GUÍA DE EVIDENCIAS DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES

TRANSVERSAL

"ECP0486_3: ASEGURAR EQUIPOS INFORMÁTICOS"

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 ECP0486_3: ASEGURAR EQUIPOS 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 (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 Asegurar equipos informáticos, 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. Configurar equipos informáticos siguiendo los procedimientos establecidos en el plan de seguridad de la organización para

protegerlos de la pérdida, manipulación y sustracción de información no autorizada.

1.1 Los tipos de usuarios se definen, estableciendo los privilegios de acceso a los recursos (aplicaciones software, carpetas, entre otros), según las funciones desempeñadas dentro de la organización.
1.2 Las cuentas de usuario se crean, utilizando las herramientas específicas del sistema operativo, dándoles un nombre de usuario, una contraseña y asignándolas a los tipos de usuarios definidos en el sistema informático.
1.3 La política de contraseñas se configura, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.
1.4 El control de acceso al equipo informático se establece, configurando parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.
1.5 La seguridad del equipo informático ante ataques externos se refuerza, configurando un cortafuegos según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.
1.6 La seguridad de la información del equipo informático (integridad, accesos, entre otros) frente a riesgos de ataque malicioso se revisa, comprobando la instalación y configuración del software de protección adecuado (EDP (EndPoint Detection and Response), anti-ransomware, anti-malware, entre otros).
1.7 La recopilación, tratamiento y eliminación de la información por parte de los usuarios se revisa, documentando detalladamente los protocolos a seguir según el grado de confidencialidad de la información.
1.8 La política de seguridad de la organización se transmite a los usuarios, publicando informaciones tales como restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos.

2. Configurar equipos servidores, aplicando los mecanismos de protección establecidos en el plan de seguridad de la organización para protegerlos de accesos indebidos.

2.1 Los servicios que ofrece el servidor (correo, web, servicio de impresión, entre otros) se configuran, haciendo uso de los entornos específicos de cada servicio, estableciendo valores a sus parámetros de configuración, conforme a las medidas de bastionado establecidas por la organización, si procede.
2.2 Los servicios del sistema operativo preinstalados no necesarios (NFS, DNS, entre otros) en el servidor se desactivan, borrándolos del sistema, garantizando así que no pueden ser activados.
2.3 La comunicación con el servidor (autentificación de usuarios, intercambio de información) se asegura, activando y configurando protocolos de seguridad tales como TLS (TLS, SSH, entre otros).
2.4 Los mecanismos de registro de actividad e incidencias del servidor se activan, configurando el registro de eventos del sistema y

parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).

2.5 Los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor se activan, configurando y parametrizando, según el servicio, valores tales como tamaño de los ficheros logs, rotación, nivel de detalle (dirección IP, fecha, usuario, entre otros).

2.6 Las configuraciones realizadas e incidencias producidas se documentan, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas software, entre otros).

3. Eliminar información en soportes y sistemas de almacenamiento de equipos informáticos, de forma segura, aplicando procedimientos de borrado seguro y destrucción física de información, siguiendo los procedimientos establecidos en la política de seguridad de la organización para prevenir la fuga de información confidencial.

3.1 Los métodos de destrucción física (trituración, desintegración, incineración, entre otros) se revisan, comprobando que el método utilizado se corresponde con el tipo de soporte de información.

3.2 El protocolo de retención de datos se interpreta, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.

3.3 La información almacenada en los equipos informáticos y en los soportes de información se borran, utilizando herramientas software de borrado seguro de datos.

3.4 El procedimiento realizado se registra, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del hardware, entre otras.

4. Aplicar medidas de seguridad física a equipos servidores, comprobando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras, siguiendo el plan de seguridad de la organización para evitar interrupciones en la prestación de servicios del sistema.

4.1 La ubicación física de los servidores se revisa, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.

4.2 Las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores se comprueban, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.

4.3 El Sistema de Alimentación Ininterrumpida (SAI) se revisa, comprobando que está operativo a través de su sistema de alertas y reportando su estado en caso de anomalías de funcionamiento.

5. Verificar la realización de copias de seguridad, comprobando la información a respaldar, la frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.

5.1 La información del equipo informático se comprueba, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde al plan de copias de seguridad.
5.2 El plan de copias de seguridad se verifica, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.
5.3 Los dispositivos de almacenamiento de copias de seguridad (cintas, discos externos, entre otros) se comprueban, verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en el plan de copias de seguridad.
5.4 Los procedimientos de obtención y verificación de copias de seguridad se verifican, realizando pruebas de funcionamiento de los mismos.

