GUÍA DE EVIDENCIAS DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES

"ECP0487_3: Auditar redes de comunicación y sistemas 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 ECP0487_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 (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 auditar redes de comunicación y sistemas 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. Comprobar la seguridad de los sistemas informáticos, revisando el bastionado de las instalaciones, equipos y "software", para verificar la integridad, confidencialidad, disponibilidad,

trazabilidad y no repudio de la información gestionada, según indicaciones del plan de seguridad de la organización auditada.

1.1 El inventariado de activos se revisa, verificando los equipos existentes y sus características, comprobando las versiones de los programas que se ejecutan, para confirmar que está actualizado y no hay equipos ni programas que no aparezcan en el mismo.

1.2 La instalación y configuración de los sistemas operativos se revisa, confirmando que el "software" instalado es legítimo, está actualizado y tanto los usuarios como las aplicaciones cuentan con los permisos de "mínimo privilegio" para desempeñar sus funciones en el sistema.

1.3 La instalación y configuración de "software" de seguridad contra programas maliciosos tales como antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"), entre otros, se comprueba, verificando que dicho "software" es legítimo, está actualizado y tiene activas las funciones que indique el responsable de seguridad.

1.4 Las aplicaciones empleadas en la organización se revisan, comprobando licencias y versiones para confirmar que son legítimas, están actualizadas y que únicamente pueden ser accedidas por el personal autorizado, y que ese acceso tenga las limitaciones que indique el responsable de seguridad, basadas en el principio de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know").

1.5 Las cuentas de usuario de la organización se comprueban que son individuales, cuentan con una política de contraseñas robusta y han sido elaboradas bajo el principio de "mínimo privilegio" y segregación de funciones, modificando aquellas que no cumplen los criterios y eliminando las cuentas obsoletas o que no pertenecen a personas autorizadas.

1.6 Las instalaciones se comprueban de manera presencial para asegurarse de que los equipos y la información están protegidos contra accesos físicos no autorizados, usando elementos al efecto de manera separada o combinada tales como mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, aplicando un sistema de aviso previo y bloqueando sesiones por inactividad y usando políticas de "mesas limpias".

1.7 Las instalaciones se comprueban, verificando las condiciones ambientales de temperatura y humedad requeridas por el fabricante para su funcionamiento y la protección frente a desastres naturales que pueden afectar físicamente en el emplazamiento y previniendo posibles alteraciones del entorno tales como picos de electricidad o ruido eléctrico, entre otros.

1.8 Las pruebas realizadas durante la auditoría se documentan, incluyendo referencias a los activos del sistema, los parches y actualizaciones instalados en los sistemas operativos y aplicaciones, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

2. Comprobar la seguridad de la red de la organización auditada, verificando los elementos relativos indicados en el plan de seguridad, para prevenir posibles intrusiones, ataques y fugas de información.

2.1 El diseño de arquitectura de la red se revisa, mediante auditoría de caja blanca, comprobando que la red está configurada de forma que se minimice el impacto de posibles ataques del exterior: utilizando VLAN ("Virtual Local Área Networks"), cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), "routers" y otros dispositivo de red e instalado todos los recursos de la empresa que deben ser accesibles desde Internet tales como páginas web y correo electrónico, en una zona aislada o desmilitarizada (DMZ).

2.2 Los dispositivos que controlan y gestionan el tráfico de la red tales como "router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"), entre otros, se revisan, usando técnicas de caja blanca: de manera física y comprobando su configuración para verificar que únicamente aceptan el tráfico permitido y están actualizados.

2.3 Los mensajes de error generados por los dispositivos de red, "routers", "switch", "hub" cortafuegos, IDS, IPS, SIEM y cualquier otro, se revisan en forma de auditoría de caja blanca para asegurar que, de forma interna, registran cualquier anomalía para facilitar la gestión de incidentes y, de forma externa en modo auditoría de caja negra, para confirmar que no aportan información que permita a un posible atacante remoto obtener información de los puertos abiertos en el sistema.

