GUÍA DE EVIDENCIAS DEL ESTÁNDAR DE COMPETENCIAS PROFESIONLES

“ECP0489_3: Implementar sistemas seguros de acceso y transmisión de datos”

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 ECP0489_3: Implementar sistemas seguros de acceso y transmisión de datos.

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 implementar sistemas seguros de acceso y transmisión de datos, 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. Implantar protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso,

garantizando la integridad y confidencialidad de la información, así como el control de acceso, para obtener comunicaciones o canales de comunicación seguros, cumpliendo las directivas del departamento responsable de la seguridad del sistema informático.

1.1 La confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas se garantiza, haciendo uso de redes privadas virtuales, comunicándolos al proveedor del servicio para lograr soluciones ajustadas al plan de seguridad.
1.2 Las técnicas de protección de conexiones inalámbricas disponibles en el mercado se aplican, seleccionando aquellas basadas en estándares reconocidos como confiables en el sector, para cubrir vulnerabilidades, teniendo en cuenta el principio de proporcionalidad.
1.3 Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones se implantan, diferenciando usuarios por perfiles y asignándoles permisos según ese perfil.
1.4 Los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas se protegen, usando herramientas disponibles para el cifrado extremo a extremo, para garantizar la seguridad de las comunicaciones.
1.5 La identidad de los servidores se garantiza en aquellos servicios que lo soportan, usando certificados digitales, configurando las aplicaciones cliente con el certificado raíz de confianza que garantice al usuario la autenticidad del servidor.
1.6 Las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas se documentan, incluyendo las características de las configuraciones aplicadas, ajustándolo a estándares y/o en el formato establecido en la organización.
1.7 Los servicios, cuyo nivel riesgo estime el departamento entidad responsable de la gestión de la seguridad del sistema informático que lo requieran, se aseguran incorporando una autenticación de doble o triple factor basada en certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos.
1.8 Los servicios en los que se utiliza autenticación basada en contraseñas, se configuran, estableciendo políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

2. Implantar el uso de sistemas de firma y certificados de persona para asegurar la autenticidad, integridad, confidencialidad y "no repudio" de los datos que intervienen en una transferencia de información personal según las necesidades de uso y dentro de las directivas del departamento responsable de la seguridad del sistema informático.

2.1 El acceso a servicios a través de la red telemática se implanta de forma que asegure la autenticación mutua de cliente y servidor, utilizando autenticación de la clientela basada en certificados digitales de

identidad personal cuando la política de seguridad de la organización así lo requiera.

2.2 El proceso de obtención y verificación de certificados digitales de identidad personal se aplica, siguiendo los pasos establecidos por la entidad certificadora y con la periodicidad indicada por el departamento responsable de la seguridad del sistema.

2.3 Los mecanismos para la transmisión cifrada del correo electrónico y otras comunicaciones, ya sea interpersonales o entre procesos y/o componentes, se implementan empleando certificados digitales para firmar y cifrar extremo a extremo el contenido de dichos mensajes, en los casos que indique la política de seguridad de la organización.

2.4 Los mecanismos de firma digital de documentos seleccionados de acuerdo con la política de seguridad del departamento responsable se aplican, incluyendo dicha firma en el momento del envío o, en su caso, al almacenar cada documento.

2.5 Los sistemas de sellado digital de tiempo se implantan, aplicándolos a los documentos que requiera la seguridad de la organización, para garantizar la existencia de un documento electrónico en un instante concreto, garantizando que la información contenida no ha sido alterada por terceros.

2.6 La integridad de los componentes en sitios web y del "software" interno se garantiza, firmándolos mediante firma digital, según el procedimiento del sistema o herramientas de firmado.

2.7 Los sistemas de firma digital implantados se documentan indicando su ámbito de aplicación, el procedimiento para su uso, la tipología de documentos, aplicaciones a firmar y el sistema de firma aplicado, entre otros, siguiendo estándares y de acuerdo con el formato establecido en la organización.

