MINISTERIO
DE EDUCACIÓN, CULTURA
Y DEPORTE

FONDO SOCIAL EUROPEO
El FSE invierte en tu futuro

SECRETARÍA DE ESTADO DE
EDUCACIÓN, FORMACIÓN
PROFESIONAL Y UNIVERSIDADES

DIRECCIÓN GENERAL
DE FORMACIÓN PROFESIONAL

INSTITUTO NACIONAL
DE LAS CUALIFICACIONES

# PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

## CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

**Código**: **IFC153_3** **NIVEL**: **3**

## GUÍAS DE EVIDENCIA DE LA COMPETENCIA PROFESIONAL

## (DOCUMENTO RESERVADO PARA USO EXCLUSIVO DE PERSONAL ASESOR Y EVALUADOR)

# ÍNDICE GENERAL ABREVIADO

## 1. PRESENTACIÓN DE LA GUÍA

Las Guías de Evidencia de las Unidades de Competencia, en su calidad de instrumentos de apoyo a la evaluación, se han elaborado con una estructura sencilla y un contenido adecuado a las finalidades a que deben contribuir, como son las de optimizar el procedimiento de evaluación, y coadyuvar al logro de los niveles requeridos en cuanto a validez, fiabilidad y homogeneidad, tanto en el desarrollo de los procesos como en los resultados mismos de la evaluación.

Para ello, la elaboración de las Guías parte del referente de evaluación constituido por la Unidad de Competencia considerada (en adelante UC), si bien explicitando de otra manera sus elementos estructurales, en el convencimiento de que así se facilita la labor específica del personal asesor y evaluador. Hay que advertir que, en todo caso, se parte de un análisis previo y contextualización de la UC para llegar, mediante la aplicación de la correspondiente metodología, a la concreción de los citados elementos estructurales.

En la línea señalada, se han desglosado las competencias profesionales de la UC en competencias técnicas y sociales.

Las competencias técnicas aparecen desglosadas en el **saber hacer** y en el **saber**; y las sociales en el **saber estar**. Este conjunto de "saberes" constituyen las tres dimensiones más simples y clásicas de la competencia profesional.

La dimensión relacionada con el **saber hacer** aparece explicitada en forma de actividades profesionales que subyacen en las realizaciones profesionales (RPs) y criterios de realización (CRs).

Conviene destacar que la expresión formal de las actividades profesionales se ha realizado mediante un lenguaje similar al empleado por las y los trabajadores y el empresariado, de aquí su ventaja a la hora de desarrollar autoevaluaciones, o solicitar información complementaria a las empresas.

La dimensión de la competencia relacionada con el saber, comprende el conjunto de conocimientos de carácter técnico sobre conceptos y procedimientos, se ha extraído del módulo formativo correspondiente a cada UC, si bien se ha reorganizado para su mejor utilidad, asociando a cada una de las actividades profesionales principales aquellos saberes que las soportan y, en su caso, creando un bloque transversal a todas ellas.

En cuanto a la dimensión de la competencia relacionada con el saber estar, se han extraído, caso de existir, de las correspondientes RPs y CRs de la UC, en forma de capacidades de tipo actitudinal.

Por último indicar que, del análisis previo de la UC y de su contexto profesional, se ha determinado el **contexto crítico** para la evaluación, cuya propiedad fundamental radica en que, vertido en las situaciones profesionales de evaluación, permite obtener resultados en la evaluación razonablemente transferibles a todas las situaciones profesionales que se pueden dar en el contexto profesional de la UC. Precisamente por esta importante propiedad, el contexto que subyace en las situaciones profesionales de evaluación se ha considerado también en la fase de asesoramiento, lográndose así una economía de recursos humanos, materiales y económicos en la evaluación de cada candidatura.

## 2. CRITERIOS GENERALES PARA LA UTILIZACIÓN DE LAS GUÍAS DE EVIDENCIA

La estructura y contenido de esta "Guía de Evidencia de Competencia Profesional" (en adelante GEC) se basa en los siguientes criterios generales que deben tener en cuenta las Comisiones de Evaluación, el personal evaluador y el asesor.

**Primero.-** Si las Comisiones de Evaluación deciden la aplicación de un método de evaluación mediante observación en el puesto de trabajo, el referente de evaluación que se utilice para valorar las evidencias de competencia generadas por las candidatas y candidatos, serán las realizaciones profesionales y criterios de realización de la UC de que se trate, en el contexto profesional que establece el apartado 1.2. de la correspondiente GEC.

**Segundo.-** Si la Comisión de Evaluación apreciara la imposibilidad de aplicar la observación en el puesto de trabajo, esta GEC establece un marco flexible de evaluación –**las situaciones profesionales de evaluación**- para que ésta pueda realizarse en una situación de trabajo simulada, si así se decide por la citada Comisión. En este caso, para valorar las evidencias de competencia profesional generadas por las candidatas y candidatos, se utilizarán los **criterios de evaluación** del apartado 1.2. de la correspondiente GEC, formados por "criterios de mérito"; "indicadores"; "escalas de desempeño competente" y ponderaciones que subyacen en las mismas. Conviene señalar que los citados criterios de evaluación se extraen del análisis de las RPs y CRs de la UC de que se trate. Hay que destacar que la utilización de situaciones profesionales de evaluación (de las que las Comisiones de Evaluación podrán derivar **pruebas profesionales**), con sus criterios de evaluación asociados, incrementan la validez y fiabilidad en la inferencia de competencia profesional.

**Tercero.-** Sin perjuicio de lo anterior, la GEC contiene también otros referentes –**las especificaciones de evaluación relacionadas con las dimensiones de la competencia**- que permiten valorar las evidencias indirectas que aporten las candidatas y candidatos mediante su historial profesional y formativo, entre otros, así como para orientar la aplicación de otros métodos de obtención de nuevas evidencias, mediante entrevista profesional estructurada, pruebas de conocimientos, entre otras.

A modo de conclusión, puede decirse que la aplicación de los tres criterios generales anteriormente descritos, persigue la finalidad de contribuir al rigor técnico, validez, fiabilidad y homogeneidad en los resultados de la evaluación y, en definitiva, a su calidad, lo cual redundará en la mejor consideración social de las acreditaciones oficiales que se otorguen y, por tanto, en beneficio de las trabajadoras y trabajadores cuyas competencias profesionales se vean acreditadas.

# GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

**“UC0486_3: Asegurar equipos informáticos”**

***Transversal en las siguientes cualificaciones:***

IFC152_3 Gestión de sistemas informáticos.
IFC153_3 Seguridad informática.

# CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

**Código: IFC153_3** **NIVEL: 3**

# 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 UC0486_3: Asegurar equipos informáticos.

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

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

Lo explicitado por la persona candidata durante el asesoramiento deberá ser contrastado por el evaluador o evaluadora, empleando para ello el referente de evaluación (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 principales y secundarias que intervienen en el aseguramiento de equipos informáticos, y que se indican a continuación:

Nota: A un dígito se indican las actividades principales y a dos las actividades secundarias relacionadas.

***1. Asignar políticas de seguridad en el acceso de los usuarios siguiendo las necesidades de uso y condiciones de seguridad.***

1.1 Verificar la existencia de procedimientos de instalación y actualización de equipos, de copias de respaldo, de detección de errores, de restricción de

equipos y de protección contra virus y elementos no deseados a partir del plan de implantación del sistema informático de la organización.

1.2 Establecer los permisos de acceso a los recursos del sistema según el plan de seguridad y la normativa de implantación.

1.3 Verificar la integridad de la conexión y la confidencialidad en el acceso a servidores siguiendo las normas de seguridad.

1.4 Comprobar la inclusión de usos y restricciones de equipos y usuarios, los servicios de red permitidos y restringidos y el ámbito de responsabilidades en la utilización de los equipos informáticos en las políticas de usuario según las especificaciones.

1.5 Transmitir la política de seguridad a los usuarios asegurando su correcta interpretación.

1.6 Documentar las tareas realizadas aplicando los procedimientos de la organización.

1.7 Comprobar el cumplimiento de la legislación de protección de datos en la información afectada por ella siguiendo el plan de seguridad.

- Desarrollar las actividades cumpliendo el plan de seguridad del sistema informático y aplicando los procedimientos de la organización.

***2. Preparar servidores protegiéndolos frente a accesos no deseados y siguiendo las necesidades de uso y las directivas de la organización.***

2.1 Ubicar el servidor en la red en una zona protegida y aislada cumpliendo el plan de seguridad y la normativa de implantación del sistema.

2.2 Configurar los servicios que ofrece el servidor según el plan de seguridad y la normativa de implantación del sistema.

2.3 Configurar los accesos y permisos a los recursos del servidor según el propósito del mismo y cumpliendo la política de seguridad de la organización.

2.4 Activar los mecanismos de registro de actividad e incidencias del sistema y sus procedimientos de análisis permitiendo analizar dicha información.

2.5 Determinar una solución de compromiso entre funcionalidades y riesgos para los módulos adicionales del servidor a partir del análisis del mismo.

2.6 Configurar los mecanismos de autenticación según la normativa de seguridad.

2.7 Crear los roles y privilegios de los usuarios según la normativa de seguridad.

***3. Implantar cortafuegos en equipos y servidores teniendo en cuenta las necesidades de uso y las directivas de la organización.***

3.1 Seleccionar la topología del cortafuegos para el entorno de implantación en base a las necesidades planteadas.

3.2 Elegir los elementos hardware y software del cortafuegos según factores económicos y de rendimiento.

3.3 Efectuar la puesta en marcha de los cortafuegos según el nivel exigido por la política de seguridad.

3.4 Configurar las reglas de filtrado y los niveles de registro y alarmas cumpliendo la normativa de seguridad.

3.5 Verificar los cortafuegos asegurando el cumplimiento de lo especificado en la normativa de seguridad.

3.6 Documentar la instalación, actualización y procedimientos de actuación del cortafuegos según las especificaciones de la organización.

3.7 Configurar los sistemas de registro de forma que permitan su análisis en busca de problemas de seguridad.

## 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 UC0486_3 Asegurar equipos informáticos**.** Estos conocimientos se presentan agrupados a partir de las actividades profesionales principales que aparecen en cursiva y negrita:

### *1. Asignación de políticas de seguridad en el acceso de los usuarios.*

- Administración de equipos y redes:
  - Manejo de herramientas de configuración, administración y monitorización de equipos y redes.
  - Autenticación: Protocolos de autenticación, Tarjetas inteligentes, Identificación digital, Nombres de usuario, Política de contraseñas, Grupos y Directivas de grupo.
  - Control de acceso.
  - Administradores de autorización y seguridad.
  - Directivas de restricción de software.
  - Auditado de sucesos de seguridad.
  - Sistema de cifrado de archivos.
  - Infraestructura de claves públicas.
  - Seguridad del protocolo Internet (IPSec).
  - Listas de control de acceso.

