# GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

## "UC0487_3: Auditar redes de comunicación y sistemas informáticos"

## 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 UC0487_3: Auditar redes de comunicación y 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 la auditoría de redes de comunicación y 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 análisis de vulnerabilidades, mediante programas específicos para controlar posibles fallos en la seguridad de los sistemas según las necesidades de uso y dentro de las directivas de la organización.***

   1.1. Las herramientas y los tipos de pruebas de análisis de vulnerabilidades se seleccionan, adecuándolas al entorno a verificar según las especificaciones de seguridad de la organización y el sector al que pertenece la misma.
   1.2. Los programas y las pruebas se actualizan para realizar ensayos consistentes con los posibles fallos de seguridad de las versiones de hardware y software instaladas en el sistema informático.
   1.3. Los resultados de las pruebas se analizan, documentándolos conforme se indica en las normas de la organización.
   1.4. Los sistemas de acceso por contraseña se comprueban mediante herramientas específicas según las especificaciones de la normativa de seguridad.
   1.5. El análisis de vulnerabilidades se documenta, incluyendo referencias exactas a las aplicaciones y servicios que se han detectado funcionando en el sistema, el nivel de los parches instalados, vulnerabilidades de negación de servicio, vulnerabilidades detectadas y mapa de la red.

2. ***Verificar el cumplimiento de las normativas, buenas prácticas y requisitos legales aplicables para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización.***

   2.1. La asignación de responsable de seguridad a todos los ficheros con datos de carácter personal se comprueba según la normativa aplicable.
   2.2. El estado del listado de personas autorizadas a acceder a cada fichero se verifica, comprobando que está actualizado según la normativa aplicable.
   2.3. El control de accesos a los ficheros se comprueba siguiendo el procedimiento establecido en la normativa de seguridad de la organización.
   2.4. La gestión del almacenamiento de los ficheros y sus copias de seguridad se audita, comprobando que se realiza siguiendo la normativa aplicable y las normas de la organización.
   2.5. El acceso telemático a los ficheros se audita, comprobando que se realiza utilizando mecanismos que garanticen la confidencialidad e integridad cuando así lo requiera la normativa.
   2.6. El informe de la auditoría se elabora, incluyendo la relación de ficheros con datos de carácter personal, las medidas de seguridad aplicadas y aquellas pendientes de aplicación (no conformidades) así como puntos

fuertes y puntos de mejora.

3. ***Comprobar el cumplimiento de la política de seguridad establecida para afirmar la integridad del sistema según las necesidades de uso y dentro de las directivas de la organización y teniendo en cuenta la normativa aplicable nacional e internacional.***

3.1. Los procedimientos de detección y gestión de incidentes de seguridad se desarrollan y se revisan, comprobando que están incluidos en la normativa de seguridad de la organización y que incluyen todo lo necesario para administrar de forma eficiente las posibles incidencias que pueden afectar a la organización.

3.2. Los puntos de acceso de entrada y salida de la red se testean comprobando que su uso se circunscribe a lo descrito en la normativa de seguridad de la organización.

3.3. La activación y actualización de los programas de seguridad y protección de sistemas se comprueba, viendo que corresponden a las especificaciones de los fabricantes.

3.4. Los puntos de entrada y salida de la red adicional se validan, verificando que se autorizan y controlan en base a las especificaciones de seguridad y al plan de implantación de la organización.

3.5. Los procesos de auditoría informática se revisan, tanto los de carácter interno, como aquellos realizados por personal externo a la organización, comprobando que se encuentran activados, actualizados y con los parámetros especificados en las normas de la organización.

3.6. El cumplimiento de los procedimientos de las políticas de seguridad por parte de los usuarios se verifica de forma que se detecte su correcta aplicación y adecuación a las necesidades de la organización en materia de seguridad.