3. Implementar infraestructuras de clave pública, siguiendo instrucciones del fabricante y en función de las condiciones de uso, para garantizar la seguridad, según los estándares del sistema y dentro de las directivas de la organización.

3.1 La jerarquía de certificación se instala configurando la herramienta que la implementa, siguiendo las instrucciones del proveedor, en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.

3.2 La declaración de prácticas de certificación y la política de certificación se redacta, definiendo los procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.

3.3 El sistema de autoridad de certificación se instala, siguiendo las indicaciones del fabricante, las prácticas recomendadas del sector y la política de seguridad de la organización.

3.4 El certificado digital de la autoridad de certificación y su política asociada se ponen a disposición de los usuarios, siguiendo las directrices contenidas en la declaración de prácticas de certificación.

3.5 La clave privada de la autoridad de certificación se almacena, manteniéndola segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.
3.6 Los certificados digitales se emiten según los usos que van a recibir los certificados y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.
3.7 La validez de los certificados emitidos por la autoridad de certificación se comprueba, verificando que es mantenido por el servicio de revocación de certificados, según lo indicado en la declaración de prácticas de certificación.
3.8 Las infraestructuras de clave pública implantadas se documentan recogiendo sus datos de configuración, ajustándose a estándares y según el formato establecido en la organización.

4. Revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos según las directrices de la entidad responsable de la gestión de la red.

4.1 La topología de la red se adapta según las necesidades de seguridad, valorando su idoneidad mediante el análisis de modelos de referencia estándar, seleccionando una nueva topología y añadiendo o suprimiendo dispositivos de comunicaciones para minimizar posibles riesgos.
4.2 La red de la organización se segmenta de acuerdo con la compartimentación organizativa, la identidad de los equipos o usuarios y la política de seguridad de la entidad responsable, ya sea de forma física, mediante equipos tales como "routers", o de forma lógica utilizando VLAN ("Virtual Local Área Networks").
4.3 Las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, se establecen de acuerdo con la segmentación establecida y la política de seguridad de la organización.
4.4 Los mecanismos de protección para las redes de acceso, ante elementos que rompen con el perímetro tradicional de la red corporativa, tales como redes inalámbricas, dispositivos móviles y portátiles, particulares o corporativos, con conexión a las redes de la organización se establecen identificando los dispositivos empleados, delimitando su alcance y protegiendo el acceso mediante cifrado seguro, de acuerdo con la política de seguridad de la organización.
4.5 Los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention") se implementan mediante "hardware" o "software" al efecto, en virtud de los requisitos de seguridad de la organización, para detectar potenciales brechas en el acceso y/o transmisión de datos y prevenirlas a través del monitoreo, detección y bloqueo de información sensible.
4.6 El diseño de la red se modifica en su caso, introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, bien

duplicando la red física, equipos y "software", bien mediante la virtualización de sistemas.

4.7 Los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal se configuran, asegurando una transmisión de datos confiable y segura entre los distintos nodos que la conforman.

4.8 Los procedimientos de salvaguarda de configuraciones se revisan modificando, en su caso, la programación de sus copias de seguridad mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y permitiendo una eficaz recuperación.

4.9 La documentación de configuración de seguridad se elabora incluyendo todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.

5. Revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, actualizándolo, añadiendo o suprimiendo elementos y/o modificando configuraciones, para garantizar la seguridad de las comunicaciones y la protección de los datos, según las directrices de la organización.

5.1 El "software" de comunicaciones que se ejecuta en los dispositivos de red se evalúa, valorando su compatibilidad, teniendo en cuenta su funcionalidad y su idoneidad para el diseño a corto y medio plazo, comprobando su integridad, legitimidad y grado de actualización para corregir problemas de seguridad.

5.2 Los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies" se incluyen en el diseño de la red, comparando prestaciones y características e interpretando la documentación técnica asociada.