### *2. Configuración de servidores.*

- Administración de servidores:
  - Manejo de herramientas de configuración, administración y monitorización de servidores.
  - Autenticación: Protocolos de autenticación, Tarjetas inteligentes, Identificación digital, Nombres de usuario, Política de contraseñas, Grupos y Directivas de grupo.
  - Control de acceso.
  - Administradores de autorización y seguridad.
  - Directivas de restricción de software.
  - Auditado de sucesos de seguridad.
  - Sistema de cifrado de archivos.
  - Infraestructura de claves públicas.
  - Seguridad del protocolo Internet (IPSec).
  - Listas de control de acceso.
- Medidas de seguridad pasiva:
  - Ubicación y protección física de los equipos y servidores.
  - Sistemas de alimentación ininterrumpida.

### *3. Implantación de cortafuegos en equipos y servidores.*

- Cortafuegos Software o Hardware:
  - Tipos:
    - Circuito a nivel de pasarela.
    - Nivel de aplicación de pasarela.
    - De filtrado de paquetes o de capa de red.
    - De capa de aplicación.
    - Personal.
  - Políticas: Restrictiva o permisiva.
  - Manejo de herramientas de instalación, configuración y mantenimiento.
- Administración de Sistemas.
- Fraudes informáticos y robos de información.

***Saberes comunes que dan soporte a las actividades profesionales de esta unidad de competencia***

- Legislación y normativa vigente aplicable sobre seguridad relativas a la protección de datos y al procesamiento y uso de los mismos con medios electrónicos.
- Administración de Redes:
  - Protocolos de Red (TCP/IP, UDP, Ethernet y otros).
  - Servicios y características (DNS, DHCP y otros).
  - Instalación y configuración de redes: Subredes, Pasarelas, Tablas de encaminamiento, Métrica y otros
  - Niveles OSI.
  - Redes privadas Virtuales.
  - SSL/TTL.
  - NIDS.
  - Auditoría de red.
  - DMZ.

## 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:

1. En relación con otros trabajadores o profesionales deberá:

   1.1 Tratarlos con cortesía, respeto y discreción.
   1.2 Liderar y coordinar equipos de trabajo.
   1.3 Habilidades en la resolución de conflictos.
   1.4 Transmitir indicaciones claras e inequívocas al personal bajo su responsabilidad.
   1.5 Comunicarse eficazmente con las personas del equipo adecuadas en cada momento, respetando los canales establecidos en la organización.
   1.6 Participar y colaborar activamente en el equipo de trabajo.
   1.7 Proponer alternativas con el objetivo de mejorar resultados.

2. En relación con clientes / usuarios deberá:

   2.1 Tratar al cliente con cortesía, respeto y discreción.

2.2 Cumplir las normas de comportamiento profesional.
2.3 Demostrar un buen hacer profesional.
2.4 Capacidad de adaptación al contexto y las necesidades de los usuarios.
2.5 Finalizar el trabajo en los plazos establecidos.
2.6 Capacidad de comunicación con los clientes.

3. En relación a la obra, puesto de trabajo y otros aspectos deberá:

3.1 Cuidar el aspecto y aseo personal como profesional.
3.2 Responsabilizarse del trabajo que desarrolla, cumpliendo los objetivos y plazos establecidos.
3.3 Adaptarse a la organización integrándose al sistema de relaciones técnico profesionales.
3.4 Tener iniciativa para promover proyectos.
3.5 Capacidad de iniciativa para encontrar información y relacionarse con proveedores.
3.6 Tener una actitud consecuente con el mundo tecnológico. Limpieza, reciclaje de residuos, ahorro y eficiencia energética.
3.7 Cuidar los equipos de trabajo y utilizar con economía los materiales.
3.8 Respetar las instrucciones y normas internas de la empresa.
3.9 Preocuparse por cumplir siempre las medidas de seguridad en las actividades laborales.

## 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 UC0486_3: Asegurar equipos informáticos, se tiene una situación profesional de evaluación y se concreta en los siguientes términos:

### 1.2.1. Situación profesional de evaluación.

#### a) Descripción de la situación profesional de evaluación.

En esta situación profesional, la persona candidata demostrará la competencia requerida para asegurar equipos informáticos, sobre un sistema informático existente compuesto por varios equipos, operando bajo sistemas operativos estándar y comunicados entre sí mediante una red de datos. Esta situación comprenderá al menos las siguientes actividades:

1. Aplicar las políticas de seguridad para el acceso de los usuarios.

2. Configurar un servidor VPN de acceso remoto.

3. Configurar una DMZ instalando un cortafuegos.

***Condiciones adicionales:***

- Se dispondrá de los equipos, paquetes software, herramientas informáticas y documentación requeridos por la situación profesional de evaluación.

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

- Se planteará alguna contingencia o situación imprevista que sea relevante para la demostración de la competencia relacionada con la respuesta a contingencias.

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

Con el objeto de optimizar la validez y fiabilidad del resultado de la evaluación, esta Guía incluye unos criterios de evaluación integrados y, por tanto, reducidos en número. 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 se especifican en el cuadro siguiente:

| *Criterios de mérito* | *Indicadores, escalas y umbrales de desempeño competente* |
|---|---|
| *Aplicación de las políticas de seguridad.* | - Verificación de la existencia de los procedimientos de instalación, actualización y copia de respaldo de la información.<br>- Comprobación de que los sistemas de protección contra virus y malware y de los sistemas de registro garantizan la seguridad de los sistemas informáticos.<br>- Establecimiento de permisos de acceso a recursos de acuerdo con el plan de seguridad.<br>- Comprobación de la integridad de las conexiones y del acceso confidencial según el plan de seguridad.<br>- Configuración de restricciones en equipos y usuarios siguiendo las especificaciones dadas.<br>- Verificación de los documentos de seguridad y el acceso a la información según la normativa de protección de datos.<br>- Documentación de los procedimientos llevados a cabo siguiendo las indicaciones dadas.<br><br>*El umbral de desempeño competente, requiere el cumplimiento total del criterio de mérito.* |
| *Configuración del servidor VPN de acceso remoto.* | - Determinación de la interfaz de red a conectar a la VPN, tipo de autenticación y forma de asignar direcciones IP.<br>- Configuración de enrutamiento y acceso remoto.<br>- Configuración de filtros.<br>- Configuración de servicios y puertos.<br>- Implantación de sistemas de seguridad en el acceso y las conexiones a la VPN.<br>- Ajuste de los niveles de registro.<br><br>*El umbral de desempeño competente está explicitado en la escala A.* |
| *Configuración de la DMZ.* | - Selección del firewall.<br>- Configuración IP de los routers, hosts y servidores.<br>- Inicialización del firewall.<br>- Configuración de las interfaces del firewall.<br>- Configuración de NAT en el firewall.<br>- Documentación del esquema de la DMZ configurada.<br><br>*El umbral de desempeño competente está explicitado en la escala B.* |

**Escala A**

| | |
|---|---|
| 5 | *El servidor VPN de acceso remoto se configura exactamente de acuerdo a las especificaciones facilitadas. Se determina la interfaz de red a conectar a la VPN así como el tipo de autenticación y la forma de asignar direcciones IP más conveniente para el cumplimiento de los requisitos marcados. Se configura el enrutamiento y el acceso remoto así como los filtros de paquetes y los servicios y puertos necesarios para cumplir con las especificaciones. Se implantan sistemas de seguridad en el acceso y las conexiones a la VPN garantizando el máximo nivel de protección. Se ajustan los niveles de registro para almacenar todos los datos que puedan proporcionar información útil.* |
| 4 | *El servidor VPN de acceso remoto se configura en base a las especificaciones facilitadas. Se determina la interfaz de red a conectar a la VPN así como el tipo de autenticación y la forma de asignar direcciones IP más conveniente para el cumplimiento de los requisitos marcados. Se configura el enrutamiento y el acceso remoto así como los filtros de paquetes y los servicios y puertos necesarios para cumplir con las especificaciones. Se implantan sistemas de seguridad en el acceso y las conexiones a la VPN garantizando un nivel de protección acorde a los niveles de seguridad requeridos. Se ajustan los niveles de registro para almacenar los datos requeridos.* |
| 3 | *El servidor VPN de acceso remoto se configura en base a las especificaciones facilitadas. Se determina la interfaz de red a conectar a la VPN así como un tipo de autenticación y una forma de asignar direcciones IP a utilizar. Se configura el enrutamiento y el acceso remoto así como los filtros de paquetes y los servicios y puertos necesarios para cumplir con las especificaciones. Se implantan sistemas de seguridad en el acceso y las conexiones a la VPN garantizando un nivel de protección acorde a los niveles de seguridad requeridos. Se ajustan los niveles de registro para almacenar los datos requeridos.* |
| 2 | *El servidor VPN de acceso remoto no se configura en base a las especificaciones facilitadas. Se determina la interfaz de red a conectar a la VPN así como un tipo de autenticación y una forma de asignar direcciones IP a utilizar. Se configura el enrutamiento y el acceso remoto así como los filtros de paquetes y los servicios y puertos necesarios para cumplir con las especificaciones. No se implantan sistemas de seguridad en el acceso y las conexiones a la VPN que garanticen un nivel de protección acorde a los niveles de seguridad requeridos. Se ajustan los niveles de registro para almacenar los datos requeridos.* |
| 1 | *El servidor VPN de acceso remoto no se configura en base a las especificaciones facilitadas. Se determina la interfaz de red a conectar a la VPN así como un tipo de autenticación y una forma de asignar direcciones IP a utilizar. No se configura el enrutamiento y el acceso remoto así como los filtros de paquetes y los servicios y puertos necesarios para cumplir con las especificaciones. No se implantan sistemas de seguridad en el acceso y las conexiones a la VPN que garanticen un nivel de protección acorde a los niveles de seguridad requeridos. No se ajustan correctamente los niveles de registro.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala B**

| | |
|---|---|
| 5 | *La DMZ se configura siguiendo las especificaciones dadas y garantizando la seguridad de equipos de la red interna y su independencia de los servidores de la DMZ. Se selecciona el firewall más adecuado para garantizar los máximos niveles de seguridad y se configura el direccionamiento IP de routers, hosts y servidores. Se inicializa el firewall y se configuran sus interfaces y el NAT para cumplir con todos los requisitos dados. Se realiza un esquema mostrando la configuración de la DMZ.* |
| 4 | *La DMZ se configura siguiendo las especificaciones dadas y garantizando la seguridad de equipos de la red interna y su independencia de los servidores de la DMZ. Se selecciona un firewall y se configura el direccionamiento IP de routers, hosts y servidores. Se inicializa el firewall y se configuran sus interfaces y el NAT para cumplir con todos los requisitos dados. Se realiza un esquema mostrando la configuración de la DMZ.* |
| 3 | *La DMZ se configura siguiendo las especificaciones dadas y garantizando la seguridad de equipos de la red interna y su independencia de los servidores de la DMZ. Se selecciona un firewall y se configura el direccionamiento IP de routers, hosts y servidores. Se inicializa el firewall y se configuran sus interfaces y el NAT para cumplir con todos los requisitos dados. No se realiza correctamente un esquema de la configuración de la DMZ.* |
| 2 | *La DMZ no se configura siguiendo las especificaciones dadas. Se selecciona un firewall y se configura el direccionamiento IP de routers, hosts y servidores. Se inicializa el firewall pero no se configuran sus interfaces y el NAT para cumplir con todos los requisitos dados. No se realiza correctamente un esquema de la configuración de la DMZ.* |
| 1 | *La DMZ no se configura siguiendo las especificaciones dadas. Se selecciona un firewall pero no se configura correctamente el direccionamiento IP de routers, hosts y servidores. Se inicializa el firewall pero no se configuran sus interfaces y el NAT para cumplir con todos los requisitos dados. No se realiza correctamente un esquema de la configuración de la DMZ.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 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.