2.4 Los elementos de la red se comprueban que únicamente son accedidos de forma remota por personal y bajo las condiciones de tiempo y lugar de origen, previamente autorizados en la política de seguridad y sólo a través de las VPN (Redes privadas Virtuales).

2.5 El uso de programas o herramientas en la nube se revisa, verificando que se lleva a cabo de la forma acordada con el proveedor del servicio y permitida dentro de la política de seguridad de la organización.

2.6 Las redes Wifi se comprueban, verificando que utilizan protocolos seguros de cifrado y que únicamente acceden a ellas las personas autorizadas en la política de seguridad.

2.7 La conexión a Internet por parte de los usuarios de la organización se comprueba, verificando que únicamente pueden acceder a los servicios y contenidos previamente autorizados en la política de seguridad.

2.8 Los sistemas anti DDoS (Denegación de servicio) de la organización se verifica que están habilitados y funcionales, comprobando si se han configurado sistemas al efecto tales como reglas de cortafuegos, sistemas de monitorización y/o servicios externos de protección, entre otros.

2.9 Las pruebas realizadas durante la auditoría se documentan, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

3. ***Comprobar la seguridad del sitio web, realizando pruebas de simulación de ataques para detectar posibles fallos de seguridad.***

   3.1 La instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores web se verifica, comprobando que están instaladas las últimas versiones estables y que únicamente tienen instalados los módulos imprescindibles para su funcionamiento, revisando la documentación asociada.
   3.2 Las cuentas de usuario del sitio web se comprueban, verificando que son generadas bajo el principio de "mínimo privilegio" y cuentan con una política de acceso segura.
   3.3 La información generada de forma pública por el servidor web y/o el sistema de gestión de contenidos (CMS) se verifica, comprobando que no muestre ninguna información que permita obtener fácilmente información relacionada con la configuración del sistema tal como tipo de programa empleado, versión, entre otros.
   3.4 La gestión de sesiones en el sistema se comprueba, verificando que tanto las "cookies" como los "tokens" de sesión se generan de forma segura y no predecible, tal como evitando la numeración secuencial para la identificación de usuarios, para impedir que un atacante externo pueda aprovecharse de ellas para acceder al sistema de forma no autorizada.
   3.5 Los formularios y puntos de acceso de información por parte del usuario se comprueban, verificando que cuentan con mecanismos que impidan la entrada de caracteres que provoquen un comportamiento no deseado del sistema como la introducción de código (por inyección de SQL o XSS -"Cross-site scripting"-, entre otros) o la generación de errores en el sistema tales como desbordamiento de "buffer" por introducción de cadenas largas.
   3.6 La gestión de errores y excepciones del sistema se comprueba, verificando que éstos son registrados y la información mostrada en el lado del cliente no revela información que pueda permitir a los usuarios una posterior explotación del fallo.
   3.7 La información entre el cliente y el servidor se comprueba que se envía de forma segura, verificando que se realiza a través de protocolos tales como HTTPS y TLS, que la información enviada se cifra, siguiendo estándares actualizados.
   3.8 Las pruebas realizadas durante la auditoría se documentan, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

4. ***Comprobar la seguridad de la información tratada por la organización auditada, verificando y asegurando los elementos relativos indicados en el plan de seguridad, para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y el "no***

repudio" y el cumplimiento de la normativa aplicable de protección de datos.