5.3 Los procedimientos de salvaguarda del "software" se revisan, modificando en su caso la programación de los "backup", almacenándolos en condiciones de seguridad y permitiendo una eficaz recuperación.

5.4 Los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros se revisan, ajustándolos de forma que garanticen la seguridad, la trazabilidad de los parámetros y las definiciones de configuración, estableciendo protocolos para el cambio cíclico de contraseñas fijas que no caducan, estableciendo mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde puntos permitidos y por administradores autorizados.

5.5 La configuración de seguridad en el ámbito de red se aplica garantizando el funcionamiento de puntos críticos, tales como la seguridad de puerto y configurando los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree"), protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR), entre otros.

5.6 La documentación del "software" de seguridad se elabora incluyendo productos, referencias y todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.

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**0489_3: Implementar sistemas seguros de acceso y transmisión de datos**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Normativa y estándares relacionados con el acceso y la transmisión de datos

- Normativa aplicable de protección de datos
- Estándares de seguridad relacionados con tecnologías específicas de acceso y transmisión de datos.

2. Implantación de protocolos y herramientas en operaciones de intercambio de datos

- Seguridad de la información y criptografía. Cifrado de clave simétrica. Cifrado de clave pública y firma.
- Técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones.
- Herramientas de cifrado extremo a extremo.
- Redes privadas virtuales. IP Security Protocol. Túneles cifrados. Configuración.
- Protección de conexiones inalámbricas. Vulnerabilidades y protección. Protocolos. "Principio de proporcionalidad".
- Implantación y configuración de certificados digitales de servidores.
- Técnicas de seguridad para la autenticación de doble o triple factor. Certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos.
- Autenticación basada en contraseñas. Políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.

3. Implantación del uso de sistemas de firma y certificados de persona

- Procedimientos de acceso a servicios a través de una red telemática. Autenticación mutua de cliente y servidor. Autenticación del cliente basada en certificados digitales de identidad personal.
- Proceso de obtención y verificación de certificados digitales de identidad personal. Entidades certificadoras.
- Transmisión cifrada del correo electrónico y comunicaciones interpersonales o entre procesos y/o componentes. Firma y cifrado extremo a extremo.
- Firma digital de documentos. Herramientas.
- Sistemas de sellado digital de tiempo.

- Garantía de integridad en componentes web y "software" mediante firma digital.

4. Implementación de infraestructuras de clave pública

- Infraestructura de clave pública (PKI).
- Política de certificado y declaración de prácticas de certificación. Procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.
- Jerarquías de autoridades de certificación. Emisión de certificados digitales. Usos.
- Comprobación de validez de los certificados. Servicio de revocación de certificados.
- Infraestructuras de gestión de privilegios (PMI).

5. Seguridad de la red de área local Topología y "Hardware"

- Modelos de referencia estándar en lo concerniente a la seguridad.
- Dispositivos de comunicaciones y configuración segura.
- Topologías seguras. Subredes perimetrales de aislamiento o desmilitarizadas (DMZ).
- Técnicas de segmentación de una red. Técnicas físicas y lógicas (VLAN).
- Filtrado perimetral entre segmentos de red y entre máquinas específicas. Reglas de filtrado.
- Redes inalámbricas y dispositivos móviles y portátiles. Protección contra rotura del perímetro de la red.
- Prevención de fuga de datos (DLP: "Data Loss Prevention"). "Hardware" y "software" de detección y prevención de brechas. Monitoreo, detección y bloqueo de información sensible.
- Redundancia en red troncal. Alta disponibilidad.
- Procedimientos de salvaguarda de configuraciones. Periodicidad del proceso. Almacenamiento seguro. Restauración de copias.