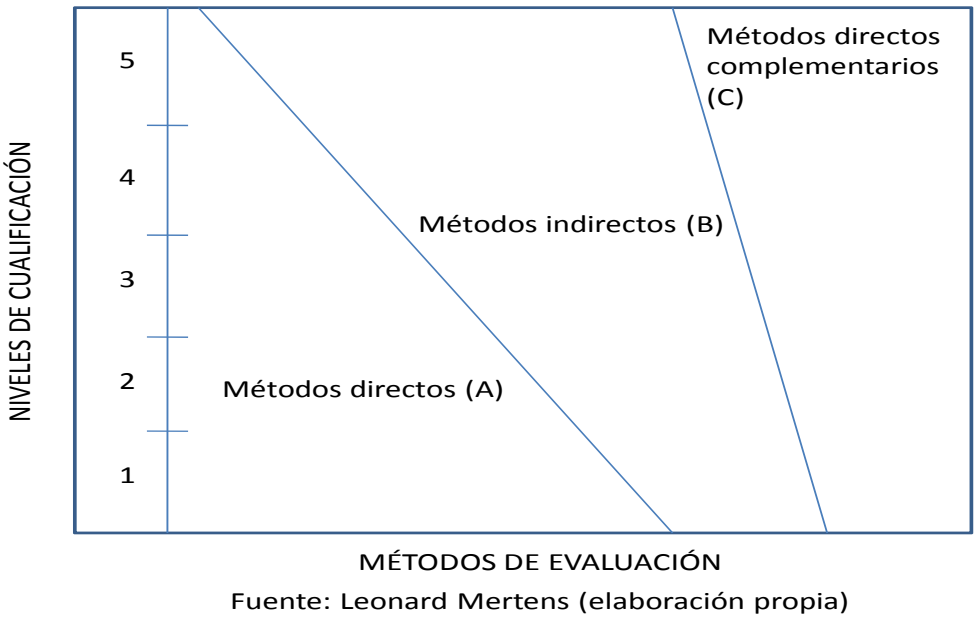
## 2.1. Métodos de evaluación y criterios generales de elección

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 un candidato de bajo nivel cultural al que se le aprecien dificultades de expresión escrita. 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 no formal y no tenga experiencia en aseguramiento de equipos informáticos, se le someterá, al menos, a una prueba profesional de evaluación y a una entrevista profesional estructurada sobre la dimensión relacionada con el “saber” y “saber estar” de la competencia profesional.

b) En la fase de evaluación siempre se deben contrastar las evidencias indirectas de competencia presentadas por la persona candidata. Deberá tomarse como referente 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/a 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 3. En este nivel tiene importancia el dominio de los métodos de trabajo empleados y habilidades en la resolución de imprevistos, por lo que en función del método de evaluación utilizado, se recomienda que en la comprobación de lo explicitado por la persona candidata se complemente con una prueba práctica que tenga como referente las actividades de la situación profesional de evaluación. Esta se planteará sobre un contexto reducido que permita optimizar la observación de competencias, minimizando los medios materiales y el tiempo necesario para su realización, cumpliéndose 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.

h) En el desarrollo de la SPE se recomienda utilizar equipos informáticos de tipo servidor o estación de trabajo con sistemas operativos estándar unidos mediante una red de datos, además de distintos firewall, tanto hardware como software, y las herramientas necesarias para su correcta configuración. Los equipos deberían contar con sus correspondientes sistemas operativos con licencia propietaria o licencia pública general (GPL).

i) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con la seguridad como puede ser el intento de intrusión al sistema por distintas vías o la aparición de virus y malware u otro tipo de incidencias como pueden ser fallos de red o de otro tipo (proporcionando un registro de incidencias simulado a analizar por la persona candidata), a lo largo de las actividades, que tendrá que resolver de forma que plantee la solución más adecuada.

# GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

**“UC0487_3: Auditar redes de comunicación y sistemas informáticos”**

# CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

**Código: IFC153_3** **NIVEL: 3**

# 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 UC0487_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 (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 principales y secundarias que intervienen en la auditoría de redes de comunicación y sistemas informáticos, y que se indican a continuación:

Nota: A un dígito se indican las actividades principales y a dos las actividades secundarias relacionadas.

1. ***Detectar vulnerabilidades en la seguridad de los sistemas, mediante programas específicos, según necesidades de uso y dentro de las directivas de la organización.***

1.1 Seleccionar las herramientas y pruebas de análisis de vulnerabilidades, adecuándolas al entorno a verificar y siguiendo las especificaciones de seguridad de la organización.
1.2 Actualizar los programas y pruebas, minimizando posibles fallos de seguridad de las versiones de hardware y software.
1.3 Contrastar los resultados de las pruebas, documentándolas.
1.4 Comprobar los sistemas de acceso por contraseña, utilizando herramientas específicas y siguiendo las especificaciones de la normativa de seguridad.
1.5 Documentar el análisis de vulnerabilidades, haciendo referencia a aplicaciones y servicios que se han detectado funcionando en el sistema, el nivel de los parches instalados, vulnerabilidades de negación de servicio, vulnerabilidades detectadas y mapa de la red y en formato normalizado.

- Desarrollar las actividades cumpliendo las normas de prevención de riesgos laborales aplicables y los procedimientos y normativa de la organización

***2. Verificar el cumplimiento de la normativa y requisitos legales vigentes en materia de protección de datos personales según las necesidades de uso y dentro de las directivas de la organización.***

2.1 Comprobar que los ficheros con datos de carácter personal tienen asignado un responsable de seguridad de acuerdo con la normativa legal aplicable.
2.2 Comprobar que el listado de personas con acceso autorizado a los ficheros existe y se encuentra actualizado de acuerdo con la normativa legal aplicable.
2.3 Comprobar el control de accesos a los ficheros, siguiendo el procedimiento establecido en la normativa de seguridad de la organización.
2.4 Comprobar que se gestiona el almacenamiento de los ficheros y sus copias de seguridad, siguiendo la normativa legal aplicable y los procedimientos de la organización.
2.5 Comprobar que los mecanismos de acceso telemático a los ficheros garantizan la confidencialidad e integridad de la información que así lo requiera, siguiendo la normativa legal y de la organización.
2.6 Redactar el informe de auditoría, recogiendo la relación de ficheros con datos de carácter personal, contemplando las medidas de seguridad aplicadas e indicando las medidas de seguridad pendientes de aplicación.

- Desarrollar las actividades cumpliendo las normas de prevención de riesgos laborales aplicables y garantizando la confidencialidad e integridad.

***3. Comprobar el cumplimiento de la política de seguridad establecida por la organización según las necesidades de uso y dentro de las directivas de la organización.***

3.1 Verificar que la normativa de seguridad de la organización incluye los procedimientos de detección y gestión de incidentes de seguridad, comprobando los procesos y herramientas implantadas.
3.2 Testear el uso de los puntos de acceso de entrada y salida de la red, verificando que se circunscribe a lo descrito en la normativa de seguridad de la organización.
3.3 Contrastar que los programas de seguridad y protección de sistemas están activados y actualizados, según las especificaciones de los fabricantes, verificando los sistemas y su situación.
3.4 Validar los puntos adicionales de entrada y salida de la red, verificando que son autorizados y controlados según las especificaciones de seguridad y el

plan de implantación de la organización, revisando los registros de autorización y los sistemas de control implantados.

3.5 Revisar los procesos de auditoría informática interna y externa, contrastándolos con alguna auditoría anterior realizada.

3.6 Comprobar el cumplimiento por parte de los usuarios de los procedimientos de las políticas de seguridad, entrevistándose con los usuarios.

- Desarrollar las actividades cumpliendo las normas de prevención de riesgos laborales y siguiendo la normativa legal aplicable.

**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 UC0487_3: Auditar redes de comunicación y sistemas informáticos.

***1. Análisis de vulnerabilidades.***

- Uso de herramientas específicas (análisis de red, puertos y servicios, vulnerabilidades, protocolos, páginas web, ataques informáticos, otros).
- Aseguramiento de la consistencia de los ensayos y del entorno a verificar.
- Aplicación de metodologías de análisis de vulnerabilidades.

***2. Verificación del cumplimiento de la normativa y requisitos legales vigentes en materia de protección de datos personales.***

- Normativa específica aplicable en protección de datos personales.
- Aplicación de metodologías de gestión de calidad.

***3. Cumplimiento de la política de seguridad establecida.***

- Metodologías y procedimientos de detección y gestión de incidentes de seguridad.
- Aplicación de Metodologías de Análisis de Seguridad.
- Métodos de auditoría de sistemas informáticos.

***Saberes comunes que dan soporte a las actividades profesionales de esta unidad de competencia***

- Normativa aplicable de prevención de riesgos laborales.
- Manejo de especificaciones, procedimientos y normativa de seguridad de la organización.
- Manejo de especificaciones de los fabricantes.
- Seguimiento de pruebas y documentación.
- Aplicación de metodologías de análisis de riesgos, impactos, amenazas.
- Aplicación de metodología de auditoría en general.

**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:

1. En relación con otros trabajadores o profesionales deberá:

   1.1 Tratarlos con cortesía, respeto y discreción.
   1.2 Liderar y coordinar equipos de trabajo.
   1.3 Habilidades en la resolución de conflictos.
   1.4 Transmitir indicaciones claras e inequívocas al personal bajo su responsabilidad.
   1.5 Comunicarse eficazmente con las personas del equipo adecuadas en cada momento, respetando los canales establecidos en la organización.
   1.6 Participar y colaborar activamente en el equipo de trabajo.
   1.7 Proponer alternativas con el objetivo de mejorar resultados.

2. En relación con clientes / usuarios deberá:

   2.1 Tratar al cliente con cortesía, respeto y discreción.
   2.2 Cumplir las normas de comportamiento profesional.
   2.3 Demostrar un buen hacer profesional.
   2.4 Capacidad de adaptación al contexto y las necesidades de los usuarios.
   2.5 Finalizar el trabajo en los plazos establecidos.
   2.6 Capacidad de comunicación con los clientes.