4.1 La asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos se comprueba, verificando que se accede a la información requerida en cada caso y su alineación con el principio de "mínimo privilegio" y "necesidad de saber".
4.2 Las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos se comprueban, verificando que se cumple con los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio.
4.3 El intercambio de información se comprueba, verificando que se realiza únicamente a través de los canales autorizados, de la forma convenida y por las personas definidas en la normativa de la organización.
4.4 El registro de actividades del tratamiento de los datos se revisa, verificando que está completo y actualizado, comprobando que el tratamiento únicamente se efectúa por personas autorizadas en la normativa de seguridad de la organización.
4.5 Los protocolos de eliminación de información se revisan, confirmando que garantizan el borrado seguro de la información, destruyendo el papel en máquinas y contenedores específicos que no permitan la recuperación de la información y, en caso de cesión de dispositivos digitales a terceros, que no se pueda acceder a la información contenida previamente en él.
4.6 La realización de copias de seguridad se verifica, comprobando que está alineado con la política de seguridad de la organización de forma que, ante una eliminación de datos por un desastre natural, o por personas de modo accidental o intencionado, es posible recuperar la información en los plazos de tiempo convenidos.
4.7 La aplicación de la normativa de seguridad por parte de los usuarios se revisa, verificando que saben cómo y dónde reportar los incidentes informáticos, no hacen uso de dispositivos no autorizados o de origen desconocido, aplican la política de "mesas limpias", bloquean el equipo si van a estar ausentes y no divulgan información asociada con su trabajo.
4.8 El informe de la auditoría se elabora, incluyendo el alcance de la misma, la documentación revisada, las pruebas y entrevistas realizadas, los posibles obstáculos encontrados y las evidencias obtenidas, presentando especial atención a los hallazgos clasificados y no conformidades de las que también se indicará su criticidad, detallando el grado de cumplimiento legal y las medidas de mejora convenientes.

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**0487_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. Normativa y estándares relacionados con la auditoría de seguridad

- Normativa aplicable de servicios de Internet
- Normativa aplicable de protección de datos
- Estándares aplicables a la auditoría.

2. Auditoría de seguridad en el aplicativo de sistemas informáticos

- Procedimientos de verificación del inventariado del aplicativo en equipos. "Software" de base, aplicaciones genéricas o específicas de seguridad. Comprobación y actualización de versiones. Comprobación de legitimidad del "software".
- Técnicas de revisión de la instalación y configuración de sistemas operativos. Parámetros y valores de configuración que afectan a la seguridad.
- Conceptos de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know"). Determinación del grado de cumplimiento en el acceso a aplicaciones.
- Clasificaciones de "software" de seguridad contra programas maliciosos. Antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"). Utilidad y ámbito de aplicación.
- Instalación y configuración de "software" de seguridad contra programas maliciosos. Parámetros y valores a comprobar. Verificación de Funciones activadas y desactivadas.
- Comprobación de cuentas de usuario de sistemas y aplicaciones. Robustez de contraseñas y aplicación del principio de "mínimo privilegio".
- Informes de auditoría de sistemas.

3. Auditoría de seguridad en equipos e instalaciones de un sistema informático

- Procedimientos de inventariado de activos y de verificación de equipos y sus características.
- Elementos de protección de instalaciones y equipos. Mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, de modo que se asegure que están protegidos contra accesos físicos no autorizados. Configuración y aplicación de manera separada o combinada.
- Aplicación de políticas de "mesas limpias". Puntos a comprobar.
- Verificación de condiciones ambientales de temperatura y humedad para un sistema o instalación.
- Verificación de protección frente a desastres en una instalación. Características de emplazamiento. Valoración de riesgos.
- Verificación de protecciones frente a alteraciones. Protección frente a caídas del suministro eléctrico, picos de electricidad y ruido.

4. Auditoría de seguridad en redes

- Intrusiones, ataques y fugas de información.
- Técnicas de diseño, herramientas y aplicaciones de protección de redes. VLAN, cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de

prevención de intrusiones (IPS), "routers" y otros dispositivos de red, y creación de una zona aislada o desmilitarizada (DMZ). Configuración y ámbito de aplicación.
- Revisión del diseño de la arquitectura de una red. auditorías de caja blanca y caja negra. Determinación de recursos accesibles. Zonas aisladas o desmilitarizadas (DMZ).
- Revisión de dispositivos que controlan y gestionan el tráfico de la red. "Router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"). Auditoría de caja blanca para comprobación de configuración. Auditoría de caja negra para comprobación del acceso y visibilidad.
- Interpretación de mensajes de error generados por los dispositivos de red.
- Comprobación de acceso. Garantía de acceso únicamente a personal autorizado. Condiciones de tiempo y lugar de origen. VPN (Redes privadas Virtuales).
- Formas de uso de programas o herramientas en la nube según proveedores. Comprobaciones de cumplimiento de la seguridad.
- Protocolos de cifrado seguros en redes Wifi. Verificación de configuración de acceso.
- Comprobación de conexión hacia Internet. Verificación de acceso a servicios y contenidos para determinados usuarios.
- Verificación de la protección anti DDoS (Denegación del servicio).
- Informes de auditoría de la red.