6. "Software" de comunicaciones en red y el control de acceso

- Taxonomía de "software" de comunicaciones. Comprobaciones de integridad, legitimidad y actualización.
- Cortafuegos ("firewalls") y "proxies".
- Procedimientos de salvaguarda del "software". Periodicidad. Almacenamiento seguro. Restauración de copias.
- Identificación de accesos a la red y a la administración de los equipos. Autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros. Configuración de políticas para contraseñas.
- Seguridad de puerto y los mecanismos de control de tormentas de difusión. Protocolo de árbol de expansión ("spanning-tree"). Protocolos de redundancia ("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR),

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:

- Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
- Adaptarse a la organización, a sus cambios organizativos y tecnológicos, así como a situaciones o contextos nuevos.
- Mantener una actitud asertiva, empática y conciliadora con las personas demostrando cordialidad y amabilidad en el trato.
- Mostrar iniciativa en la búsqueda de soluciones y en la resolución de problemas.
- 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 "ECP0489_3: Implementar sistemas seguros de acceso y transmisión de datos", 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 implementar sistemas seguros de acceso y transmisión de datos, 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. Implantar protocolos y herramientas en operaciones de intercambio seguro de datos.

2. Implantar el uso de sistemas de firma y certificados de persona.

3. Implementar infraestructuras de clave pública.

4. Revisar la seguridad del "hardware" y el diseño de la red de área local.

5. Revisar el "software" de comunicaciones en red y el control de acceso de manera periódica.

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***
Eficacia en la implantación de protocolos y herramientas en operaciones de intercambio seguro de datos.	- Garantía de la confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas se garantiza, haciendo uso de redes privadas virtuales. - Aplicación de las técnicas de protección de conexiones inalámbricas. - Implantación de los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para

	garantizar la integridad y confidencialidad de las comunicaciones. - Protección de los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas con herramientas para cifrado extremo a extremo. - Garantía de la identidad de los servidores usando certificados digitales. - Documentación de las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas. - Aseguramiento mediante autenticación de doble o triple factor de los servicios, cuyo nivel riesgo lo requiera. - Configuración los servicios en los que se utiliza autenticación basada en contraseñas. *El umbral de desempeño competente está explicitado en la Escala A*
Eficacia en la implantación del uso de sistemas de firma y certificados de persona.	- Implantación del acceso a servicios a través de la red telemática mediante certificados digitales de identidad personal. - Aplicación del proceso de obtención y verificación de certificados digitales de identidad personal. - Implantación de los certificados digitales extremo a extremo para la transmisión cifrada del correo electrónico y otras comunicaciones. - Aplicación del los mecanismos de firma digital de documentos. - Implantación de los sistemas de sellado digital de tiempo. - Garantía de la integridad de los componentes en sitios "web" y del "software" interno. - Documentación de los sistemas de firma digital implantados. *El umbral de desempeño competente está explicitado en la Escala B*
Eficacia en la implantación del infraestructuras de clave pública.	- Instalación de la jerarquía de certificación. - Redacción de la declaración de prácticas de certificación y la política de certificación. - Instalación del sistema de autoridad de certificación. - Puesta a disposición de los usuarios del certificado digital de la autoridad de certificación y su política asociada. - Almacenaje de la clave privada de la autoridad de certificación. - Emisión de los certificados digitales.

	- Comprobación de La validez de los certificados emitidos por la autoridad de certificación. - Documentación de las infraestructuras de clave pública implantadas. *El umbral de desempeño competente está explicitado en la Escala C*
Exhaustividad en la revisión de la seguridad del "hardware" y el diseño de la red de área local.	- Adaptación de la topología de la red según las necesidades de seguridad. - Segmentado de la red de la organización de acuerdo con la política de seguridad. - Establecimiento de las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas. - Establecimiento de los mecanismos de protección para las redes de acceso. - Implementación de los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"). - Modificación del diseño de la red introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos. - Configuración de los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal. - Revisión de los procedimientos de salvaguarda de configuraciones. - Elaborción de la documentación de configuración de seguridad. *El umbral de desempeño competente está explicitado en la Escala D*
Rigor en la revisión del "software" de comunicaciones en red y el control de acceso de manera periódica.	- Evaluación del "software" de comunicaciones que se ejecuta en los dispositivos de red. - Inclusión en el diseño de la red de los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies". - Revisión de los procedimientos de salvaguarda del "software". - Revisión de los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros. - Aplicación de la configuración de seguridad en el ámbito de puntos críticos de red.