3. En relación a la obra, puesto de trabajo y otros aspectos deberá:

   3.1 Cuidar el aspecto y aseo personal como profesional.
   3.2 Responsabilizarse del trabajo que desarrolla, cumpliendo los objetivos y plazos establecidos.
   3.3 Adaptarse a la organización integrándose al sistema de relaciones técnico profesionales.
   3.4 Tener iniciativa para promover proyectos.
   3.5 Capacidad de iniciativa para encontrar información y relacionarse con proveedores.
   3.6 Tener una actitud consecuente con el mundo tecnológico. Limpieza, reciclaje de residuos, ahorro y eficiencia energética.
   3.7 Cuidar los equipos de trabajo y utilizar con economía los materiales.
   3.8 Respetar las instrucciones y normas internas de la empresa.

## 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 UC0487_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 para auditar redes de comunicación y sistemas informáticos en una empresa concreta a partir de las especificaciones legales y normativa de seguridad, con herramientas y metodologías de análisis de riesgos y vulnerabilidades. Esta situación comprenderá al menos las siguientes actividades:

1. Detectar vulnerabilidades en la seguridad de los sistemas.

2. Verificar el cumplimiento de la normativa y requisitos legales vigentes en materia de protección de datos personales.

3. Comprobar el cumplimiento de la política de seguridad establecida.

***Condiciones adicionales:***

- Se dispondrá de la documentación e información necesaria de la empresa, requeridos para la situación profesional de evaluación.

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

- Se planteará alguna contingencia o situación imprevista que sea relevante para la demostración de la competencia relacionada con la respuesta a contingencias.

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

Con el objeto de optimizar la validez y fiabilidad del resultado de la evaluación, esta Guía incluye unos criterios de evaluación integrados y, por tanto, reducidos en número. 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 se especifican en el cuadro siguiente:

| *Criterios de mérito* | *Indicadores, escalas y umbrales de desempeño competente* |
|---|---|
| *Auditoría documental.* | - Revisión de documentación.<br>- Redacción del informe de situación actual.<br><br>*El umbral de desempeño competente está explicitado en la escala A.* |
| *Detección de vulnerabilidades.* | - Planificación del análisis de vulnerabilidades.<br>- Selección de las herramientas y pruebas de análisis.<br>- Actualización de programas y pruebas.<br>- Contraste y documentación de resultados.<br>- Comprobación de los sistemas de acceso por contraseña.<br>- Redacción del informe de análisis de vulnerabilidades.<br><br>*El umbral de desempeño competente está explicitado en la escala B.* |
| *Auditoría del cumplimiento de la normativa y requisitos legales vigentes.* | - Revisión del cumplimiento de la normativa vigente aplicable de protección de datos.<br>- Redacción del informe de auditoría.<br><br>*El umbral de desempeño competente está explicitado en la escala C.* |
| *Auditoría de la política de seguridad.* | - Revisión de la Política de seguridad de la organización.<br>- Redacción del informe de auditoría.<br><br>*El umbral de desempeño competente está explicitado en la escala D.* |

**Escala A**

| | |
|---|---|
| 5 | *Se solicita toda la documentación que incluye: listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos y las auditorías anteriores. Se revisa dicha documentación y se redacta un informe completo de la situación actual de la organización.* |
| **4** | *Se solicita una gran parte de la documentación necesaria (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores). Se revisa dicha documentación y se redacta un informe de situación actual de la organización.* |
| 3 | *Se solicita parte de la documentación necesaria (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores). Se revisa parte de dicha documentación pero sí se redacta un informe de situación actual de la organización aunque no aborda todo lo necesario.* |
| 2 | *Se solicita parte de la documentación (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores). No se revisa dicha documentación pero sí se redacta un informe de situación actual de la organización.* |
| 1 | *No se solicita toda la documentación (listado de activos, las normas, procedimientos y políticas de la organización, el análisis de riesgos, las auditorías anteriores), ni se revisa dicha documentación y no se redacta un informe de situación actual de la organización.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala B**

| | |
|---|---|
| 5 | *Se planifica el análisis de vulnerabilidades incluyendo todas las acciones necesarias para auditar el sistema, se seleccionan adecuadamente las herramientas y pruebas de análisis, se actualizan los programas y pruebas y se comprueban los sistemas de acceso por contraseña, según las especificaciones, procedimientos y normativa de seguridad de la organización. Se contrastan y documentan los resultados, y se redacta un informe completo de análisis de vulnerabilidades.* |
| **4** | *Se planifica el análisis de vulnerabilidades, se seleccionan adecuadamente las herramientas y pruebas de análisis, aunque no se actualizan los programas y pruebas, se comprueban los sistemas de acceso por contraseña, según las especificaciones, procedimientos y normativa de seguridad de la organización. Se contrastan y documentan los resultados, y se redacta un informe completo de análisis de vulnerabilidades.* |
| 3 | *Se planifica el análisis de vulnerabilidades, se seleccionan adecuadamente las herramientas y pruebas de análisis, pero no se actualizan los programas y pruebas, se comprueban los sistemas de acceso por contraseña, pero no se siguen las especificaciones, procedimientos y normativa de seguridad de la organización. Se contrastan y documentan los resultados, y se redacta un informe completo de análisis de vulnerabilidades.* |
| 2 | *No se planifica el análisis de vulnerabilidades, se seleccionan adecuadamente las herramientas y pruebas de análisis, pero no se actualizan los programas y pruebas, ni se comprueban los sistemas de acceso por contraseña, y no se siguen las especificaciones, procedimientos y normativa de seguridad de la organización. Se redacta un informe de análisis de vulnerabilidades.* |
| 1 | *No se planifica el análisis de vulnerabilidades, no se seleccionan adecuadamente las herramientas y pruebas de análisis, no se actualizan los programas y pruebas, ni se comprueban los sistemas de acceso por contraseña, y no se siguen las especificaciones, procedimientos y normativa de seguridad de la organización. No se contrastan y documentan los resultados, ni se redacta un informe de análisis de vulnerabilidades.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala C**

| | |
|---|---|
| 4 | *Se revisa el cumplimiento de todos los siguientes puntos de la legislación vigente en materia de protección de datos: asignación de responsable de seguridad a todos los ficheros con datos de carácter personal, existencia y estado del listado de acceso autorizado a los ficheros, existencia y estado del listado de control de accesos a los ficheros, proceso de gestión del almacenamiento de los ficheros y sus copias de seguridad, mecanismos de acceso telemático a los ficheros. Las deficiencias detectadas se redactan de forma clara, precisa y completa en el informe de auditoría.* |
| **3** | *Se revisa el cumplimiento de como mínimo los siguientes puntos de la legislación vigente en materia de protección de datos: asignación de responsable de seguridad a todos los ficheros con datos de carácter personal, existencia del listado de acceso autorizado a los ficheros, existencia del listado de control de accesos a los ficheros, proceso de gestión del almacenamiento de los ficheros y sus copias de seguridad, mecanismos de acceso telemático a los ficheros. Las deficiencias detectadas se redactan de forma clara, precisa y completa en el informe de auditoría.* |
| 2 | *Se revisa parcialmente el cumplimiento de los siguientes puntos de la legislación vigente en materia de protección de datos: asignación de responsable de seguridad a todos los ficheros con datos de carácter personal, existencia del listado de acceso autorizado a los ficheros, existencia del listado de control de accesos a los ficheros, proceso de gestión del almacenamiento de los ficheros y sus copias de seguridad, mecanismos de acceso telemático a los ficheros. No se incluyen las deficiencias detectadas de forma clara en el informe.* |
| 1 | *No se revisan muchos de los aspectos fundamentales de la legislación vigente en materia de protección de datos.* |

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

**Escala D**

| | |
|---|---|
| 4 | *Se revisa exhaustivamente el cumplimiento de la Política de seguridad de la organización que incluye la verificación de la existencia y funcionalidad de los procedimientos de detección y gestión de incidentes de seguridad, de uso de los puntos de acceso de entrada y salida de red, de activación y actualización de los programas de seguridad y protección de sistemas, de autorización y control de los puntos de entrada y salida de la red, de los procesos de auditoría, del cumplimiento de los usuarios de los procedimientos de las políticas de seguridad. Se redacta un informe de auditoría que incluye todas las deficiencias detectadas en política de seguridad.* |
| **3** | *Se revisa el cumplimiento de la Política de seguridad de la organización que incluye la verificación de la existencia de los procedimientos de detección y gestión de incidentes de seguridad, de uso de los puntos de acceso de entrada y salida de red, de activación y actualización de los programas de seguridad y protección de sistemas, de autorización y control de los puntos de entrada y salida de la red, de los procesos de auditoría, del cumplimiento de los usuarios de los procedimientos de las políticas de seguridad. Se redacta un informe de auditoría que incluye todas las deficiencias detectadas en política de seguridad.* |
| 2 | *Se revisa parcialmente el cumplimiento de la Política de seguridad de la organización que incluye la verificación de la existencia y funcionalidad de los procedimientos de detección y gestión de incidentes de seguridad, de uso de los puntos de acceso de entrada y salida de red, de activación y actualización de los programas de seguridad y protección de sistemas, de autorización y control de los puntos de entrada y salida de la red, de los procesos de auditoría, del cumplimiento de los usuarios de los procedimientos de las políticas de seguridad. Se redacta un informe de auditoría que no incluye todas las deficiencias detectadas.* |
| 1 | *No se revisa adecuadamente el cumplimiento de la Política de seguridad de la organización. Se redacta un informe de auditoría.* |

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.

