GUÍA DE EVIDENCIAS DE LA UNIDAD DE COMPETENCIA

"UC0959_2: Configurar la ciberseguridad en equipos finales"

CUALIFICACIÓN PROFESIONAL: OPERACIONES DE SEGURIDAD EN SISTEMAS INFORMÁTICOS

Código: IFC300_2 NIVEL: 2

1. ESPECIFICACIONES DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA.

Dado que la evaluación de la competencia profesional se basa en la recopilación de pruebas o evidencias de competencia generadas por cada persona candidata, el referente a considerar para la valoración de estas evidencias de competencia (siempre que éstas no se obtengan por observación del desempeño en el puesto de trabajo) es el indicado en los apartados 1.1 y 1.2 de esta GEC, referente que explicita la competencia recogida en las realizaciones profesionales y criterios de realización de la UC0959_2: Configurar la ciberseguridad en equipos finales.

1.1. Especificaciones de evaluación relacionadas con las dimensiones de la competencia profesional.

Las especificaciones recogidas en la GEC deben ser tenidas en cuenta por el asesor o asesora para el contraste y mejora del historial formativo de la persona candidata (especificaciones sobre el saber) e historial profesional (especificaciones sobre el saber hacer y saber estar).

Lo explicitado por la persona candidata durante el asesoramiento deberá ser contrastado por el evaluador o evaluadora, empleando para ello el referente de evaluación (UC y los criterios fijados en la correspondiente GEC) y el método que la Comisión de Evaluación determine. Estos métodos pueden ser, entre otros, la observación de la persona candidata en el puesto de trabajo, entrevistas profesionales, pruebas objetivas u otros. En el punto 2.1 de esta Guía se hace referencia a los mismos.

Este apartado comprende las especificaciones del “saber” y el “saber hacer”, que configuran las “competencias técnicas”, así como el “saber estar”, que comprende las “competencias sociales”.

a) Especificaciones relacionadas con el “saber hacer”.

La persona candidata demostrará el dominio práctico relacionado con las actividades profesionales que intervienen en configurar la ciberseguridad en equipos finales, y que se indican a continuación:

Nota: A un dígito se indican las actividades profesionales expresadas en las realizaciones profesionales de la unidad de competencia, y a dos dígitos las reflejadas en los criterios de realización.

1. Instalar sistemas de protección frente a "malware" en equipos finales ("end point"), configurando los parámetros de protección, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para

garantizar su seguridad, según normas y procedimientos de la entidad responsable.

1.1 La configuración del sistema operativo se verifica para el funcionamiento de la protección frente a "malware", validando los parámetros especificados según indique la documentación técnica.
1.2 Los programas de utilidad incluidos en el sistema operativo se configuran para el uso de la protección frente a "malware", previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.
1.3 La seguridad relativa al "software" no deseado se define en el sistema de protección frente a "malware", asignando parámetros tales como extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados digitalmente o con firma desconocida o caducada, junto con el veredicto de bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro para proteger al sistema frente a "malware" y "software" no deseado.
1.4 Los eventos de notificación y alarmas se configuran en el sistema de protección frente a "malware", estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog" u otros.
1.5 Los paquetes de instalación del "software" cliente para equipos y servidores se configuran en el sistema, definiendo parámetros tales como versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros.
1.6 Las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas se configuran en el sistema de protección frente a "malware", estableciendo las condiciones de actualización de todos los equipos.
1.7 Las opciones anti "tampering" para la protección contra la desactivación y desinstalación del "software" cliente de protección frente a "malware" se configuran, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.
1.8 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad, para comprobar la funcionalidad del sistema de seguridad.
1.9 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