	- Elaboración de la documentación del "software" de seguridad. *El umbral de desempeño competente está explicitado en la Escala E*
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 implantar, protocolos y herramientas en operaciones de intercambio seguro de datos, garantiza la confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas haciendo uso de redes privadas virtuales, aplica las técnicas de protección de conexiones inalámbricas, implantar los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones, protege los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas con herramientas para cifrado extremo a extremo, garantiza la identidad de los servidores usando certificados digitales, documenta las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas, asegura mediante autenticación de doble o triple factor de los servicios, cuyo nivel riesgo lo requiera, configura los servicios en los que se utiliza autenticación basada en contraseñas.*
3	***Para implantar protocolos y herramientas en operaciones de intercambio seguro de datos, garantiza la confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas haciendo uso de redes privadas virtuales, aplica las técnicas de protección de conexiones inalámbricas, implantar los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones, protege los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas con herramientas para cifrado extremo a extremo, garantiza la identidad de los servidores usando certificados digitales, documenta las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas, asegura mediante autenticación de doble o triple factor de los servicios, cuyo nivel riesgo lo requiera, configura los servicios en los que se utiliza autenticación basada en contraseñas, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para implantar protocolos y herramientas en operaciones de intercambio seguro de datos, garantiza la confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas haciendo uso de redes privadas virtuales, aplica las técnicas de protección de conexiones inalámbricas, implantar los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones, protege los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas con herramientas para cifrado extremo a extremo, garantiza la identidad de los servidores usando*

	certificados digitales, documenta las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas, asegura mediante autenticación de doble o triple factor de los servicios, cuyo nivel riesgo lo requiera, configura los servicios en los que se utiliza autenticación basada en contraseñas, pero comete amplias irregularidades que alteran el resultado final.
1	*No implanta protocolos y herramientas en operaciones de intercambio seguro de datos, garantiza la confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas haciendo uso de redes privadas virtuales, aplica las técnicas de protección de conexiones inalámbricas, implantar los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones, protege los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas con herramientas para cifrado extremo a extremo, garantiza la identidad de los servidores usando certificados digitales, documenta las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas, asegura mediante autenticación de doble o triple factor de los servicios, cuyo nivel riesgo lo requiera, configura los servicios en los que se utiliza autenticación basada en contraseñas.*

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

Escala B

4	*Para implantar el, uso de sistemas de firma y certificados de persona, implanta el acceso a servicios a través de la red telemática mediante certificados digitales de identidad personal, aplica el proceso de obtención y verificación de certificados digitales de identidad personal, implanta los certificados digitales extremo a extremo para la transmisión cifrada del correo electrónico y otras comunicaciones, aplica los mecanismos de firma digital de documentos, implanta los sistemas de sellado digital de tiempo, garantiza la integridad de los componentes en sitios "web" y del "software" interno, documentar los sistemas de firma digital implantados.*
3	***Para implantar el uso de sistemas de firma y certificados de persona, implanta el acceso a servicios a través de la red telemática mediante certificados digitales de identidad personal, aplica el proceso de obtención y verificación de certificados digitales de identidad personal, implanta los certificados digitales extremo a extremo para la transmisión cifrada del correo electrónico y otras comunicaciones, aplica los mecanismos de firma digital de documentos, implanta los sistemas de sellado digital de tiempo, garantiza la integridad de los componentes en sitios "web" y del "software" interno, documentar los sistemas de firma digital implantados, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para implantar el uso de sistemas de firma y certificados de persona, implanta el acceso a servicios a través de la red telemática mediante certificados digitales de identidad personal, aplica el proceso de obtención y verificación de certificados digitales de identidad personal, implanta los certificados digitales extremo a extremo para la transmisión cifrada del correo electrónico y otras comunicaciones, aplica los mecanismos de firma digital de documentos, implanta los sistemas de sellado digital de tiempo, garantiza la integridad de los componentes en sitios "web" y del "software" interno, documentar los sistemas de firma digital implantados, pero comete amplias irregularidades que alteran el resultado final.*