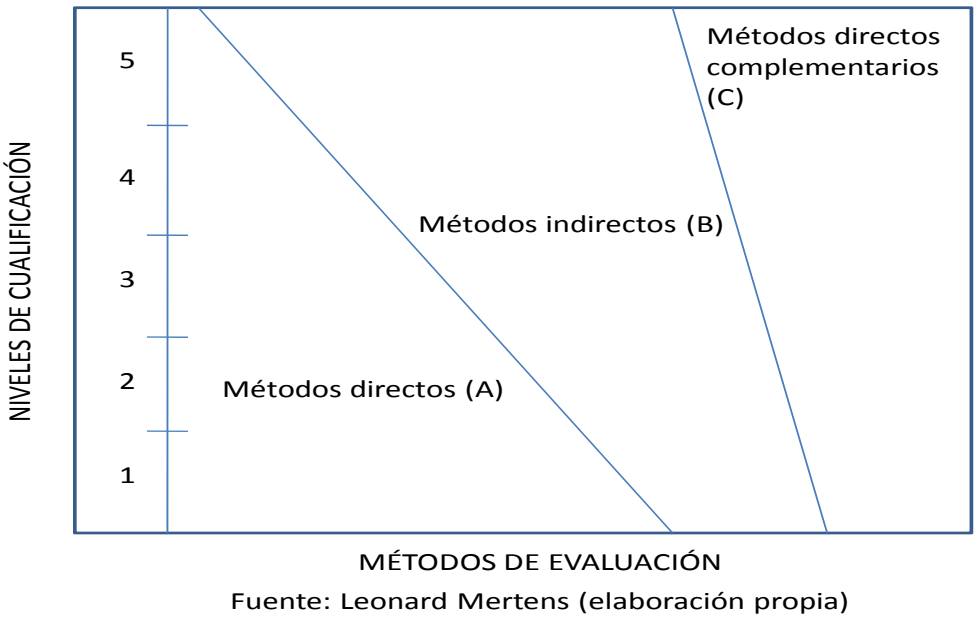
### 2.1. Métodos de evaluación y criterios generales de elección

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 un candidato de bajo nivel cultural al que se le aprecien dificultades de expresión escrita. 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 no formal y no tenga experiencia en 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 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/a 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 3. En este nivel tiene importancia el dominio de habilidades de planificación y realización de informes de auditoría, por lo que en función del método de evaluación utilizado, se recomienda que en la comprobación de lo explicitado por la persona candidata se complemente con una prueba práctica que tenga como referente las actividades de la situación profesional de evaluación. Esta se planteará sobre un contexto reducido que permita optimizar la observación de competencias, minimizando los medios materiales y el tiempo necesario para su realización, cumpliéndose 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.

h) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con la documentación contemplada en el caso práctico, siendo errónea en algunos casos, no coherente con el resto de documentos o que no incluya parte de la información, que tendrá que resolver de forma que plantee la solución más adecuada.

# GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

**“UC0488_3: Detectar y responder ante incidentes de seguridad”.**

## CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

**Código: IFC153_3** **NIVEL: 3**

# 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 UC0488_3: Detectar y responder ante incidentes de seguridad.

## 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 principales y secundarias que intervienen en la detección y respuesta ante incidentes de seguridad, y que se indican a continuación:

Nota: A un dígito se indican las actividades principales y a dos las actividades secundarias relacionadas.

***1. Implantar procedimientos de respuesta ante incidentes y mecanismos de detección de intrusos según directrices nacionales e internacionales.***

1.1 Verificar que los procedimientos de detección y respuesta de incidentes están documentados indicando los roles y responsabilidades de seguridad, según la política de la organización.
1.2 Testear que los sistemas se modelan de forma que se detecten signos de comportamiento sospechoso.
1.3 Chequear que los mecanismos de registro del sistema están activados y se planifican los procedimientos de análisis de los mismos, según las especificaciones de seguridad.
1.4 Comprobar que los sistemas de detección de intrusos están instalados, actualizados y configurados en función de las especificaciones de seguridad.
1.5 Verificar que los procedimientos de restauración del sistema informático permiten la recuperación del mismo dentro de las necesidades de la organización.

- Desarrollar las actividades cumpliendo las normas de prevención de riesgos laborales aplicables, siguiendo las especificaciones de seguridad y procedimientos de la organización y asegurando la consistencia de los ensayos y del entorno a verificar.

***2. Detectar incidentes de seguridad de forma activa y preventiva, minimizando el riesgo, según directrices nacionales e internacionales.***

2.1 Comprobar que las herramientas de detección de intrusiones utilizadas no han sido comprometidas ni afectadas por programas maliciosos, analizando su funcionamiento.
2.2 Detectar funcionamientos sospechosos a partir de un análisis de los parámetros con herramientas específicas según la normativa de seguridad.
2.3 Verificar periódicamente la integridad de los componentes software del sistema usando programas específicos.
2.4 Probar el correcto funcionamiento de los dispositivos de protección física del sistema informático de acuerdo con la normativa de seguridad de la organización.
2.5 Redactar un informe diario de actividad incluyendo los sucesos y signos extraños que pudieran considerarse una alerta.

- Desarrollar las actividades cumpliendo las normas de prevención de riesgos laborales aplicables, siguiendo las especificaciones de seguridad y procedimientos de la organización y asegurando la consistencia de los ensayos y del entorno a verificar.

***3. Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas de contención y solución de incidentes según los requisitos de servicio y las directivas de la organización.***

3.1 Iniciar los protocolos de seguridad cuando se detecta un incidente siguiendo la normativa de seguridad de la organización.
3.2 Aislar el sistema vulnerado, recogiendo información para el análisis forense de la incidencia según los procedimientos de seguridad de la organización.
3.3 Analizar el sistema atacado mediante herramientas de detección de intrusos según los procedimientos de seguridad de la organización.

3.4 Contener la intrusión mediante la aplicación de las medidas establecidas en la normativa de seguridad de la organización.
3.5 Documentar el incidente de forma que permita su análisis posterior y la implantación de medidas que impidan que se repita la situación.
3.6 Determinar los daños causados del sistema atacado según las directivas de la organización.
3.7 Planificar las acciones a tomar que restituyan la normal prestación de servicios del sistema vulnerado según las normas de calidad y el plan de explotación de la organización.

- Desarrollar las actividades cumpliendo las normas de prevención de riesgos laborales aplicables, siguiendo los procedimientos de la organización y asegurando la consistencia de los ensayos y del entorno a verificar.

## 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 UC0488_3: Detectar y responder ante incidentes de seguridad. Estos conocimientos se presentan agrupados a partir de las actividades profesionales principales que aparecen en cursiva y negrita:

### *1. Implantación de procedimientos de respuesta ante incidentes y mecanismos de detección de intrusos.*

- Procedimientos de detección y respuesta ante incidentes:
  - Políticas de seguridad.
  - Roles.
  - Responsabilidades de seguridad.
- Mecanismos de detección de intrusos:
  - Instalación.
  - Actualización.
  - Modelado de sistemas.
  - Mecanismos de registro.
- Restauración de un sistema informático:
  - Configuración.
  - Recuperación de datos.

### *2. Detección activa y preventiva de incidentes de seguridad.*

- Análisis del funcionamiento de herramientas de detección de intrusos:
  - Parámetros indicativos
- Utilización de herramientas de detección de intrusos y de funcionamientos sospechosos.
- Pruebas de dispositivos de protección física.

### *3. Coordinación de la respuesta ante incidentes.*

- Especificaciones, procedimientos y normativa de seguridad de una organización:
- Especificaciones, procedimientos y normativa de calidad de la organización.
- Aplicación de Metodologías de Análisis de Seguridad.

- Aplicación de Metodologías de análisis de riesgos, vulnerabilidades, impactos, amenazas, contención de intrusos...

***Saberes comunes que dan soporte a las actividades profesionales de esta unidad de competencia***

- Normas de prevención de riesgos laborales aplicable.
- Normativa legal aplicable.
- Uso de herramientas específicas (análisis de red, puertos y servicios, vulnerabilidades, detección de intrusión, antivirus, protocolos, páginas web, ataques informáticos, etc.).
- Aplicación de Metodologías de Análisis de Seguridad.
- Aseguramiento de la consistencia de los ensayos y del entorno a verificar.
- Documentación de las pruebas.
- Aplicación de Metodologías de análisis de riesgos, vulnerabilidades, impactos y amenazas.
- Aplicación de Metodología de auditoría.

## 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:

1. En relación con otros trabajadores o profesionales deberá:

   1.1 Tratarlos con cortesía, respeto y discreción.
   1.2 Liderar y coordinar equipos de trabajo.
   1.3 Habilidades en la resolución de conflictos.
   1.4 Transmitir indicaciones claras e inequívocas al personal bajo su responsabilidad.
   1.5 Comunicarse eficazmente con las personas del equipo adecuadas en cada momento, respetando los canales establecidos en la organización.
   1.6 Participar y colaborar activamente en el equipo de trabajo.
   1.7 Proponer alternativas con el objetivo de mejorar resultados.

2. En relación con clientes / usuarios deberá:

   2.1 Tratar al cliente con cortesía, respeto y discreción.
   2.2 Cumplir las normas de comportamiento profesional.
   2.3 Demostrar un buen hacer profesional.
   2.4 Capacidad de adaptación al contexto y las necesidades de los usuarios.
   2.5 Finalizar el trabajo en los plazos establecidos.
   2.6 Capacidad de comunicación con los clientes.

3. En relación a la obra, puesto de trabajo y otros aspectos deberá:

   3.1 Cuidar el aspecto y aseo personal como profesional.
   3.2 Responsabilizarse del trabajo que desarrolla, cumpliendo los objetivos y plazos establecidos.
   3.3 Adaptarse a la organización integrándose al sistema de relaciones técnico profesionales.
   3.4 Tener iniciativa para promover proyectos.

3.5 Capacidad de iniciativa para encontrar información y relacionarse con proveedores.
3.6 Tener una actitud consecuente con el mundo tecnológico. Limpieza, reciclaje de residuos, ahorro y eficiencia energética.
3.7 Cuidar los equipos de trabajo y utilizar con economía los materiales.
3.8 Respetar las instrucciones y normas internas de la empresa.

## 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 UC0488_3: Detectar y responder ante incidentes de seguridad, 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 detectar y responder ante incidentes de seguridad en un entorno compuesto por una empresa que disponga de una red de comunicaciones con salida al exterior con varios equipos en funcionamiento en más de dos áreas y con una política de seguridad definida. Esta situación comprenderá al menos las siguientes actividades:

1. Implantar procedimientos de respuesta ante incidentes y mecanismos de detección de intrusos.

2. Detectar incidentes de seguridad de forma activa y preventiva.

3. Coordinar la respuesta ante incidentes de seguridad.

***Condiciones adicionales:***

- Se dispondrá de los equipos, herramientas de análisis y documentación requeridos para la situación profesional de evaluación.

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

- Se deberá evaluar la respuesta a las contingencias. Para ello se podrá plantear una situación anómala no contemplada inicialmente en el caso práctico.