2. Instalar sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response"), configurando los parámetros de protección, siguiendo especificaciones recibidas

de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

2.1 Los paquetes de instalación del "software" cliente de protección frente a amenazas avanzadas para equipos y servidores se configuran en el sistema, definiendo parámetros tales como versión de sistema operativo, datos específicos de suscripción a la plataforma de nube, y datos de conexión.
2.2 Las alertas avanzadas de detección de intrusión se definen en el sistema, estableciendo parámetros tales como tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores, entre otras, asignando la severidad de las alertas para la detección y notificando los eventos detectados por la plataforma.
2.3 Los eventos de notificación y alarmas se configuran en el sistema de protección frente a amenazas avanzadas, estableciendo parámetros tales como correos frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog", entre otros.
2.4 Las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas se configuran en el sistema, estableciéndolas en todos los equipos.
2.5 Las opciones anti "tampering" para la protección de desactivación y desinstalación del "software" cliente de protección se configuran, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.
2.6 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.
2.7 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

3. Instalar sistemas de cifrado de información en disco, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

3.1 La configuración del sistema operativo se verifica para el funcionamiento del cifrado, validando los parámetros especificados según indique la documentación técnica.
3.2 Los programas de utilidad incluidos en el sistema operativo, se configuran para el uso del cifrado, previa instalación en su caso y

verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.

3.3 El almacenamiento seguro de información se define, configurándolo mediante la asignación de parámetros tales como tamaño, permisos de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes.

3.4 La relación de políticas de cifrado de información se aplican en el sistema, estableciendo parámetros tales como unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave, certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor.

3.5 Las opciones anti "tampering" de protección de desactivación y desinstalación del "software" cliente de cifrado se configuran en el sistema, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto del cliente.

3.6 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

3.7 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

b) Especificaciones relacionadas con el “saber”.

La persona candidata, en su caso, deberá demostrar que posee los conocimientos técnicos (conceptos y procedimientos) que dan soporte a las actividades profesionales implicadas en las realizaciones profesionales de la **UC0959_2: Configurar la ciberseguridad en equipos finales**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Configuración de la seguridad en sistemas operativos

- Configuración del sistema operativo para el funcionamiento de protección frente a "malware", sistemas avanzados de detección y respuesta y sistemas de cifrado de información en disco. Parámetros.
- Configuración de programas de utilidad incluidos en el sistema operativo para el uso de una protección frente a "malware", sistemas avanzados de detección y respuesta y sistemas de cifrado de información en disco.

2. Sistemas de protección frente a "malware"

- Sistema de protección frente a "malware". Parámetros de configuración: extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados

digitalmente o con firma desconocida o caducada, entre otros. Acciones asociadas: bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro de protección, entre otros. Eventos de notificación y alarmas: correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante "syslog" u otros.

- Instalación del "software" cliente para equipos y servidores. Parámetros: versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros.
- Parámetros activos de detección de "malware": frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas. Condiciones de actualización de todos los equipos.
- Opciones anti "tampering" para la protección contra la desactivación y desinstalación del "software" cliente de protección frente a "malware" en un sistema. Parámetros: contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.

3. Sistemas avanzados de detección y respuesta (EDR: "Endpoint Detection and Response")

- Instalación de paquetes de "software" cliente de protección frente a amenazas avanzadas para equipos y servidores. Parámetros: versión de sistema operativo, datos específicos de suscripción a la plataforma de nube, y datos de conexión entre otros.
- Tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores. Configuración de alertas avanzadas de detección de intrusión.
- Parámetros activos de detección de amenazas avanzadas: frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas.
- Opciones anti "tampering" para la protección de desactivación y desinstalación del "software" cliente de protección frente a amenazas avanzadas. Parámetros: contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección.
- Sistemas XDR ("Extended Detection and Response").

4. Sistemas de cifrado de información en disco

- Almacenamiento seguro de información. Configuración de sistemas de cifrado. Parámetros: tamaño, permisos de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes, entre otros.
- Definición de políticas de cifrado. Establecimiento de unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave, certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor.
- Opciones anti "tampering" de protección de desactivación y desinstalación del "software" cliente de cifrado. Parámetros: contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto de los clientes.

c) Especificaciones relacionadas con el "saber estar".