1	*No implanta el uso de sistemas de firma y certificados de persona, implanta el acceso a servicios a través de la red telemática mediante certificados digitales de identidad personal, aplica el proceso de obtención y verificación de certificados digitales de identidad personal, implanta los certificados digitales extremo a extremo para la transmisión cifrada del correo electrónico y otras comunicaciones, aplica los mecanismos de firma digital de documentos, implanta los sistemas de sellado digital de tiempo, garantiza la integridad de los componentes en sitios "web" y del "software" interno, documentar los sistemas de firma digital implantados.*

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

Escala C

4	*Para implementar, infraestructuras de clave pública, instala la jerarquía de certificación, redacta la declaración de prácticas de certificación y la política de certificación, instala el sistema de autoridad de certificación, pone a disposición de los usuarios el certificado digital de la autoridad de certificación y su política asociada, almacena la clave privada de la autoridad de certificación, emite los certificados digitales, comprueba La validez de los certificados emitidos por la autoridad de certificación, documenta las infraestructuras de clave pública implantadas.*
3	***Para implementar infraestructuras de clave pública, instala la jerarquía de certificación, redacta la declaración de prácticas de certificación y la política de certificación, instala el sistema de autoridad de certificación, pone a disposición de los usuarios el certificado digital de la autoridad de certificación y su política asociada, almacena la clave privada de la autoridad de certificación, emite los certificados digitales, comprueba La validez de los certificados emitidos por la autoridad de certificación, documenta las infraestructuras de clave pública implantadas, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para implementar infraestructuras de clave pública, instala la jerarquía de certificación, redacta la declaración de prácticas de certificación y la política de certificación, instala el sistema de autoridad de certificación, pone a disposición de los usuarios el certificado digital de la autoridad de certificación y su política asociada, almacena la clave privada de la autoridad de certificación, emite los certificados digitales, comprueba La validez de los certificados emitidos por la autoridad de certificación, documenta las infraestructuras de clave pública implantadas, pero comete amplias irregularidades que alteran el resultado final.*
1	*No implementa infraestructuras de clave pública, instala la jerarquía de certificación, redacta la declaración de prácticas de certificación y la política de certificación, instala el sistema de autoridad de certificación, pone a disposición de los usuarios el certificado digital de la autoridad de certificación y su política asociada, almacena la clave privada de la autoridad de certificación, emite los certificados digitales, comprueba La validez de los certificados emitidos por la autoridad de certificación, documenta las infraestructuras de clave pública implantadas.*

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

Escala D

4	*Para revisar la seguridad del, "hardware" y el diseño de la red de área local, adapta la topología de la red según las necesidades de seguridad, segmenta la red de la organización de acuerdo con la política de seguridad, establece las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, establece los mecanismos de protección para las redes de acceso, implementa los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"), modifica el diseño de la red introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, configura los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal, revisa los procedimientos de salvaguarda de configuraciones.*
3	***Para revisar la seguridad del "hardware" y el diseño de la red de área local, adapta la topología de la red según las necesidades de seguridad, segmenta la red de la organización de acuerdo con la política de seguridad, establece las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, establece los mecanismos de protección para las redes de acceso, implementa los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"), modifica el diseño de la red introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, configura los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal, revisa los procedimientos de salvaguarda de configuraciones, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para revisar la seguridad del "hardware" y el diseño de la red de área local, adapta la topología de la red según las necesidades de seguridad, segmenta la red de la organización de acuerdo con la política de seguridad, establece las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, establece los mecanismos de protección para las redes de acceso, implementa los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"), modifica el diseño de la red introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, configura los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal, revisa los procedimientos de salvaguarda de configuraciones, pero comete amplias irregularidades que alteran el resultado final.*
1	*No revisa la seguridad del "hardware" y el diseño de la red de área local, adapta la topología de la red según las necesidades de seguridad, segmenta la red de la organización de acuerdo con la política de seguridad, establece las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, establece los mecanismos de protección para las redes de acceso, implementa los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention"), modifica el diseño de la red introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, configura los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal, revisa los procedimientos de salvaguarda de configuraciones.*