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

Con el objeto de optimizar la validez y fiabilidad del resultado de la evaluación, esta Guía incluye unos criterios de evaluación integrados y, por tanto, reducidos en número. 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 se especifican en el cuadro siguiente:

| *Criterios de mérito* | *Indicadores, escalas y umbrales de desempeño competente* |
|---|---|
| *Implantación de procedimientos de respuesta ante incidentes y mecanismos de detección de intrusos.* | - Verificación de que los procedimientos de detección y respuesta de incidentes están documentados, incluyen los roles y responsabilidades de seguridad e implementan correctamente la política de seguridad necesaria en la empresa.<br>- Testeo de que los sistemas se modelan de forma que se detecten signos de comportamiento malicioso.<br>- Chequeo de que los mecanismos de registro del sistema están activados y que se planifican los procedimientos de análisis de los mismos según las especificaciones.<br>- Comprobación de que los sistemas de detección de intrusos están instalados, actualizados y configurados en función de las especificaciones de seguridad.<br>- Verificación de que los procedimientos de restauración del sistema informático permiten la recuperación del mismo.<br><br>*El umbral de desempeño competente requiere el cumplimiento total de los indicadores del criterio de mérito.* |

| | |
|---|---|
| *Detección de incidentes de seguridad.* | - Comprobación de las herramientas de detección de intrusiones.<br>- Análisis de los parámetros.<br>- Verificación periódica de los componentes software.<br>- Prueba del funcionamiento de los dispositivos de protección física.<br>- Redacción del informe diario de actividad.<br><br>*El umbral de desempeño competente está explicitado en la escala A.* |
| *Coordinación de la respuesta ante incidentes de seguridad.* | - Inicio de los protocolos de seguridad.<br>- Aislamiento del sistema vulnerado y recogida de información.<br>- Análisis el sistema atacado.<br>- Contención de la intrusión.<br>- Documentación del incidente.<br>- Determinación de los daños causados.<br>- Planificación de las acciones a tomar.<br><br>*El umbral de desempeño competente está explicitado en la escala B.* |

**Escala A**

| | |
|---|---|
| 5 | *Se comprueba que todas las herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos. Se analizan todos los parámetros de funcionamiento, se verifican periódicamente los componentes software del sistema, se comprueba el funcionamiento de los dispositivos de protección física del sistema informático y se redacta el informe diario de actividad.* |
| **4** | *Se comprueba que las herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos, se analizan únicamente los parámetros de funcionamiento críticos, se verifican periódicamente los componentes software del sistema, se comprueba el funcionamiento de los dispositivos de protección física del sistema informático, y se redacta el informe diario de actividad.* |
| 3 | *No se comprueba que las herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos, no se analizan todos los parámetros de funcionamiento críticos, se verifican periódicamente los componentes software del sistema, se comprueba el funcionamiento de los dispositivos de protección física del sistema informático, y no se redacta el informe diario de actividad.* |
| 2 | *No se comprueba que las herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos, no se analizan todos los parámetros de funcionamiento críticos, no se verifican periódicamente los componentes software del sistema, ni se comprueba el funcionamiento de los dispositivos de protección física del sistema informático, pero no se redacta el informe diario de actividad.* |
| 1 | *No se comprueba que las herramientas utilizadas para detectar intrusiones no han sido comprometidas ni afectadas por programas maliciosos, no se analizan todos los parámetros de funcionamiento críticos, no se verifican periódicamente los componentes software del sistema, ni se comprueba el funcionamiento de los dispositivos de protección física del sistema informático, y no se redacta el informe diario de actividad.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala B**

| | |
|---|---|
| 5 | *Se inician los protocolos de seguridad cuando se detecta un incidente, se aísla el sistema vulnerado y se recoge toda la información para su análisis forense, se analiza el sistema atacado, se contiene la intrusión, se documenta el incidente para su análisis, se determinan los daños causados del sistema atacado y se planifican las acciones a tomar para continuar con la normal prestación de servicios del sistema vulnerado* |
| **4** | *Se inician los protocolos de seguridad cuando se detecta un incidente, se aísla el sistema vulnerado y se recoge únicamente la información crítica para su análisis forense, se analiza el sistema atacado, se contiene la intrusión, se documenta el incidente para su análisis, se determinan los daños causados del sistema atacado y se planifican las acciones a tomar para continuar con la normal prestación de servicios del sistema vulnerado* |
| 3 | *Se inician los protocolos de seguridad cuando se detecta un incidente, no se aísla el sistema vulnerado ni se recoge información para su análisis forense, se analiza el sistema atacado, se contiene la intrusión, se documenta el incidente para su análisis, se determinan los daños causados del sistema atacado y se planifican las acciones a tomar para continuar con la normal prestación de servicios del sistema vulnerado* |
| 2 | *Se inician los protocolos de seguridad cuando se detecta un incidente, no se aísla el sistema vulnerado ni se recoge información para su análisis forense, se analiza el sistema atacado, se contiene la intrusión, no se documenta el incidente para su análisis, se determinan los daños causados del sistema atacado y se planifican las acciones a tomar para continuar con la normal prestación de servicios del sistema vulnerado* |
| 1 | *Se inician los protocolos de seguridad cuando se detecta un incidente, no se aísla el sistema vulnerado ni se recoge información para su análisis forense, se analiza el sistema atacado, se contiene la intrusión, no se documenta el incidente para su análisis, se determinan los daños causados del sistema atacado pero no se planifican las acciones a tomar para continuar con la normal prestación de servicios del sistema vulnerado* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 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.

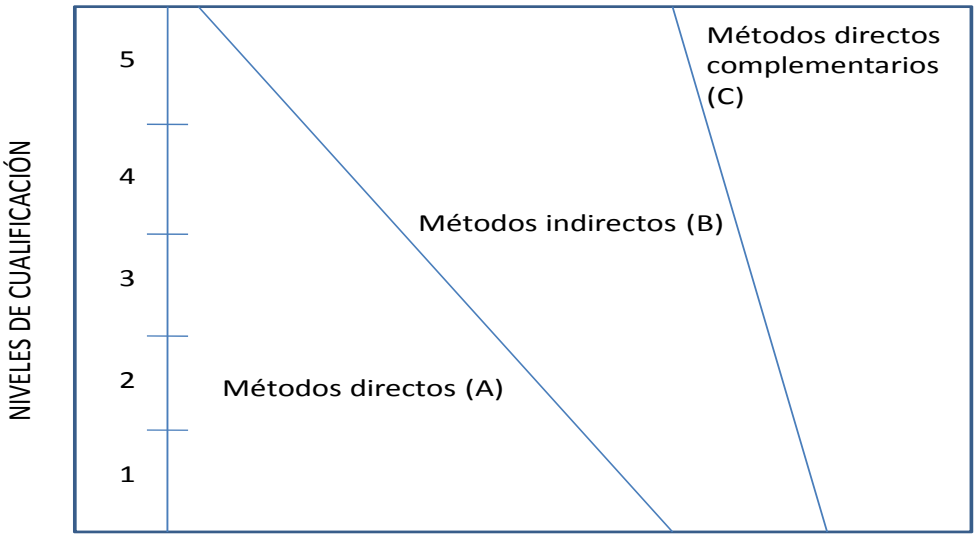
## 2.1. Métodos de evaluación y criterios generales de elección

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 un candidato de bajo nivel cultural al que se le aprecien dificultades de expresión escrita. 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 no formal y no tenga experiencia en la detección y respuesta ante incidentes de seguridad, 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/a 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 3. En este nivel tiene importancia el dominio de la planificación y realización de informes, por lo que en función del método de evaluación utilizado, se recomienda que en la comprobación de lo explicitado por la persona candidata se complemente con una prueba práctica que tenga como referente las actividades de la situación profesional de evaluación. Esta se planteará sobre un contexto reducido que permita optimizar la observación de competencias, minimizando los medios materiales y el tiempo necesario para su realización, cumpliéndose 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.

h) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con la documentación contemplada en el caso práctico, siendo errónea en algunos casos, no coherente con el resto de documentos o que no incluya parte de la información, situación que tendrá que resolver de forma que plantee la solución más adecuada.

# GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

**“UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos”**

## CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

**Código: IFC153_3** **NIVEL: 3**

# 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 UC0489_3: Diseñar e 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 (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 principales y secundarias que intervienen en el diseño e implementación de sistemas seguros de acceso y transmisión de datos, y que se indican a continuación:

Nota: A un dígito se indican las actividades principales y a dos las actividades secundarias relacionadas.

1. ***Aplicar políticas de seguridad y cifrado de información en las conexiones de red, siguiendo las directivas de la organización y de acuerdo con las necesidades de uso.***

    1.1 Seleccionar los requerimientos de implantación de la solución de red privada virtual, adecuándolos al plan de seguridad.
    1.2 Implantar el uso de VPN en las comunicaciones con otras compañías, según normativa de seguridad y el diseño de la red de la organización.
    1.3 Seleccionar las técnicas de protección de conexiones inalámbricas más idóneas, teniendo en cuenta las normas de seguridad.
    1.4 Implantar el uso de servicios a través de la red telemática que emplean técnicas criptográficas, según la normativa de seguridad de la organización.
    1.5 Implantar el uso de servicios de encapsulación en aquellos servicios que no incorporan técnicas criptográficas, garantizando la seguridad de las comunicaciones.
    1.6 Implantar el uso de servicios que incorporan soporte para certificados digitales, garantizando la identidad del servidor.

2. ***Implantar sistemas de firma digital en la transferencia de información, siguiendo las directivas de la organización y de acuerdo con las necesidades de uso.***

    2.1 Implantar el uso de autenticación basada en certificados digitales al acceder a servicios a través de la red telemática.
    2.2 Asegurar que se aplica el proceso de obtención y verificación de firmas si es necesario, según requerimientos del sistema informático y procesos de negocio.
    2.3 Asegurar que se utilizan certificados digitales firmando y cifrando su contenido en los mensajes de correo electrónico.
    2.4 Asegurar el empleo de sistemas de firma digital de documentos con certificados digitales, según normativa de seguridad de la organización.
    2.5 Definir sistemas de sellado digital de tiempo en documentos, según normativa de seguridad de la organización.
    2.6 Garantizar la integridad de los componentes web mediante firmas digitales.

3. ***Implementar infraestructuras de clave pública, siguiendo las directivas de la organización.***

    3.1 Diseñar la jerarquía de la certificación, en función de las necesidades de la organización.
    3.2 Redactar las prácticas y políticas de certificación, de forma que definan los procedimientos, derechos y obligaciones de los usuarios y los responsables de la autoridad de certificación.
    3.3 Instalar el sistema de autoridad de certificación, siguiendo las indicaciones del fabricante.
    3.4 Ofrecer a los usuarios de manera eficiente, el certificado y la política de certificación, siguiendo las directivas contenidas en las prácticas de certificación.
    3.5 Mantener segura la clave privada de la autoridad de certificación, creando las copias de respaldo establecidas en las prácticas de certificación.
    3.6 Emitir los certificados digitales, según los usos que va a recibir esos certificados y siguiendo los procedimientos indicados en las prácticas de certificación.

3.7 Mantener accesible el servicio de revocación de certificados para consultar la validez de los certificados, según lo indicado en las prácticas de certificación. Desarrollar las actividades siguiendo las directivas contenidas en las prácticas de certificación.

**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 UC0489_3 Diseñar e implementar sistemas seguros de acceso y transmisión de datos. Estos conocimientos se presentan agrupados a partir de las actividades profesionales principales que aparecen en cursiva y negrita:

***1. Implantación de políticas de seguridad y cifrado de información en las conexiones de red.***

- Comunicaciones Seguras:
  - Definición, finalidad y funcionalidad de redes privadas virtuales.
  - Protocolo IPSec.
  - Protocolos SSL y SSH.
  - Túneles cifrados.
  - Ventajas e inconvenientes de las diferentes implantaciones de VPN.

