GUÍA DE EVIDENCIAS DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES

"ECP2798_2: Responder ante eventos de ciberseguridad"

1. ESPECIFICACIONES DE EVALUACIÓN DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES.

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 los elementos de la competencia (EC) e indicadores de calidad (IC) del ECP2798_2: Responder ante eventos de ciberseguridad.

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 (Estándar de Competencias Profesionales (ECP) 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 que intervienen en responder ante eventos de ciberseguridad, y que se indican a continuación:

Nota: A un dígito se indican las actividades profesionales expresadas en los elementos de la competencia del estándar de competencias profesionales, y dos dígitos las reflejadas en los indicadores de calidad.

1. ***Implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.***

    1.1 Los eventos de sistemas recolectados en el sistema de monitorización se parametrizan configurándolos de modo que se asegure que la información que proporciona es completa y precisa para facilitar su posterior tratamiento.
    1.2 Las reglas de tratamiento de los eventos normalizados se implementan, configurándolas en función de su severidad para la generación de alertas.
    1.3 Las reglas de correlación entre eventos normalizados y alertas se implementan, configurándolas en función de su severidad para la generación de alertas.
    1.4 Las reglas de agregación de eventos normalizados y alertas se implementan, configurando métricas y elementos para su agrupación.
    1.5 Los mecanismos de remediación automática o semiautomática de las alertas son implementados, de acuerdo con las condiciones de remediación.
    1.6 La documentación de las alertas y reglas de normalización, agregación y correlación realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

2. ***Ejecutar procedimientos frente alertas de seguridad, identificando parámetros, origen y condiciones y comunicando a las personas responsables de su gestión, para subsanar incidencias de seguridad, según normas y procedimientos de la entidad responsable.***

    2.1 El procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización se selecciona, interpretando cada alerta y consultando el maestro de alertas y procedimientos establecido por la organización.
    2.2 Los procedimientos de seguridad se aplican, de acuerdo con las condiciones de entorno de la alerta específica, identificando parámetros relacionados tales como direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros.
    2.3 El escalado de alertas se ejecuta, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos.
    2.4 Las alertas gestionadas se cierran, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación.
    2.5 La documentación relativa a las alertas gestionadas se confecciona, siguiendo los modelos internos establecidos por la organización,

recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

3. ***Colaborar en la definición de procedimientos de respuesta a alertas de seguridad, recabando requisitos, condiciones de entorno y objetivos, definiéndolos y registrándolos, para preparar la respuesta ante incidencias, según normas y procedimientos de la entidad responsable.***

3.1 Las alertas sin procedimiento asociado se marcan en la documentación para su uso posterior, utilizando el maestro de alertas y procedimientos operativos e identificando aquellas alertas no recogidas en él.
3.2 Los requisitos, condiciones de entorno y objetivos de remediación para cada alerta se recaban, previa identificación, documentándolos según modelos internos establecidos por la organización, para su control, uso y trazabilidad.
3.3 Los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable, se redactan, indicando las acciones a realizar y prestando especial atención a los requisitos de continuidad de negocio definidas por la organización.
3.4 Los procedimientos de seguridad se prueban, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización.
3.5 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

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 los elementos de la competencia del ECP**2798_2: Responder ante eventos de ciberseguridad**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Eventos y alertas de seguridad

- Sistemas de monitorización. Parametrización de eventos.
- Reglas de tratamiento de eventos normalizados. Severidad de las alertas.
- Reglas de correlación de eventos normalizados y alertas.
- Reglas de agregación de eventos normalizados y alertas. Métricas y elementos para su agrupación.
- Remediación automática o semiautomática de alertas.

2. Procedimientos ante alertas de seguridad

- Interpretación de las alertas. Maestro de alertas y procedimientos. Procedimientos operativos de seguridad.
- Condiciones de entorno de alertas específicas. Parámetros relacionados: direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros. Condiciones de escalado.
- Cierre de alertas.

3. Apoyo a la definición de procedimientos de respuesta a alertas de seguridad

- Identificación y documentación de alertas sin procedimiento asociado.
- Requisitos, condiciones de entorno y objetivos de remediación para alertas.
- Procedimientos de seguridad, elementos: alerta, condiciones de entorno, objetivos y requisitos de remediación, acciones a realizar. Garantía de la continuidad de negocio.

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:

- Aplicar las instrucciones de trabajo de manera organizada, precisa y meticulosa.
- Comprender y valorar las motivaciones y consecuencias del trabajo bien realizado.
- 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.
- Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

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 del Estándar de Competencias Profesionales implicado.

Así mismo, la situación profesional de evaluación se sustenta en actividades profesionales que permiten inferir competencia profesional respecto a la práctica totalidad de elementos de la competencia del Estándar de Competencias Profesionales.