5. Auditoría de seguridad web

- Verificación de la instalación y configuración de sistemas de gestión de contenidos (CMS) y servidores web.
- Comprobación de cuentas de usuario de un sitio web. Garantía del principio de "mínimo privilegio". Robustez de la política de contraseñas. Autenticación multifactor (MFA).
- Verificación de la información pública de un servidor web y/o un sistema de gestión de contenidos (CMS). Comprobaciones de visibilidad de información: tipo de programa y versión, entre otros.
- Procedimientos de comprobación de la gestión de sesiones en el sistema. Verificación de "cookies" y "tokens" de sesión seguros y no predecibles.
- Verificación de mecanismos de protección ante entradas de caracteres que provoquen un comportamiento no deseado del sistema. Introducción de código (por inyección de SQL o XSS, entre otros).
- Comprobación de protección ante generación de errores en el sistema. Desbordamiento de "buffer".
- Verificación de la gestión de errores y excepciones del sistema. Registro. Visibilidad de la información mostrada en el lado del cliente.
- Comprobación de envío seguro de la información entre el cliente y el servidor. Uso de protocolos tales como HTTPS y TLS. Cifrado de información enviada. Estándares.
- Informes de auditoría web.
- Sistemas WAF ("Web Application Firewall").

6. Auditoría de protección de datos

- Integridad, disponibilidad, confidencialidad, autenticidad, "no repudio" y trazabilidad de procesos.

- Comprobación de la asignación de roles de usuarios responsables de la gestión, tratamiento y almacenamiento de los datos. Alineación con el principio de "mínimo privilegio" y "necesidad de saber".
- Comprobación de medidas de seguridad físicas y lógicas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos.
- Comprobaciones sobre el intercambio de información. Canales y control del acceso.
- Verificación del registro de actividades de tratamiento de datos. Comprobaciones de completitud y grado de actualización. Verificación del acceso por personas autorizadas.
- Verificación del borrado seguro de la información. Destrucción de soportes. Herramientas de borrado permanente. Contenedores específicos de soportes desechados.
- Revisión y verificación de usos y costumbres del usuario que afectan a la seguridad.
- Verificación de la realización de copias de seguridad.
- Informes de auditoría de protección de datos.

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.
- Respetar los procedimientos y normas internas de 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 "ECP0487_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 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 la protección de equipos informáticos contra la pérdida, manipulación y sustracción de información.

2. Comprobar la seguridad de la red de la organización.

3. Comprobar la seguridad del sitio "web".

4. Comprobar el plan de seguridad y la información tratada por la organización auditada.

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 en la configuración la protección de equipos informáticos contra la pérdida, manipulación y sustracción de información.	- Revisión del inventariado de activos, equipos existentes y versiones de los programas que se ejecutan. - Revisión de la instalación y configuración de los sistemas operativos. - Configuración de la política de contraseñas, su complejidad, caducidad, revocación, bloqueo, reutilización, entre otros. - Comprobación del establecimiento del control de acceso al equipo informático: intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros. - Revisión del refuerzo de la seguridad del equipo informático ante ataques externos: cortafuegos y reglas de filtrado. - Comprobación presencial de la protección contra accesos físicos no autorizados. *El umbral de desempeño competente está explicitado en la Escala A*
Rigor en la comprobación de la seguridad de la red de la organización.	- Revisión del diseño de arquitectura de la red. - Revisión de los dispositivos que controlan y gestionan el tráfico de la red. - Revisión de los mensajes de error generados por los dispositivos de red. - Comprobación del acceso a los elementos de la red. - Revisión del uso de programas o herramientas en la nube. - Verificación de las redes WIFI. - Comprobación de la conexión a Internet por parte de los usuarios de la organización. - Verificación de los sistemas anti DDoS (Denegación de servicio) de la organización. - Documentación de las pruebas realizadas durante la auditoría. *El umbral de desempeño competente está explicitado en la Escala B*