***2. Implantación de sistemas de firma digital en la transferencia de información.***

- Identidad electrónica. Firma Electrónica. Certificados digitales.
- Campos y estructura de los certificados digitales.
- Obtención, verificación y uso de los certificados digitales.
- Propiedades de la firma electrónica reconocida.
- Integridad del firmante. Integridad del documento. Garantizar el no repudio.
- Aplicaciones y usos de la firma electrónica.
- Firma nativa y no nativa de documentos electrónicos.
- Sellado digital de tiempo en documentos.

***3. Implementación de infraestructuras de clave pública.***

- Infraestructura de clave pública (PKI):
  - Identificación y componentes de una PKI y su modelo de relaciones.
  - Autoridad de certificación y sus elementos.
  - Política de certificado y declaración de prácticas de certificación (CPS).
  - Lista de certificados revocados (CRL).
  - Funcionamiento de las solicitudes de firma de certificados (CSR).
  - Infraestructura de gestión de privilegios (PMI).
  - Campos de certificados de atributos.
  - Aplicaciones que se apoyan en la existencia de una PKI.
  - Política de certificado y declaración de prácticas de certificación.
- Jerarquías de autoridades de certificación. Infraestructuras de gestión de privilegios (PMI).

***Saberes comunes que dan soporte a las actividades profesionales de esta unidad de competencia***

- Criptografía:
  - Teoría de la información.
  - Propiedades de la seguridad: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos.
  - Elementos fundamentales de la criptografía de clave privada y de clave pública.
  - Características y atributos de los certificados digitales.
  - Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente.
  - Algoritmos criptográficos más frecuentemente utilizados.
  - Elementos fundamentales de las funciones resumen y los criterios para su utilización.
  - Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización.

## 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:

1. En relación con los usuarios deberá:

   1.1 Tratar a los usuarios con cortesía y respeto.
   1.2 Comunicarse de forma correcta y cordial.
   1.3 Saber trabajar con el cliente presente.
   1.4 Ser asertivo.
   1.5 Finalizar el trabajo en los plazos establecidos.
   1.6 Mostrar capacidad resolutiva en la gestión de avisos de averías.

2. En relación con los compañeros deberá:

   2.1 Cumplir con las tareas asignadas siguiendo los procedimientos operativos, respetando el trabajo de otros compañeros.
   2.2 Transmitir la información que sea necesaria al resto de compañeros para la correcta ejecución del trabajo.
   2.3 Comunicarse de forma correcta y cordial.

3. En relación con otros aspectos deberá:

   3.1 Cuidar el aspecto y aseo personal.
   3.2 Cumplir las normas de comportamiento profesional.
   3.3 Mantener una actitud preventiva ante los riesgos laborales, cumpliendo las normativas de seguridad laboral.
   3.4 Tratar las herramientas, componentes, dispositivos y equipamiento con el máximo cuidado.
   3.5 Ser ordenado y limpio en el lugar de trabajo.
   3.6 Demostrar interés hacia el trabajo a realizar.

## 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 UC0489_3: Diseñar e 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 diseñar e implementar sistemas seguros de acceso y transmisión de datos utilizando un entorno de red en funcionamiento que incluya como mínimo un router, un firewall o “appliance”, un servidor y dos equipos de cliente, con conexión al exterior por medio de un acceso a Internet. Esta situación comprenderá al menos las siguientes actividades:

1. Implantar la utilización de técnicas criptográficas.

2. Implantar la utilización de la firma digital.

3. Crear una infraestructura de clave pública (PKI).

***Condiciones adicionales:***

- Se dispondrá de equipamientos, software específico y ayudas técnicas requeridas para el desarrollo de la situación profesional de evaluación.

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

- Se planteará alguna contingencia o situación imprevista que sea relevante para la demostración de la competencia relacionada con la respuesta a contingencias.

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

Con el objeto de optimizar la validez y fiabilidad del resultado de la evaluación, esta Guía incluye unos criterios de evaluación integrados y, por tanto, reducidos en número. 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 se especifican en el cuadro siguiente:

| *Criterios de mérito* | *Indicadores, escalas y umbrales de desempeño competente* |
|---|---|
| *Implantación de técnicas criptográficas.* | - Elección de protocolos seguros.<br>- Utilización de certificados digitales.<br>- Configuración de VPN.<br>- Protección en conexiones inalámbricas.<br><br>*El umbral de desempeño competente está explicitado en la escala A.* |
| *Aplicación de la firma digital.* | - Firma de los mensajes de correo.<br>- Cifrado de los mensajes de correo.<br>- Firma de los documentos digitales.<br>- Utilización del sellado digital en los documentos.<br><br>*El umbral de desempeño competente está explicitado en la escala B.* |

| | |
|---|---|
| *Creación de una infraestructura de clave pública.* | - Redacta las políticas de certificación según las directrices recibidas.<br>- Ofrece la petición y emisión de certificados como Autoridad de Certificación de manera eficiente siguiendo las directivas otorgadas.<br>- Crea copias de seguridad de la clave privada de la autoridad de certificación manteniendo ésta segura en todo momento.<br>- Posibilita la revocación de certificados y la consulta de validez en todos los casos.<br><br>*El umbral de desempeño competente requiere el cumplimiento total de los indicadores del criterio de mérito.* |

## Escala A

| | |
|---|---|
| 5 | *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido siempre preferentemente protocolos seguros y se ha garantizado la identidad de los servidores mediante certificados digitales en todos los casos. La configuración de la VPN entre distintas sedes ha sido correcta y las conexiones inalámbricas se han protegido de la manera más eficaz posible.* |
| **4** | *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido siempre preferentemente protocolos seguros y se ha garantizado la identidad de los servidores mediante certificados digitales en todos los casos. La configuración de la VPN entre distintas sedes ha sido correcta y las conexiones inalámbricas se han protegido.* |
| 3 | *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido siempre preferentemente protocolos seguros y se ha garantizado la identidad de los servidores mediante certificados digitales en todos los casos. La configuración de la VPN entre distintas sedes ha sido defectuosa y las conexiones inalámbricas no se han protegido completamente.* |
| 2 | *La implantación de técnicas criptográficas en las conexiones de red se ha realizado según las directivas recibidas. Se ha elegido protocolos seguros solo en algunos casos y no se ha garantizado la identidad de los servidores mediante certificados digitales. La configuración de la VPN entre distintas sedes ha sido incorrecta y las conexiones inalámbricas no se han protegido.* |
| 1 | *La implantación de técnicas criptográficas en las conexiones de red no se ha realizado según las directivas recibidas. No se ha elegido protocolos seguros y no se ha garantizado la identidad de los servidores mediante certificados digitales. No se ha configurado VPN y las conexiones inalámbricas no se han protegido.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala B**

| | |
|---|---|
| 4 | *La aplicación de la firma digital se ha ejecutado de manera correcta. Se ha seguido todas las directivas recibidas fielmente. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización de la mejor manera posible. Se ha permitido la posibilidad de firmar y sellar digitalmente todos los documentos de la organización de forma eficaz.* |
| 3 | *La aplicación de la firma digital se ha ejecutado de manera correcta. Se ha seguido las directivas recibidas. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización. Se ha permitido la posibilidad de firmar y sellar digitalmente todos los documentos de la organización.* |
| 2 | *La aplicación de la firma digital se ha ejecutado de manera correcta. No se ha seguido todas las directivas recibidas. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización. No se ha permitido la posibilidad de firmar ni la de sellar digitalmente todos los documentos de la organización.* |
| 1 | *La aplicación de la firma digital no se ha ejecutado de manera correcta. No se ha seguido todas las directivas recibidas. Se ha realizado la implementación para el firmado y cifrado de todos los correos de la organización de manera incorrecta. No se ha permitido la posibilidad de firmar ni la de sellar digitalmente todos los documentos de la organización.* |

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.

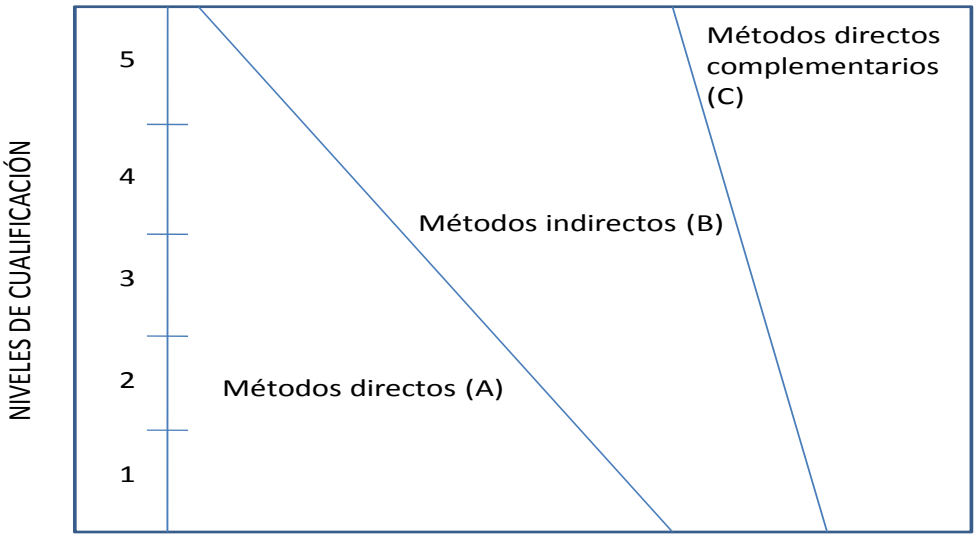
### 2.1. Métodos de evaluación y criterios generales de elección

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 un candidato de bajo nivel cultural al que se le aprecien dificultades de expresión escrita. 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 no formal y no tenga experiencia en el diseño e implementación de 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 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/a 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 3. En este nivel tiene importancia la capacidad de estar bien informado y actualizado sobre temas tecnológicos y seguridad, además de manejar y conocer los diferentes sistemas operativos existentes, por lo que en función del método de

evaluación utilizado, se recomienda que en la comprobación de lo explicitado por la persona candidata se complemente con una prueba práctica que tenga como referente las actividades de la situación profesional de evaluación. Esta se planteará sobre un contexto reducido que permita optimizar la observación de competencias, minimizando los medios materiales y el tiempo necesario para su realización, cumpliéndose 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.

h) En el desarrollo de la SPE se recomienda proporcionar indicaciones sobre directivas y las necesidades de uso de la organización.

i) Para valorar la competencia de respuesta a las contingencias, se recomienda considerar una serie de incidencias en relación con el sistemas operativo elegido para la implantación de la Autoridad de Certificación, un cambio en el software con el que cifrar los documentos o en el de gestión del correo electrónico mediante clave pública, que tendrá que resolver de forma que plantee la solución más adecuada.