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**0486_3: Asegurar equipos informáticos**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Gestión de la seguridad y riesgos de un sistema informático

- Seguridad: objetivo de la seguridad; amenazas; atacante externo e interno; tipos de ataque; mecanismos de protección.
- Riesgos: proceso de gestión de riesgos; métodos de identificación y análisis de riesgos; reducción del riesgo.
- Normativa de protección medioambiental (CO2, reciclaje, entre otros).

2. Seguridad física en el sistema informático

- Protección del sistema informático.
- Protección de los datos.
- Técnicas de borrado seguro y destrucción de información. Herramientas software de borrado seguro de información.

3. Seguridad lógica del sistema informático

- Sistemas de ficheros.
- Permisos de archivos.
- Listas de control de acceso (ACLs) a ficheros.
- Registros de actividad del sistema.

- Autenticación de usuarios: sistemas de autenticación débiles; sistemas de autenticación fuertes; sistemas de autenticación biométricos.
- Introducción a la Criptografía y Establecimiento de Políticas de Contraseñas.
- Arquitectura del servicio de copias de respaldo: sistemas centralizados, sistemas distribuidos, copias locales.
- Planificación del servicio de copias de respaldo: niveles de copia de respaldo, dimensionamiento del servicio de copias de respaldo.
- Soportes para copias de respaldo: soportes tradicionales, jerarquías de almacenamiento.

4. Acceso remoto al sistema informático

- Mecanismos del sistema operativo para control de accesos.
- Cortafuegos de servidor: filtrado de paquetes; cortafuegos de nivel de aplicación; registros de actividad del cortafuegos.

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:

- Mantener el área de trabajo con el grado apropiado de orden y limpieza.
- Demostrar creatividad en el desarrollo del trabajo que realiza.
- Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.
- Interpretar y ejecutar instrucciones de trabajo.
- Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
- Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
- 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 "ECP0486_3: Asegurar equipos 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 asegurar equipos informáticos, 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. Configurar equipos informáticos y servidores.

2. Eliminar información en soportes y sistemas de almacenamiento.

3. Verificar la realización de copias de seguridad.

Condiciones adicionales:

- Se dispondrá de equipamientos, productos específicos y ayudas técnicas requeridas por la situación profesional de evaluación.

- Se comprobará la capacidad del candidato o candidata en respuesta a contingencias.

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

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***
Rigor para configurar equipos informáticos y servidores.	- Definición de los tipos de usuarios. - Creación de las cuentas de usuario. - Configuración de la política de contraseñas. - Establecimiento del control de acceso al equipo informático. - Refuerzo de la seguridad del equipo informático ante ataques externos. - Revisión de la seguridad sobre la información del equipo informático. - Revisión de la recopilación, tratamiento y eliminación de la información por parte de los usuarios. - Transmisión de la política de seguridad de la organización. - Configuración de los servicios que ofrece el servidor. - Desactivación de los servicios del sistema operativo preinstalados no necesarios. - Consolidación de los mecanismos de registro de actividad e incidencias del servidor. - Activación de los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor. - Documentación de las configuraciones realizadas e incidencias producidas, *El umbral de desempeño competente está explicitado en la Escala A.*
Eficacia para eliminar información en soportes y sistemas de almacenamiento.	- Revisión de los métodos de destrucción física. - Interpretación de el protocolo de retención de datos. - Anulación de la información almacenada. - Registro del procedimiento realizado. *El umbral de desempeño competente está explicitado en la Escala B.*
Rigor para verificar la realización de copias de seguridad.	- Comprobación de la información del equipo informático. - Verificación el plan de copias de seguridad. - Comprobación de los dispositivos de almacenamiento de copias de seguridad. - Verificación de los procedimientos de obtención y verificación de copias de seguridad.

	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 configurar equipos informáticos y servidores, define los tipos de usuarios. Crea las cuentas de usuario. Configura la política de contraseñas. Establece el control de acceso al equipo informático. Refuerza la seguridad del equipo informático ante ataques externos. Revisa la seguridad sobre la información del equipo informático. Revisa la recopilación, tratamiento y eliminación de la información por parte de los usuarios. Transmite la política de seguridad de la organización. Configura los servicios que ofrece el servidor. Desactiva los servicios del sistema operativo preinstalados no necesarios. Consolida los mecanismos de registro de actividad e incidencias del servidor. Activa los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor. Documenta las configuraciones realizadas e incidencias producidas.

3

Para configurar equipos informáticos y servidores, define los tipos de usuarios. Crea las cuentas de usuario. Configura la política de contraseñas. Establece el control de acceso al equipo informático. Refuerza la seguridad del equipo informático ante ataques externos. Revisa la seguridad sobre la información del equipo informático. Revisa la recopilación, tratamiento y eliminación de la información por parte de los usuarios. Transmite la política de seguridad de la organización. Configura los servicios que ofrece el servidor. Desactiva los servicios del sistema operativo preinstalados no necesarios. Consolida los mecanismos de registro de actividad e incidencias del servidor. Activa los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor. Documenta las configuraciones realizadas e incidencias producidas. La persona candidata comete ligeras irregularidades que no alteran el resultado final.

