la copia de seguridad. - Almacenamiento de la copia. *El umbral de desempeño competente está explicitado en la Escala B.*

Escala A

5	*La comprobación de las herramientas de monitorización se ha realizado con el manual del software presente y se han trazado los accesos y la actividad del sistema. Los ficheros de trazas se han recopilado y se han analizado en busca de accesos no deseados. Las incidencias encontradas se han registrado. Los cambios en la configuración de usuario se han documentado.*
4	***La comprobación de las herramientas de monitorización se ha realizado sin el manual del software presente y se han trazado los accesos y la actividad del sistema. Los ficheros de trazas se han recopilado y se han analizado en busca de accesos no deseados. Las incidencias encontradas se han registrado. Los cambios en la configuración de usuario se han documentado.***
3	*La comprobación de las herramientas de monitorización no se ha realizado. Los ficheros de trazas se han recopilado y se han analizado en busca de accesos no deseados. Las incidencias encontradas se han registrado. Los cambios en la configuración de usuario se han documentado.*
2	*No se han comprobado las herramientas de monitorización. Los ficheros de trazas se han recopilado y se han analizado en busca de accesos no deseados. Las incidencias encontradas se han registrado. Los cambios en la configuración de usuario no se han documentado.*
1	*No se han comprobado las herramientas de monitorización. Los ficheros de trazas se han recopilado y se han analizado en busca de accesos no deseados. Las incidencias encontradas no se han registrado. Los cambios en la configuración de usuario no se han documentado.*

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

Escala B

4	*La copia de seguridad se ha realizado protegiendo la integridad de los datos, y en el soporte establecido en el plan de seguridad del sistema. La copia se ha verificado siguiendo las indicaciones del plan de seguridad. La copia se ha almacenado de acuerdo a las condiciones del fabricante del soporte y según las indicaciones del plan de seguridad.*
3	***La copia de seguridad se ha realizado protegiendo la integridad de los datos, y en el soporte establecido en el plan de seguridad del sistema. La copia se ha verificado sin seguir las indicaciones del plan de seguridad. La copia se ha almacenado de acuerdo a las condiciones del fabricante del soporte y según las indicaciones del plan de seguridad.***
2	*La copia de seguridad se ha realizado protegiendo la integridad de los datos, y en el soporte establecido en el plan de seguridad del sistema. La copia no se ha verificado. La copia se ha almacenado de acuerdo a las condiciones del fabricante del soporte y según las indicaciones del plan de seguridad.*
1	*La copia de seguridad se ha realizado sin proteger la integridad de los datos, y en un soporte que no es el indicado en el plan de seguridad del sistema. La copia no se ha verificado. La copia se ha almacenado de acuerdo a las condiciones del fabricante del soporte y según las indicaciones del plan de seguridad.*

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.

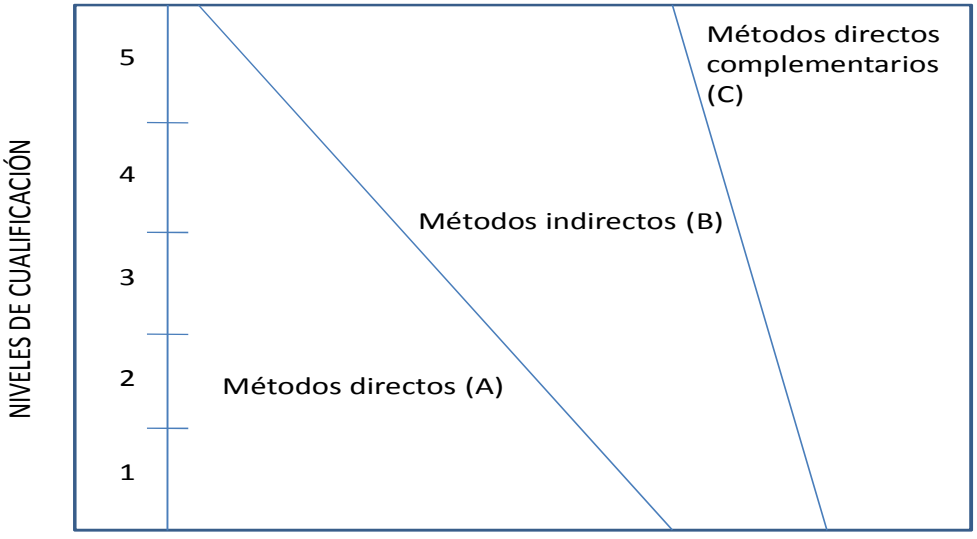
2.1. Métodos de evaluación y criterios generales de elección.

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 mantenimiento de la seguridad de los subsistemas físicos y lógicos en sistemas informáticos, 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 2 y sus competencias tienen componentes manuales, cognitivos y actitudinales. Por sus características y dado, que en este caso, tiene mayor relevancia el componente de

destrezas manuales en función del método de evaluación utilizado, se recomienda que en la comprobación de lo explicitado por la persona candidata se complemente con una prueba práctica que tenga como referente las actividades de la situación profesional de evaluación. Esta se planteará sobre un contexto reducido que permita optimizar la observación de competencias, minimizando los medios materiales y el tiempo necesario para su realización, cumpliéndose las normas de seguridad, prevención de riesgos laborales y medioambientales 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 provocar una situación anómala que impida el acceso al sistema informático por parte de un usuario y que genere una incidencia de seguridad.

i) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con el acceso al sistema informático por parte de un usuario que puede ser por ejemplo el bloqueo del acceso o un cambio en sus permisos, a lo largo de las actividades, que tendrá que resolver de forma que plantee la solución más adecuada.