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

Escala E

4	

	Para revisar el, "software" de comunicaciones en red y el control de acceso de manera periódica, evalúa el "software" de comunicaciones que se ejecuta en los dispositivos de red, incluye en el diseño de la red los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies", revisa los procedimientos de salvaguarda del "software", revisa los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, aplica la configuración de seguridad en el ámbito de puntos críticos de red, elabora la documentación del "software" de seguridad.
3	***Para revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, evalúa el "software" de comunicaciones que se ejecuta en los dispositivos de red, incluye en el diseño de la red los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies", revisa los procedimientos de salvaguarda del "software", revisa los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, aplica la configuración de seguridad en el ámbito de puntos críticos de red, elabora la documentación del "software" de seguridad, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, evalúa el "software" de comunicaciones que se ejecuta en los dispositivos de red, incluye en el diseño de la red los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies", revisa los procedimientos de salvaguarda del "software", revisa los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, aplica la configuración de seguridad en el ámbito de puntos críticos de red, elabora la documentación del "software" de seguridad, pero comete amplias irregularidades que alteran el resultado final.*
1	*No revisa el "software" de comunicaciones en red y el control de acceso de manera periódica, evalúa el "software" de comunicaciones que se ejecuta en los dispositivos de red, incluye en el diseño de la red los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies", revisa los procedimientos de salvaguarda del "software", revisa los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, aplica la configuración de seguridad en el ámbito de puntos críticos de red, elabora la documentación del "software" 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.

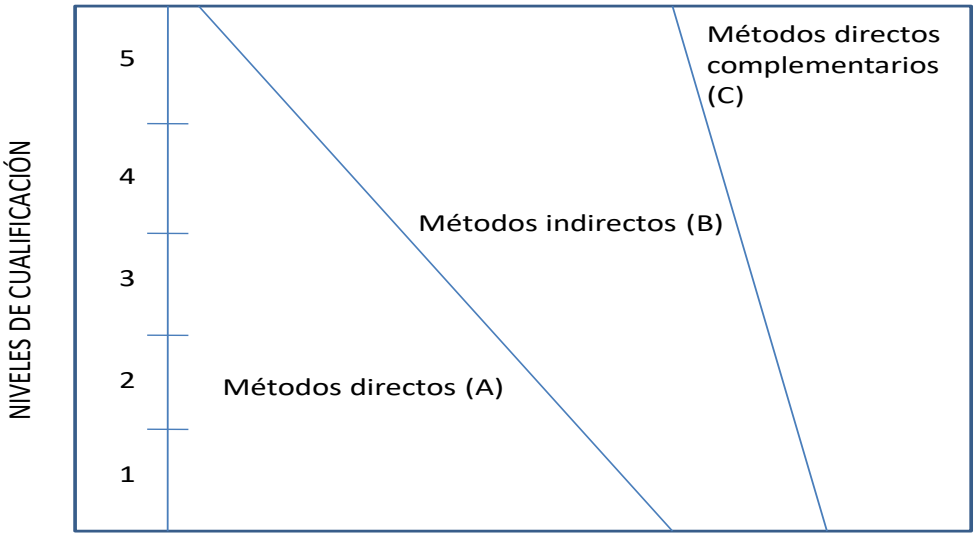
2.1. Métodos de evaluación y criterios generales de elección.

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 Implementar sistemas seguros de acceso y transmisión de datos, 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.