**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 **UC0487_3: Auditar redes de comunicación y sistemas informáticos.** Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

***1. Vulnerabilidades.***

- Fallos de programa.
- Programas maliciosos.
- Programación segura.

***2. Análisis de vulnerabilidades.***

- Análisis local.
- Análisis remoto: análisis de caja blanca; análisis de caja negra.
- Optimización del proceso de auditoría.
- Contraste de vulnerabilidades e informe de auditoría.

***3. Normativa aplicable.***

- Normativa europea.
- Normativa nacional: Código penal; normativa de protección de datos. Normativa para el Tratamiento Automatizado de Datos.
- Trámites para la aplicación de la normativa de protección de datos en la empresa.

***4. Cortafuegos de red.***

- Componentes de un cortafuegos de red.
- Tipos de cortafuegos de red: filtrado de paquetes; cortafuegos de red de aplicación.
- Arquitecturas de cortafuegos de red: cortafuegos de red con dos interfaces; zona desmilitarizada.
- Otras arquitecturas de cortafuegos de red.

**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 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.

## 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 UC0487_3: Auditar redes de comunicación y 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 la competencia requerida para auditar redes de comunicación y sistemas informáticos en una empresa concreta a partir de las especificaciones legales y normativa de seguridad, con herramientas y metodologías de análisis de riesgos y vulnerabilidades. Esta situación comprenderá al menos las siguientes actividades:

1. Detectar vulnerabilidades en la seguridad de los sistemas.

2. Verificar el cumplimiento de la normativa y requisitos legales vigentes en materia de protección de datos personales.

3. Comprobar el cumplimiento de la política de seguridad establecida.

***Condiciones adicionales:***

- Se dispondrá de la documentación e información necesaria de la empresa, requeridos para la situación profesional de evaluación.

- Se asignará un tiempo total para que la persona 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*** |
|---|---|
| *Auditoría documental.* | - Revisión de documentación.<br>- Redacción del informe de situación actual.<br><br>*El umbral de desempeño competente está explicitado en la escala A.* |
| *Detección de vulnerabilidades.* | - Planificación del análisis de vulnerabilidades.<br>- Selección de las herramientas y pruebas de análisis.<br>- Actualización de programas y pruebas.<br>- Contraste y documentación de resultados.<br>- Comprobación de los sistemas de acceso por contraseña.<br>- Redacción del informe de análisis de vulnerabilidades.<br><br>*El umbral de desempeño competente está explicitado en la escala B.* |
| *Auditoría del cumplimiento de la normativa y requisitos legales vigentes.* | - Revisión del cumplimiento de la normativa vigente aplicable de protección de datos.<br>- Redacción del informe de auditoría.<br><br>*El umbral de desempeño competente está explicitado en la escala C.* |
| *Auditoría de la política de seguridad.* | - Revisión de la Política de seguridad de la organización.<br>- Redacción del informe de auditoría.<br><br>*El umbral de desempeño competente está explicitado en la escala D.* |

## Escala A

| | |
|---|---|
| 5 | *Se solicita toda la documentación que incluye: listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos y las auditorías anteriores. Se revisa dicha documentación y se redacta un informe completo de la situación actual de la organización.* |
| **4** | ***Se solicita una gran parte de la documentación necesaria (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores). Se revisa dicha documentación y se redacta un informe de situación actual de la organización.*** |
| 3 | *Se solicita parte de la documentación necesaria (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores). Se revisa parte de dicha documentación pero sí se redacta un informe de situación actual de la organización aunque no aborda todo lo necesario.* |
| 2 | *Se solicita parte de la documentación (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores). No se revisa dicha documentación pero sí se redacta un informe de situación actual de la organización.* |
| 1 | *No se solicita toda la documentación (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores), ni se revisa dicha documentación y no se redacta un informe de situación actual de la organización.* |