La persona candidata debe demostrar la posesión de actitudes de comportamiento en el trabajo y formas de actuar e interactuar, según las siguientes especificaciones:

- Aplicar las instrucciones de trabajo de manera organizada, precisa y meticulosa.
- Comprender y valorar las motivaciones y consecuencias del trabajo bien realizado.
- Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
- Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.
- Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

1.2. Situaciones profesionales de evaluación y criterios de evaluación.

La situación profesional de evaluación define el contexto profesional en el que se tiene que desarrollar la misma. Esta situación permite al evaluador o evaluadora obtener evidencias de competencia de la persona candidata que incluyen, básicamente, todo el contexto profesional de la Unidad de Competencia implicada.

Así mismo, la situación profesional de evaluación se sustenta en actividades profesionales que permiten inferir competencia profesional respecto a la práctica totalidad de realizaciones profesionales de la Unidad de Competencia.

Por último, indicar que la situación profesional de evaluación define un contexto abierto y flexible, que puede ser completado por las CC.AA., cuando éstas decidan aplicar una prueba profesional a las personas candidatas.

En el caso de la "UC0959_2: Configurar la ciberseguridad en equipos finales", 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 configurar la ciberseguridad en

equipos finales, 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. Instalar sistemas de protección frente a 'malware' en equipos finales ('end point').

2. Instalar sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response').

3. Instalar sistemas de cifrado de información en disco.

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***
Exactitud en la instalación de sistemas de protección frente a 'malware' en equipos finales ('end point').	- Verificación de la configuración del sistema operativo para el funcionamiento de la protección frente a 'malware'. - Configuración de los programas de utilidad incluidos en el sistema operativo para el uso de la protección frente a 'malware'.

	- Definición de la seguridad relativa al 'software' no deseado en el sistema de protección frente a 'malware'. - Configuración de los eventos de notificación y alarmas en el sistema de protección frente a 'malware', de los paquetes de instalación del 'software' cliente para equipos y servidores y de las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas estableciendo parámetros.. - Configuración de las opciones anti 'tampering' para la protección contra la desactivación y desinstalación del 'software' cliente de protección frente a 'malware', estableciendo parámetros de seguridad. - Verificación de la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización. *El umbral de desempeño competente está explicitado en la Escala A.*
Exactitud en la instalación de sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response').	- Configuración de los paquetes de instalación del software cliente de protección frente a amenazas avanzadas para equipos y servidores en el sistema. - Definición de las alertas avanzadas de detección de intrusión en el sistema. - Configuración de los eventos de notificación y alarmas en el sistema de protección frente a amenazas avanzadas. - Configuración de las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema. - Configuración de las opciones anti 'tampering' para la protección de desactivación y desinstalación del 'software' cliente de protección, estableciendo parámetros de seguridad. - Verificación de la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización. *El umbral de desempeño competente está explicitado en la Escala B.*

Precisión en la instalación de sistemas de cifrado de información en disco.	- Verificación de la configuración del sistema operativo para el funcionamiento del cifrado. - Configuración de los programas de utilidad incluidos en el sistema operativo, para el uso del cifrado. - Definición del almacenamiento seguro de información, configurándolo mediante la asignación de parámetros. - Aplicación de la relación de políticas de cifrado de información en el sistema, estableciendo parámetros según cada tipo de equipo y servidor. - Configuración de las opciones anti 'tampering' de protección de desactivación y desinstalación del 'software' cliente de cifrado en el sistema. - Verificación de la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior. *El umbral de desempeño competente está explicitado en la Escala C.*
Cumplimiento del tiempo asignado, considerando el que emplearía un o una profesional competente.	
El desempeño competente requiere el cumplimiento, en todos los criterios de mérito, de la normativa aplicable en materia de prevención de riesgos laborales, protección medioambiental	

Escala A

4	*Para instalar sistemas de protección frente a 'malware' en equipos finales ('end point'), verifica la configuración del sistema operativo para el funcionamiento de la protección frente a 'malware'. Configura los programas de utilidad incluidos en el sistema operativo para el uso de la protección frente a 'malware'. Define la seguridad relativa al 'software' no deseado en el sistema de protección frente a 'malware'. Configura los eventos de notificación y alarmas en el sistema de protección frente a 'malware', de los paquetes de instalación del 'software' cliente para equipos y servidores y de las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas estableciendo parámetros.. Configura las opciones anti 'tampering' para la protección contra la desactivación y desinstalación del 'software' cliente de protección frente a 'malware', estableciendo parámetros de seguridad. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales*

y pruebas de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización.