2

Para configurar equipos informáticos y servidores, define los tipos de usuarios. Crea las cuentas de usuario. Configura la política de contraseñas. Establece el control de acceso al equipo informático. Refuerza la seguridad del equipo informático ante ataques externos. Revisa la seguridad sobre la información del equipo informático. Revisa la recopilación, tratamiento y eliminación de la información por parte de los usuarios. Transmite la política de seguridad de la organización. Configura los servicios que ofrece el servidor. Desactiva los servicios del sistema operativo preinstalados no necesarios. Consolida los mecanismos de registro de actividad e incidencias del servidor. Activa los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor. Documenta las configuraciones realizadas e incidencias producidas. La persona candidata, comete amplias irregularidades que alteran el resultado final.

1

	No configura equipos informáticos ni servidores.

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

Escala B

4	*Para eliminar información en soportes y sistemas de almacenamiento, revisa los métodos de destrucción física. Interpreta el protocolo de retención de datos. Anula la información almacenada. Registra el procedimiento realizado.*
3	***Para eliminar información en soportes y sistemas de almacenamiento, revisa los métodos de destrucción física. Interpreta el protocolo de retención de datos. Anula la información almacenada. Registra el procedimiento realizado. La persona candidata comete ligeras irregularidades que no alteran el resultado final.***
2	*Para eliminar información en soportes y sistemas de almacenamiento, revisa los métodos de destrucción física. Interpreta el protocolo de retención de datos. Anula la información almacenada. Registra el procedimiento realizado. La persona candidata, comete amplias irregularidades que alteran el resultado final.*
1	*No elimina información en soportes ni sistemas de almacenamiento.*

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

Escala C

4	*Para verificar la realización de copias de seguridad, comprueba la información del equipo informático. Verifica el plan de copias de seguridad. Comprueba los dispositivos de almacenamiento de copias de seguridad. Verifica los procedimientos de obtención y verificación de copias de seguridad.*
3	***Para verificar la realización de copias de seguridad, comprueba la información del equipo informático. Verifica el plan de copias de seguridad. Comprueba los dispositivos de almacenamiento de copias de seguridad. Verifica los procedimientos de obtención y verificación de copias de seguridad. La persona candidata comete ligeras irregularidades que no alteran el resultado final.***
2	*Para verificar la realización de copias de seguridad, comprueba la información del equipo informático. Verifica el plan de copias de seguridad. Comprueba los dispositivos de almacenamiento de copias de seguridad. Verifica los procedimientos de obtención y verificación de copias de seguridad. La persona candidata, comete amplias irregularidades que alteran el resultado final.*

1		*No verifica la realización de copias de seguridad.*

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

2. MÉTODOS DE EVALUACIÓN DEL 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.

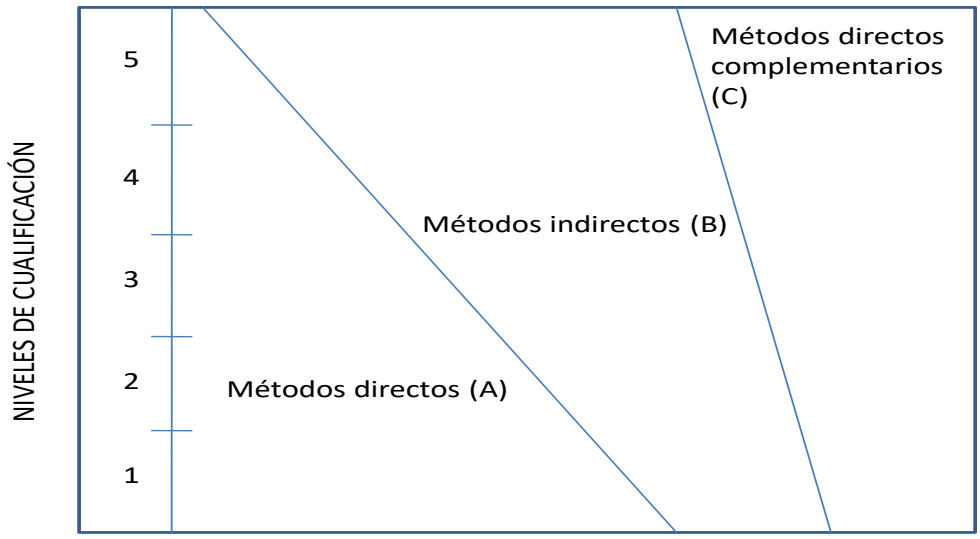
2.1. Métodos de evaluación y criterios generales de elección.

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 Asegurar equipos 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 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 "3" 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.