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 del "ECP2798_2: Responder ante eventos de ciberseguridad", 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 responder ante eventos de ciberseguridad, cumpliendo la normativa relativa a protección medioambiental, planificación de la actividad preventiva y aplicando estándares de calidad. Esta situación comprenderá al menos las siguientes actividades:

1. Implementar eventos y alertas de seguridad.

2. Ejecutar procedimientos frente alertas de seguridad, para subsanar incidencias de seguridad, según normas y procedimientos.

3. Colaborar en la definición de procedimientos de respuesta a alertas de seguridad, para preparar la respuesta ante incidencias.

Condiciones adicionales:

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

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 de evaluación se especifican en el cuadro siguiente:

Criterios de mérito	*Indicadores de desempeño competente*

Idoneidad en la implementación de eventos y alertas de seguridad.	- Parametrización de los eventos de sistemas recolectados en el sistema de monitorización configurándolos de modo que se asegure que la información que proporciona es completa y precisa. - Implementación de las reglas de tratamiento de los eventos normalizados; de las reglas de correlación entre eventos normalizados y alertas, y de las reglas de agregación de eventos normalizados y alertas. - Implementación de los mecanismos de remediación automática o semiautomática de las alertas. - Confección de la documentación de las alertas y reglas de normalización, agregación y correlación realizados, siguiendo los modelos internos establecidos por la organización. *El umbral de desempeño competente está explicitado en la Escala A.*
Eficacia em la ejecución de procedimientos frente alertas de seguridad, para subsanar incidencias de seguridad, según normas y procedimientos.	- Selección del procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización. - Aplicación de los procedimientos de seguridad, de acuerdo con las condiciones de entorno de la alerta específica. - Ejecución del escalado de alertas, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos. - Cerramiento de las alertas gestionadas, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación. - Confección de la documentación relativa a las alertas gestionadas. *El umbral de desempeño competente está explicitado en la Escala B.*
Destreza en la colaboración de la definición de procedimientos de respuesta a alertas de seguridad, para preparar la respuesta ante incidencias.	- Marcación de las alertas sin procedimiento asociado en la documentación para su uso posterior. - Recopilación de los requisitos, condiciones de entorno y objetivos de remediación para cada alerta, documentándolos según modelos internos. - Redacción de los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable.

	- Prueba de los procedimientos de seguridad, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos. *El umbral de desempeño competente está explicitado en la Escala C.*
Cumplimiento del tiempo asignado, considerando el que emplearía un o una profesional competente.	
El desempeño competente requiere el cumplimiento, en todos los criterios de mérito, de la normativa aplicable en materia de prevención de riesgos laborales, protección medioambiental	

Escala A

4

Para implementar eventos y alertas de seguridad, parametriza los eventos de sistemas recolectados en el sistema de monitorización configurándolos de modo que se asegure que la información que proporciona es completa y precisa. Implementa las reglas de tratamiento de los eventos normalizados; de las reglas de correlación entre eventos normalizados y alertas, y de las reglas de agregación de eventos normalizados y alertas. Implementa los mecanismos de remediación automática o semiautomática de las alertas. Confecciona la documentación de las alertas y reglas de normalización, agregación y correlación realizados, siguiendo los modelos internos establecidos por la organización.

3

Para implementar eventos y alertas de seguridad, parametriza los eventos de sistemas recolectados en el sistema de monitorización configurándolos de modo que se asegure que la información que proporciona es completa y precisa. Implementa las reglas de tratamiento de los eventos normalizados; de las reglas de correlación entre eventos normalizados y alertas, y de las reglas de agregación de eventos normalizados y alertas. Implementa los mecanismos de remediación automática o semiautomática de las alertas. Confecciona la documentación de las alertas y reglas de normalización, agregación y correlación realizados, siguiendo los modelos internos establecidos por la organización, pero comete ciertas irregularidades que no alteran el resultado final.

2

Para implementar eventos y alertas de seguridad, parametriza los eventos de sistemas recolectados en el sistema de monitorización configurándolos de modo que se asegure que la información que proporciona es completa y precisa. Implementa las reglas de tratamiento de los eventos normalizados; de las reglas de correlación entre eventos normalizados y alertas, y de las reglas de agregación de eventos normalizados y alertas. Implementa los mecanismos de remediación automática o semiautomática de las alertas. Confecciona la documentación de las alertas y reglas de normalización, agregación y correlación realizados, siguiendo los modelos internos establecidos por la organización, pero comete ciertas irregularidades que alteran el resultado final.