3

Para instalar sistemas de protección frente a 'malware' en equipos finales ('end point'), verifica la configuración del sistema operativo para el funcionamiento de la protección frente a 'malware'. Configura los programas de utilidad incluidos en el sistema operativo para el uso de la protección frente a 'malware'. Define la seguridad relativa al 'software' no deseado en el sistema de protección frente a 'malware'. Configura los eventos de notificación y alarmas en el sistema de protección frente a 'malware', de los paquetes de instalación del 'software' cliente para equipos y servidores y de las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas estableciendo parámetros.. Configura las opciones anti 'tampering' para la protección contra la desactivación y desinstalación del 'software' cliente de protección frente a 'malware', estableciendo parámetros de seguridad. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, pero comete pequeñas irregularidades que no alteran el resultado final.

2

Para instalar sistemas de protección frente a 'malware' en equipos finales ('end point'), verifica la configuración del sistema operativo para el funcionamiento de la protección frente a 'malware'. Configura los programas de utilidad incluidos en el sistema operativo para el uso de la protección frente a 'malware'. Define la seguridad relativa al 'software' no deseado en el sistema de protección frente a 'malware'. Configura los eventos de notificación y alarmas en el sistema de protección frente a 'malware', de los paquetes de instalación del 'software' cliente para equipos y servidores y de las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas estableciendo parámetros.. Configura las opciones anti 'tampering' para la protección contra la desactivación y desinstalación del 'software' cliente de protección frente a 'malware', estableciendo parámetros de seguridad. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, pero comete grandes irregularidades que alteran el resultado final.

1

No instala sistemas de protección frente a 'malware' en equipos finales ('end point').

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

Escala B

4

Para instalar sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response'), configura los paquetes de instalación del software cliente de protección frente a amenazas avanzadas para equipos y servidores en el sistema. Define las alertas avanzadas de detección de intrusión en el sistema. Configura los eventos de notificación y alarmas en el sistema de protección frente a amenazas avanzadas. Configura las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema. Configura las opciones anti 'tampering' para la

	protección de desactivación y desinstalación del 'software' cliente de protección, estableciendo parámetros de seguridad. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización.
3	***Para instalar sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response'), configura los paquetes de instalación del software cliente de protección frente a amenazas avanzadas para equipos y servidores en el sistema. Define las alertas avanzadas de detección de intrusión en el sistema. Configura los eventos de notificación y alarmas en el sistema de protección frente a amenazas avanzadas. Configura las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema. Configura las opciones anti 'tampering' para la protección de desactivación y desinstalación del 'software' cliente de protección, estableciendo parámetros de seguridad. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, pero comete pequeñas irregularidades que no alteran el resultado final.***
2	*Para instalar sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response'), configura los paquetes de instalación del software cliente de protección frente a amenazas avanzadas para equipos y servidores en el sistema. Define las alertas avanzadas de detección de intrusión en el sistema. Configura los eventos de notificación y alarmas en el sistema de protección frente a amenazas avanzadas. Configura las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema. Configura las opciones anti 'tampering' para la protección de desactivación y desinstalación del 'software' cliente de protección, estableciendo parámetros de seguridad. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, pero comete grandes irregularidades que alteran el resultado final.*
1	*No instala sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response').*

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

Escala C

4	*Para instalar sistemas de cifrado de información en disco, verifica la configuración del sistema operativo para el funcionamiento del cifrado. Configura los programas de utilidad incluidos en el sistema operativo, para el uso del cifrado. Define el almacenamiento seguro de información, configurándolo mediante la asignación de parámetros. Aplica la relación de políticas de cifrado de información en el sistema, estableciendo parámetros según cada tipo de equipo y servidor. Configura las opciones anti 'tampering' de protección de desactivación y desinstalación del 'software' cliente de cifrado en el sistema. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los*

	modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.
3	***Para instalar sistemas de cifrado de información en disco, verifica la configuración del sistema operativo para el funcionamiento del cifrado. Configura los programas de utilidad incluidos en el sistema operativo, para el uso del cifrado. Define el almacenamiento seguro de información, configurándolo mediante la asignación de parámetros. Aplica la relación de políticas de cifrado de información en el sistema, estableciendo parámetros según cada tipo de equipo y servidor. Configura las opciones anti 'tampering' de protección de desactivación y desinstalación del 'software' cliente de cifrado en el sistema. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior, pero comete pequeñas irregularidades que no alteran el resultado final.***
2	*Para instalar sistemas de cifrado de información en disco, verifica la configuración del sistema operativo para el funcionamiento del cifrado. Configura los programas de utilidad incluidos en el sistema operativo, para el uso del cifrado. Define el almacenamiento seguro de información, configurándolo mediante la asignación de parámetros. Aplica la relación de políticas de cifrado de información en el sistema, estableciendo parámetros según cada tipo de equipo y servidor. Configura las opciones anti 'tampering' de protección de desactivación y desinstalación del 'software' cliente de cifrado en el sistema. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior, pero comete grandes irregularidades que alteran el resultado final.*
1	*No instala sistemas de cifrado de información en disco.*

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

2. MÉTODOS DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA Y ORIENTACIONES PARA LAS COMISIONES DE EVALUACIÓN Y EVALUADORES/AS.

La selección de métodos de evaluación que deben realizar las Comisiones de Evaluación será específica para cada persona candidata, y dependerá fundamentalmente de tres factores: nivel de cualificación de la unidad de competencia, características personales de la persona candidata y evidencias de competencia indirectas aportadas por la misma.

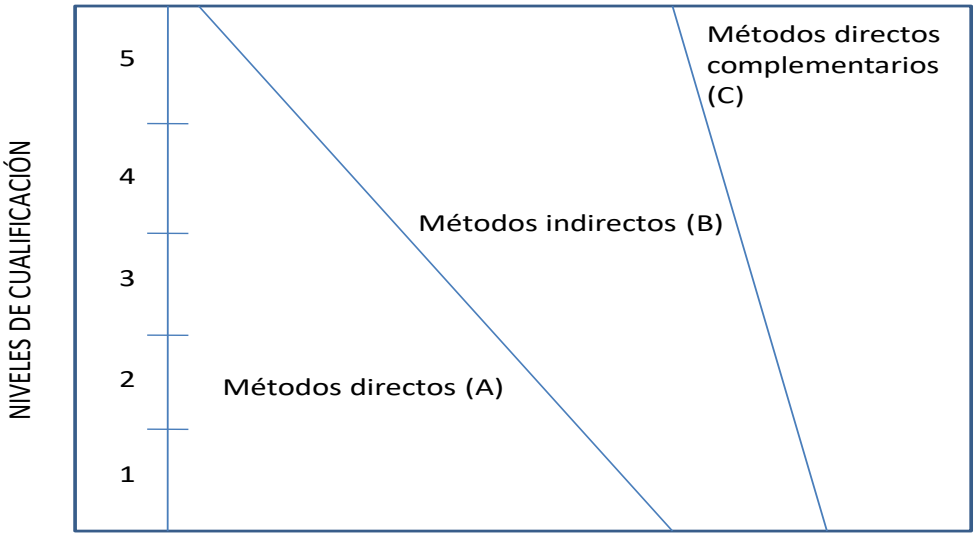
2.1. Métodos de evaluación y criterios generales de elección.

Los métodos que pueden ser empleados en la evaluación de la competencia profesional adquirida por las personas a través de la experiencia laboral, y vías no formales de formación son los que a continuación se relacionan:

a) **Métodos indirectos**: Consisten en la valoración del historial profesional y formativo de la persona candidata; así como en la valoración de muestras sobre productos de su trabajo o de proyectos realizados. Proporcionan evidencias de competencia inferidas de actividades realizadas en el pasado.

b) **Métodos directos**: Proporcionan evidencias de competencia en el mismo momento de realizar la evaluación. Los métodos directos susceptibles de ser utilizados son los siguientes:

- Observación en el puesto de trabajo (A).
- Observación de una situación de trabajo simulada (A).
- Pruebas de competencia profesional basadas en las situaciones profesionales de evaluación (C).
- Pruebas de habilidades (C).
- Ejecución de un proyecto (C).
- Entrevista profesional estructurada (C).
- Preguntas orales (C).
- Pruebas objetivas (C).