Exhaustividad en la comprobación de la seguridad del sitio "web".	- Verificación de las veriones y módulos de instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores "web". - Comprobación de la política de acceso de las cuentas de usuario del sitio "web". - Verificación de la información generada de forma pública por el servidor "web" y/o el sistema de gestión de contenidos (CMS). - Comprobación de la seguridad en la generación de los tokens de sesión en el sistema. - Comprobación de la limitación de inyección de caracteres no previstos en los formularios y puntos de acceso de información por parte del usuario. - Comprobación presencial de la protección contra accesos físicos no autorizados. - Comprobación de la seguridad del envío de información entre el cliente y el servidor. - Documentación de las pruebas realizadas durante la auditoría y las contramedidas aplicadas. *El umbral de desempeño competente está explicitado en la Escala C*
Rigor en la comprobación del plan de seguridad y la información tratada por la organización auditada.	- Comprobación de la asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos. - Comprobación de las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos. - Comprobación del intercambio de información. - Revisión del registro de actividades del tratamiento de los datos. - Revisión de los protocolos de eliminación de información . - Verificación de la realización de copias de seguridad. - Revisión de la aplicación de la normativa de seguridad por parte de los usuarios. - Elaboración del informe de la auditoría. *El umbral de desempeño competente está explicitado en la Escala D*
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 comprobar la seguridad de los sistemas informáticos, instalaciones, equipos y "software", revisa el inventariado de activos, equipos existentes y versiones de los programas que se ejecutan, revisa la instalación y configuración de los sistemas operativos, configura la política de contraseñas, su complejidad, caducidad, revocación, bloqueo, reutilización, entre otros., comprueba el establecimiento del control de acceso al equipo informático: intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros, revisa el refuerzo de la seguridad del equipo informático ante ataques externos: cortafuegos y reglas de filtrado, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba las condiciones ambientales y la protección frente a desastres naturales de las instalaciones, documenta las pruebas realizadas durante la auditoría.*
3	***Para comprobar la seguridad de los sistemas informáticos, instalaciones, equipos y "software", revisa el inventariado de activos, equipos existentes y versiones de los programas que se ejecutan, revisa la instalación y configuración de los sistemas operativos, configura la política de contraseñas, su complejidad, caducidad, revocación, bloqueo, reutilización, entre otros., comprueba el establecimiento del control de acceso al equipo informático: intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros, revisa el refuerzo de la seguridad del equipo informático ante ataques externos: cortafuegos y reglas de filtrado, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba las condiciones ambientales y la protección frente a desastres naturales de las instalaciones, documenta las pruebas realizadas durante la auditoría, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para comprobar la seguridad de los sistemas informáticos, instalaciones, equipos y "software", revisa el inventariado de activos, equipos existentes y versiones de los programas que se ejecutan, revisa la instalación y configuración de los sistemas operativos, configura la política de contraseñas, su complejidad, caducidad, revocación, bloqueo, reutilización, entre otros., comprueba el establecimiento del control de acceso al equipo informático: intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros, revisa el refuerzo de la seguridad del equipo informático ante ataques externos: cortafuegos y reglas de filtrado, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba las condiciones ambientales y la protección frente a desastres naturales de las instalaciones, documenta las pruebas realizadas durante la auditoría, pero comete amplias irregularidades que alteran el resultado final.*
1	*No comprueba la seguridad de los sistemas informáticos, instalaciones, equipos y "software", revisa el inventariado de activos, equipos existentes y versiones de los programas que se ejecutan, revisa la instalación y configuración de los sistemas operativos, configura la política de contraseñas, su complejidad, caducidad, revocación, bloqueo, reutilización, entre otros., comprueba el establecimiento del control de acceso al equipo informático: intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros, revisa el refuerzo de la seguridad del equipo informático ante ataques externos: cortafuegos y reglas de filtrado, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba las condiciones ambientales y la protección frente a desastres naturales de las instalaciones, documenta las pruebas realizadas durante la auditoría.*