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

## Escala B

| | |
|---|---|
| 5 | *Se planifica el análisis de vulnerabilidades incluyendo todas las acciones necesarias para auditar el sistema, se seleccionan adecuadamente las herramientas y pruebas de análisis, se actualizan los programas y pruebas y se comprueban los sistemas de acceso por contraseña, según las especificaciones, procedimientos y normativa de seguridad de la organización. Se contrastan y documentan los resultados, y se redacta un informe completo de análisis de vulnerabilidades.* |
| **4** | ***Se planifica el análisis de vulnerabilidades, se seleccionan adecuadamente las herramientas y pruebas de análisis, aunque no se actualizan los programas y pruebas, se comprueban los sistemas de acceso por contraseña, según las especificaciones, procedimientos y normativa de seguridad de la organización. Se contrastan y documentan los resultados, y se redacta un informe completo de análisis de vulnerabilidades.*** |
| 3 | *Se planifica el análisis de vulnerabilidades, se seleccionan adecuadamente las herramientas y pruebas de análisis, pero no se actualizan los programas y pruebas, se comprueban los sistemas de acceso por contraseña, pero no se siguen las especificaciones, procedimientos y normativa de seguridad de la organización. Se contrastan y documentan los resultados, y se redacta un informe completo de análisis de vulnerabilidades.* |
| 2 | *No se planifica el análisis de vulnerabilidades, se seleccionan adecuadamente las herramientas y pruebas de análisis, pero no se actualizan los programas y pruebas, ni se comprueban los sistemas de acceso por contraseña, y no se siguen las especificaciones, procedimientos y normativa de seguridad de la organización. Se redacta un informe de análisis de vulnerabilidades.* |
| 1 | *No se planifica el análisis de vulnerabilidades, no se seleccionan adecuadamente las herramientas y pruebas de análisis, no se actualizan los programas y pruebas, ni se comprueban los sistemas de acceso por contraseña, y no se siguen las especificaciones, procedimientos y normativa de seguridad de la organización. No se contrastan y documentan los resultados, ni se redacta un informe de análisis de vulnerabilidades.* |

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

## Escala C

| | |
|---|---|
| 4 | *Se revisa el cumplimiento de todos los siguientes puntos de la legislación vigente en materia de protección de datos: asignación de responsable de seguridad a todos los ficheros con datos de carácter personal, existencia y estado del listado de acceso autorizado a los ficheros, existencia y estado del listado de control de accesos a los ficheros, proceso de gestión del almacenamiento de los ficheros y sus copias de seguridad, mecanismos de acceso telemático a los ficheros. Las deficiencias detectadas se redactan de forma clara, precisa y completa en el informe de auditoría.* |
| **3** | ***Se revisa el cumplimiento de como mínimo los siguientes puntos de la legislación vigente en materia de protección de datos: asignación de responsable de seguridad a todos los ficheros con datos de carácter personal, existencia del listado de acceso autorizado a los ficheros, existencia del listado de control de accesos a los ficheros, proceso de gestión del almacenamiento de los ficheros y sus copias de seguridad, mecanismos de acceso telemático a los ficheros. Las deficiencias detectadas se redactan de forma clara, precisa y completa en el informe de auditoría.*** |
| 2 | *Se revisa parcialmente el cumplimiento de los siguientes puntos de la legislación vigente en materia de protección de datos: asignación de responsable de seguridad a todos los ficheros con datos de carácter personal, existencia del listado de acceso autorizado a los ficheros, existencia del listado de control de accesos a los ficheros, proceso de gestión del almacenamiento de los ficheros y sus copias de seguridad, mecanismos de acceso telemático a los ficheros. No se incluyen las deficiencias detectadas de forma clara en el informe.* |
| 1 | *No se revisan muchos de los aspectos fundamentales de la legislación vigente en materia de protección de datos.* |