Fuente: Leonard Mertens (elaboración propia)

Como puede observarse en la figura anterior, en un proceso de evaluación que debe ser integrado ("holístico"), uno de los criterios de elección depende del nivel de cualificación de la UC. Como puede observarse, a menor nivel, deben priorizarse los métodos de observación en una situación de trabajo real o simulada, mientras que, a niveles superiores, debe priorizarse la utilización de métodos indirectos acompañados de entrevista profesional estructurada.

La consideración de las características personales de la persona candidata, debe basarse en el principio de equidad. Así, por este principio, debe priorizarse la selección de aquellos métodos de carácter complementario que faciliten la generación de evidencias válidas. En este orden de ideas, nunca debe aplicarse una prueba de conocimientos de carácter escrito a 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 Configurar la ciberseguridad en equipos

finales, se le someterá, al menos, a una prueba profesional de evaluación y a una entrevista profesional estructurada sobre la dimensión relacionada con el "saber" y "saber estar" de la competencia profesional.

b) En la fase de evaluación siempre se deben contrastar las evidencias indirectas de competencia presentadas por la persona candidata. Deberá tomarse como referente la UC, el contexto que incluye la situación profesional de evaluación, y las especificaciones de los “saberes” incluidos en las dimensiones de la competencia. Se recomienda utilizar una entrevista profesional estructurada.

c) Si se evalúa a la persona candidata a través de la observación en el puesto de trabajo, se recomienda tomar como referente los logros expresados en las realizaciones profesionales considerando el contexto expresado en la situación profesional de evaluación.

d) Si se aplica una prueba práctica, se recomienda establecer un tiempo para su realización, considerando el que emplearía un 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) Esta Unidad de Competencia es de nivel "2" y sus competencias conjugan básicamente destrezas cognitivas y actitudinales. Por las características de estas competencias, la persona candidata ha de movilizar fundamentalmente sus destrezas cognitivas aplicándolas de forma competente a múltiples situaciones y contextos profesionales. Por esta razón, se recomienda que la comprobación de lo explicitado por la persona candidata se complemente con una prueba de desarrollo práctico, que tome como referente las actividades de la situación profesional de evaluación, todo ello con independencia del método de evaluación utilizado. Esta prueba se planteará sobre un contexto definido que permita evidenciar las citadas competencias, minimizando los recursos y el tiempo necesario para su realización, e implique el cumplimiento de las normas de seguridad, prevención de riesgos laborales y medioambientales requeridas.

g) Si se utiliza la entrevista profesional para comprobar lo explicitado por la persona candidata se tendrán en cuenta las siguientes recomendaciones:

Se estructurará la entrevista a partir del análisis previo de toda la documentación presentada por la persona candidata, así como de la información obtenida en la fase de asesoramiento y/o en otras fases de la evaluación.

La entrevista se concretará en una lista de cuestiones claras, que generen respuestas concretas, sobre aspectos que han de ser explorados a lo largo de la misma, teniendo en cuenta el referente de evaluación y el perfil de la persona candidata. Se debe evitar la improvisación.

El evaluador o evaluadora debe formular solamente una pregunta a la vez dando el tiempo suficiente de respuesta, poniendo la máxima atención y neutralidad en el contenido de las mismas, sin enjuiciarlas en ningún momento. Se deben evitar las interrupciones y dejar que la persona candidata se comunique con confianza, respetando su propio ritmo y solventando sus posibles dificultades de expresión.

Para el desarrollo de la entrevista se recomienda disponer de un lugar que respete la privacidad. Se recomienda que la entrevista sea grabada mediante un sistema de audio vídeo previa autorización de la persona implicada, cumpliéndose la ley de protección de datos.