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

Escala B

4	*Para comprobar la seguridad de la red de la organización, revisa el diseño de arquitectura de la red, revisa los dispositivos que controlan y gestionan el tráfico de la red, revisa los mensajes de error generados por los dispositivos de red, comprueba el acceso a los elementos de la red, revisa el uso de programas o herramientas en la nube, verifica las redes WIFI, comprueba la conexión a Internet por parte de los usuarios de la organización, verifica los sistemas anti DDoS (Denegación de servicio) de la organización.*
3	***Para comprobar la seguridad de la red de la organización, revisa el diseño de arquitectura de la red, revisa los dispositivos que controlan y gestionan el tráfico de la red, revisa los mensajes de error generados por los dispositivos de red, comprueba el acceso a los elementos de la red, revisa el uso de programas o herramientas en la nube, verifica las redes WIFI, comprueba la conexión a Internet por parte de los usuarios de la organización, verifica los sistemas anti DDoS (Denegación de servicio) de la organización, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para comprobar la seguridad de la red de la organización, revisa el diseño de arquitectura de la red, revisa los dispositivos que controlan y gestionan el tráfico de la red, revisa los mensajes de error generados por los dispositivos de red, comprueba el acceso a los elementos de la red, revisa el uso de programas o herramientas en la nube, verifica las redes WIFI, comprueba la conexión a Internet por parte de los usuarios de la organización, verifica los sistemas anti DDoS (Denegación de servicio) de la organización, pero comete amplias irregularidades que alteran el resultado final.*
1	*No comprueba la seguridad de la red de la organización, revisa el diseño de arquitectura de la red, revisa los dispositivos que controlan y gestionan el tráfico de la red, revisa los mensajes de error generados por los dispositivos de red, comprueba el acceso a los elementos de la red, revisa el uso de programas o herramientas en la nube, verifica las redes WIFI, comprueba la conexión a Internet por parte de los usuarios de la organización, verifica los sistemas anti DDoS (Denegación de servicio) de la organización*

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

Escala C

4	*Para comprobar la seguridad del sitio "web", verifica las versiones y módulos de instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores "web", comprueba la política de acceso de las cuentas de usuario del sitio "web", verfica la información generada de forma pública por el servidor "web" y/o el sistema de gestión de contenidos (CMS), comprueba la seguridad en la generación de los tokens de sesión en el sistema, comprueba la limitación de inyección de caracteres no previstos en los formularios y puntos de acceso de información por parte del usuario,*

	comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba la seguridad del envío de información entre el cliente y el servidor, documenta las pruebas realizadas durante la auditoría y las contramedidas aplicadas.
3	***Para comprobar la seguridad del sitio "web", verifica las versiones y módulos de instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores "web", comprueba la política de acceso de las cuentas de usuario del sitio "web", verfica la información generada de forma pública por el servidor "web" y/o el sistema de gestión de contenidos (CMS), comprueba la seguridad en la generación de los tokens de sesión en el sistema, comprueba la limitación de inyección de caracteres no previstos en los formularios y puntos de acceso de información por parte del usuario, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba la seguridad del envío de información entre el cliente y el servidor, documenta las pruebas realizadas durante la auditoría y las contramedidas aplicadas, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para comprobar la seguridad del sitio "web", verifica las versiones y módulos de instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores "web", comprueba la política de acceso de las cuentas de usuario del sitio "web", verfica la información generada de forma pública por el servidor "web" y/o el sistema de gestión de contenidos (CMS), comprueba la seguridad en la generación de los tokens de sesión en el sistema, comprueba la limitación de inyección de caracteres no previstos en los formularios y puntos de acceso de información por parte del usuario, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba la seguridad del envío de información entre el cliente y el servidor, documenta las pruebas realizadas durante la auditoría y las contramedidas aplicadas, pero comete amplias irregularidades que alteran el resultado final.*
1	*No comprueba la seguridad del sitio "web", verifica las versiones y módulos de instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores "web", comprueba la política de acceso de las cuentas de usuario del sitio "web", verfica la información generada de forma pública por el servidor "web" y/o el sistema de gestión de contenidos (CMS), comprueba la seguridad en la generación de los tokens de sesión en el sistema, comprueba la limitación de inyección de caracteres no previstos en los formularios y puntos de acceso de información por parte del usuario, comprueba presencialmente la protección contra accesos físicos no autorizados, comprueba la seguridad del envío de información entre el cliente y el servidor, documenta las pruebas realizadas durante la auditoría y las contramedidas aplicadas.*