1

	No implementa eventos y alertas de seguridad

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

Escala B

4	*Para ejecutar procedimientos frente alertas de seguridad, para subsanar incidencias de seguridad, según normas y procedimientos, Selecciona el procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización. Aplica los procedimientos de seguridad, de acuerdo con las condiciones de entorno de la alerta específica. Ejecuta el escalado de alertas, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos. Cierra las alertas gestionadas, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación. Confecciona la documentación relativa a las alertas gestionadas.*
3	***Para ejecutar procedimientos frente alertas de seguridad, para subsanar incidencias de seguridad, según normas y procedimientos, Selecciona el procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización. Aplica los procedimientos de seguridad, de acuerdo con las condiciones de entorno de la alerta específica. Ejecuta el escalado de alertas, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos. Cierra las alertas gestionadas, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación. Confecciona la documentación relativa a las alertas gestionadas, pero comete ciertas irregularidades que no alteran al resultado final.***
2	*Para ejecutar procedimientos frente alertas de seguridad, para subsanar incidencias de seguridad, según normas y procedimientos, Selecciona el procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización. Aplica los procedimientos de seguridad, de acuerdo con las condiciones de entorno de la alerta específica. Ejecuta el escalado de alertas, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos. Cierra las alertas gestionadas, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación. Confecciona la documentación relativa a las alertas gestionadas, pero comete ciertas irregularidades que alteran el resultado final*
1	*No ejecuta procedimientos frente alertas de seguridad, para subsanar incidencias de seguridad, según normas y procedimientos.*

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

Escala C

4	

	Para colaborar en la definición de procedimientos de respuesta a alertas de seguridad, para preparar la respuesta ante incidencias, marca las alertas sin procedimiento asociado en la documentación para su uso posterior. Recopila los requisitos, condiciones de entorno y objetivos de remediación para cada alerta, documentándolos según modelos internos. Redacta los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable. Prueba los procedimientos de seguridad, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos.
3	***Para colaborar en la definición de procedimientos de respuesta a alertas de seguridad, para preparar la respuesta ante incidencias, marca las alertas sin procedimiento asociado en la documentación para su uso posterior. Recopila los requisitos, condiciones de entorno y objetivos de remediación para cada alerta, documentándolos según modelos internos. Redacta los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable. Prueba los procedimientos de seguridad, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos, pero comete ciertas irregularidades que no afectan al resultado final.***
2	*Para colaborar en la definición de procedimientos de respuesta a alertas de seguridad, para preparar la respuesta ante incidencias, marca las alertas sin procedimiento asociado en la documentación para su uso posterior. Recopila los requisitos, condiciones de entorno y objetivos de remediación para cada alerta, documentándolos según modelos internos. Redacta los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable. Prueba los procedimientos de seguridad, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos, pero comete ciertas irregularidades que afectan al resultado final.*
1	*No colabora en la definición de procedimientos de respuesta a alertas de seguridad, para preparar la respuesta ante incidencias.*

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

2. MÉTODOS DE EVALUACIÓN DE LA ESTÁNDAR DE COMPETENCIAS PROFESIONALES 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 del estándar de competencias profesionales, características personales de la persona candidata y evidencias de competencia indirectas aportadas por la misma.

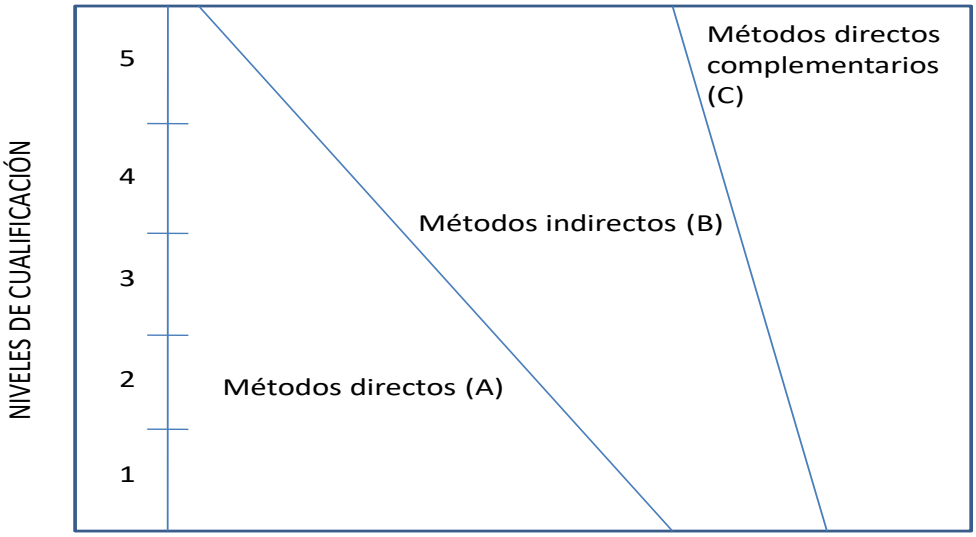
2.1. Métodos de evaluación y criterios generales de elección.

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 del ECP. 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 una persona candidata a la que se le aprecien dificultades de expresión escrita, ya sea por razones basadas en el desarrollo de las competencias básicas o factores de integración cultural, entre otras. 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 formal y no tenga experiencia en el proceso de Responder ante eventos de

ciberseguridad, 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 el ECP, 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 los elementos de la competencia 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 o una 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) Este Estándar de Competencias Profesionales es de nivel "2" y sus competencias conjugan básicamente destrezas cognitivas y actitudinales. Por las características de estas competencias, la persona candidata ha de movilizar fundamentalmente sus destrezas cognitivas aplicándolas de forma competente a 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 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.