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

## Escala D

| | |
|---|---|
| 4 | *Se revisa exhaustivamente el cumplimiento de la Política de seguridad de la organización que incluye la verificación de la existencia y funcionalidad de los procedimientos de detección y gestión de incidentes de seguridad, de uso de los puntos de acceso de entrada y salida de red, de activación y actualización de los programas de seguridad y protección de sistemas, de autorización y control de los puntos de entrada y salida de la red, de los procesos de auditoría, del cumplimiento de los usuarios de los procedimientos de las políticas de seguridad. Se redacta un informe de auditoría que incluye todas las deficiencias detectadas en política de seguridad.* |
| **3** | ***Se revisa el cumplimiento de la Política de seguridad de la organización que incluye la verificación de la existencia de los procedimientos de detección y gestión de incidentes de seguridad, de uso de los puntos de acceso de entrada y salida de red, de activación y actualización de los programas de seguridad y protección de sistemas, de autorización y control de los puntos de entrada y salida de la red, de los procesos de auditoría, del cumplimiento de los usuarios de los procedimientos de las políticas de seguridad. Se redacta un informe de auditoría que incluye todas las deficiencias detectadas en política de seguridad.*** |
| 2 | *Se revisa parcialmente el cumplimiento de la Política de seguridad de la organización que incluye la verificación de la existencia y funcionalidad de los procedimientos de detección y gestión de incidentes de seguridad, de uso de los puntos de acceso de entrada y salida de red, de activación y actualización de los programas de seguridad y protección de sistemas, de autorización y control de los puntos de entrada y salida de la red, de los procesos de auditoría, del cumplimiento de los usuarios de los procedimientos de las políticas de seguridad. Se redacta un informe de auditoría que no incluye todas las deficiencias detectadas.* |
| 1 | *No se revisa adecuadamente el cumplimiento de la Política de seguridad de la organización. Se redacta un informe de auditoría.* |

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.

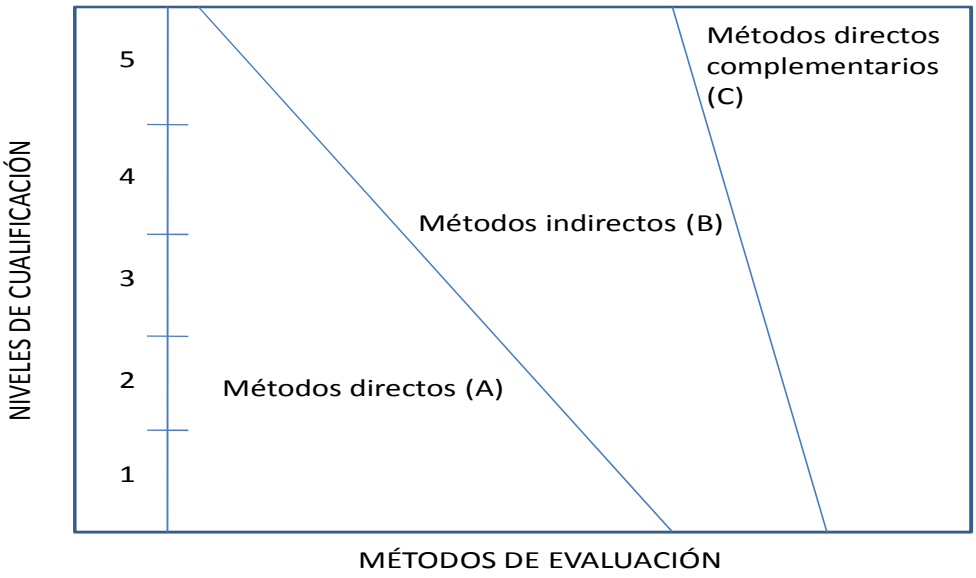
### 2.1. Métodos de evaluación y criterios generales de elección

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 auditar redes de comunicación y 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 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) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con la documentación contemplada en el caso práctico, siendo errónea en algunos casos, no coherente con el resto de documentos o que no incluya parte de la información, que tendrá que resolver de forma que plantee la solución más adecuada.