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

Escala D

4	*Para comprobar el, plan de seguridad y la información tratada por la organización auditada, comprueba la asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos, comprueba las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, comprueba el intercambio de información, revisa el registro de actividades del tratamiento de los datos, revisa los protocolos de eliminación de información, verifica la realización de copias de*

	seguridad, revisa la aplicación de la normativa de seguridad por parte de los usuarios, elabora el informe de la auditoría.
3	***Para comprobar el plan de seguridad y la información tratada por la organización auditada, comprueba la asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos, comprueba las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, comprueba el intercambio de información, revisa el registro de actividades del tratamiento de los datos, revisa los protocolos de eliminación de información, verifica la realización de copias de seguridad, revisa la aplicación de la normativa de seguridad por parte de los usuarios, elabora el informe de la auditoría, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para comprobar el plan de seguridad y la información tratada por la organización auditada, comprueba la asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos, comprueba las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, comprueba el intercambio de información, revisa el registro de actividades del tratamiento de los datos, revisa los protocolos de eliminación de información , verifica la realización de copias de seguridad, revisa la aplicación de la normativa de seguridad por parte de los usuarios, elabora el informe de la auditoría, pero comete amplias irregularidades que alteran el resultado final.*
1	*No comprueba el plan de seguridad y la información tratada por la organización auditada, comprueba la asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos, comprueba las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, comprueba el intercambio de información, revisa el registro de actividades del tratamiento de los datos, revisa los protocolos de eliminación de información , verifica la realización de copias de seguridad, revisa la aplicación de la normativa de seguridad por parte de los usuarios, elabora el informe de la auditoría.*

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.

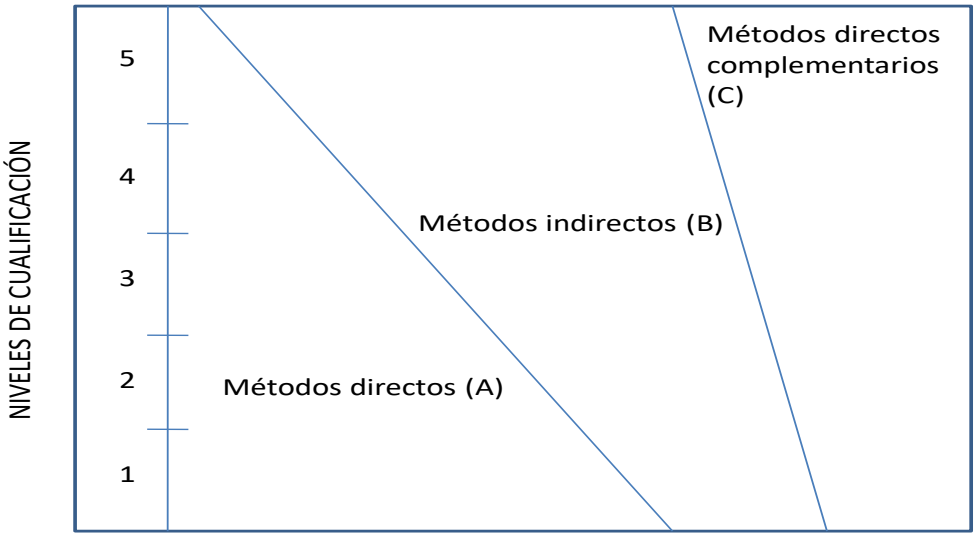
2.1. Métodos de evaluación y criterios generales de elección.

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 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 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) 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.