# GUÍA DE EVIDENCIA DE LA UNIDAD DE COMPETENCIA

## “UC0490_3: Gestionar servicios en el sistema informático”

***Transversal en las siguientes cualificaciones:***

| | |
|---|---|
| IFC153_3 | Seguridad informática. |
| IFC156_3 | Administración de servicios de Internet. |
| IFC303_3 | Programación de sistemas informáticos. |
| IFC365_3 | Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia y de videovigilancia. |

# CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

## Código: IFC153_3 NIVEL: 3

# 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 UC0490_3: Gestionar servicios en el sistema informático.

## 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 principales y secundarias que intervienen en la gestión de servicios en el sistema informático, y que se indican a continuación:

Nota: A un dígito se indican las actividades principales y a dos las actividades secundarias relacionadas.

***1. Gestionar el sistema informático siguiendo las directivas de la organización de acuerdo con las necesidades de uso.***

1.1 Determinar los parámetros de rendimiento de los procesos del sistema informático evaluando las necesidades de los procesos y prioridades.
1.2 Ajustar los parámetros que afectan a los componentes del sistema informático y a las necesidades de uso de acuerdo con el plan de explotación.
1.3 Establecer las prioridades de ejecución de los procesos del sistema informático en función al plan de explotación de la organización.
1.4 Instalar herramientas de monitorización configurándolas en función al plan de explotación de la organización.

***2. Administrar los dispositivos de almacenamiento del sistema informático siguiendo las directivas de la organización, según necesidades de uso.***

2.1 Configurar los dispositivos de almacenamiento en los distintos sistemas operativos utilizados atendiendo a las especificaciones de la organización.
2.2 Definir la estructura de almacenamiento del sistema informático atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de la organización.
2.3 Documentar los requerimientos de nomenclatura de objetos y las restricciones de usos de cada dispositivo de almacenamiento, especificando técnicamente la información.
2.4 Integrar los dispositivos de almacenamiento para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

**3.** ***Gestionar las tareas de usuarios garantizando los accesos al sistema y la disponibilidad de los recursos, según especificaciones de explotación del sistema informático.***

3.1 Configurar el acceso de los usuarios al sistema informático garantizando la seguridad e integridad del sistema, según las especificaciones de la organización.
3.2 Limitar los recursos disponibles a los usuarios con herramientas adecuadas, en base a lo especificado en las normas de uso de la organización.
3.3 Organizar perfiles de acceso en función de sus características y en relación con los roles del personal de la organización.

***4. Gestionar los servicios de red asegurando la comunicación entre sistemas, según necesidades de explotación.***

4.1 Verificar la configuración y rendimiento de los dispositivos de comunicación, según las especificaciones de la organización.
4.2 Verificar que el consumo de recursos de los servicios de comunicaciones están dentro de lo permitido en el plan de explotación de la organización.
4.3 Documentar las incidencias en los servicios de comunicaciones informando a los responsables de la explotación del sistema, según los protocolos de 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 las realizaciones profesionales de la UC0490_3: Gestionar servicios en el sistema informático.

***1. Gestión del sistema informático siguiendo las directivas de la organización.***

- Procesos de un sistema informático:
  - Estados de un proceso.
  - Manejo de señales y cambio de prioridades.
  - Monitorización de un proceso.
  - Administración de un proceso y cambio de prioridades.
- Gestión del consumo de recursos en de un sistema informático:
  - Monitorización de los recursos.
  - Técnicas utilizadas para la gestión del consumo de recursos.
  - Establecimiento de los límites normales de un recurso.
  - Gestión de alarmas proporcionadas por recursos fuera de los límites establecidos.
- Manejo de herramientas de monitorización de sistemas informáticos:
  - Instalación y administración de herramientas de monitorización.
  - Conocimiento de estándares para la monitorización de sistemas informáticos.
- Indicadores de rendimiento de sistemas informáticos:
  - Criterios para establecer los indicadores para la monitorización de los sistemas informáticos.
  - Identificación de los objetos para los cuales es necesario obtener indicadores.
  - Recolección y análisis de los datos aportados por los indicadores.
  - Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado.

***2. Administración de los dispositivos de almacenamiento del sistema informático siguiendo las directivas de la organización.***

- Dispositivos de almacenamiento:
  - Tipos de dispositivos de almacenamiento más frecuentes.
  - Sistemas de archivos. Características.
  - Estructura general de almacenamiento.
  - Herramientas para la gestión de dispositivos de almacenamiento.

***3. Gestión de las tareas de usuarios, garantizando los accesos al sistema y la disponibilidad de los recursos.***

- Selección del sistema de registro en función de las especificaciones de la organización:
  - Determinación del nivel de registros necesarios.
  - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros.
  - Asignación de responsabilidades para la gestión del registro.
- Gestión de usuarios:
  - Análisis de los requerimientos de acceso al sistema.

  - Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos.
  - Perfiles de acceso en relación con los roles fundamentales del personal de la organización.
  - Limitaciones de uso de recursos como sistemas de almacenamiento o conexiones de red.
- Manejo de herramientas de administración de usuarios y gestión de permisos:
  - Herramientas de directorio activo y servidores LDAP.
  - Herramientas de sistemas de gestión de identidades y autorizaciones (IAM).
  - Herramientas de sistemas de punto único de autenticación (SSO).
- Aspectos generales de seguridad:
  - Métodos de acceso al sistema.
  - Autenticación, autorización y registro.
  - Manejo de herramientas.

***4. Gestión de los servicios de red asegurando la comunicación entre sistemas.***

- Servicios de comunicaciones:
  - Dispositivos de comunicaciones.
  - Protocolos de comunicaciones.
  - Servicios de comunicaciones.
  - Rendimiento de los servicios de comunicaciones.
- Manejo de herramientas de administración de monitorización:
  - Procesos de monitorización y respuesta.
  - Herramientas de análisis de redes tipo Sniffer.
  - Herramientas de sistemas tipo monitorización de redes.
  - Gestión de registros de elementos de red y filtrado.
- Interpretación de informes e incidencias.

***Saberes comunes que dan soporte a las actividades profesionales de esta unidad de competencia.***

- Interpretación de documentación técnica, en su caso, en lengua extranjera.
- Elaboración documentación técnica.
- Estructura y administración de diferentes Sistemas Operativos:
  - Conceptos básicos.
  - Herramientas administrativas.
- Auditorías de calidad y seguridad de las organizaciones en general.

## 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:

1. En relación con otros trabajadores o profesionales deberá:

   1.1 Tratarlos con cortesía, respeto y discreción.
   1.2 Liderar y coordinar equipos de trabajo.
   1.3 Habilidades en la resolución de conflictos.
   1.4 Transmitir indicaciones claras e inequívocas al personal bajo su responsabilidad.

1.5 Comunicarse eficazmente con las personas del equipo adecuadas en cada momento, respetando los canales establecidos en la organización.
1.6 Participar y colaborar activamente en el equipo de trabajo.
1.7 Proponer alternativas con el objetivo de mejorar resultados.

2. En relación con clientes / usuarios deberá:

2.1 Tratar al cliente con cortesía, respeto y discreción.
2.2 Cumplir las normas de comportamiento profesional.
2.3 Demostrar un buen hacer profesional.
2.4 Adaptarse al contexto y las necesidades de los usuarios.
2.5 Finalizar el trabajo en los plazos establecidos.
2.6 Comunicarse con los clientes.

3. En relación a la obra, puesto de trabajo y otros aspectos deberá:

3.1 Cuidar el aspecto y aseo personal como profesional.
3.2 Responsabilizarse del trabajo que desarrolla, cumpliendo los objetivos y plazos establecidos.
3.3 Adaptarse a la organización integrándose al sistema de relaciones técnico profesionales.
3.4 Tener iniciativa para promover proyectos.
3.5 Tener iniciativa para encontrar información y relacionarse con proveedores.
3.6 Tener una actitud consecuente con el mundo tecnológico. Limpieza, reciclaje de residuos, ahorro y eficiencia energética.
3.7 Cuidar los equipos de trabajo y utilizar con economía los materiales.
3.8 Respetar las instrucciones y normas internas de la empresa.
3.9 Preocuparse por cumplir siempre las medidas de seguridad en las actividades laborales.

## 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 UC0490_3: Gestionar servicios en el sistema informático, 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 gestionar un sistema informático,compuesto de un mínimo de dos servidores, una cabina de almacenamiento, un encaminador, un conmutador así como dos equipos de usuario a partir de las especificaciones técnicas de la organización, así como del plan de explotación. Esta situación comprenderá al menos las siguientes actividades:

1. Gestionar el consumo de recursos en el sistema informático.
2. Manejar herramientas para la gestión de dispositivos de almacenamiento.
3. Gestionar los usuarios.
4. Configurar y administrar los servicios de red.
5. Manejar herramientas de monitorización del sistema informático.

***Condiciones adicionales:***

- Se dispondrá de equipamientos, software específico y ayudas técnicas requeridas por la situación profesional de evaluación.
- Se asignará un tiempo total para que el candidato o la candidata demuestre su competencia en condiciones de estrés profesional.
- Se valorará la competencia de respuesta a las contingencias, generando alguna incidencia durante el proceso.

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

Con el objeto de optimizar la validez y fiabilidad del resultado de la evaluación, esta Guía incluye unos criterios de evaluación integrados y, por tanto, reducidos en número. 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 se especifican en el cuadro siguiente:

| *Criterios de mérito* | *Indicadores, escalas y umbrales de desempeño competente* |
|---|---|
| *Gestión del consumo de recursos.* | - Monitorización de los recursos.<br>- Utilización de técnicas para la gestión del consumo de recursos.<br>- Límites de los recursos establecidos adecuadamente.<br>- Gestión de alarmas proporcionadas por los recursos que están fuera de los límites establecidos.<br><br>*El umbral de desempeño competente está explicitado en la Escala A.* |
| *Manejo de herramientas de monitorización.* | - Uso de las herramientas de monitorización del sistema operativo.<br>- Instalación de herramientas de monitorización externas.<br>- Destreza en la configuración y manejo de las herramientas de monitorización.<br><br>*El umbral de desempeño competente requiere el cumplimiento total de este criterio de mérito* |
| *Manejo de herramientas para la gestión de dispositivos de almacenamiento.* | - Uso de las herramientas de gestión de dispositivos de almacenamiento del sistema operativo.<br>- Instalación de herramientas de gestión de dispositivos de almacenamiento externas.<br>- Destreza en la configuración y manejo de las herramientas de gestión de dispositivos de almacenamiento.<br><br>*El umbral de desempeño competente requiere el cumplimiento total de este criterio de mérito.* |
| *Gestión de los usuarios.* | - Análisis de los requerimientos de acceso al sistema.<br>- Perfiles y roles en el personal de la organización establecidos.<br>- Limitación del acceso a los recursos como son los sistemas de almacenamiento o las conexiones de red.<br>- Manejo de herramientas de administración de usuarios y gestión de permisos.<br><br>*El umbral de desempeño competente está explicitado en la Escala B.* |
| *Configuración y administración de los servicios de red.* | - Gestión de los principales protocolos y dispositivos de comunicaciones.<br>- Manejo de herramientas analizadoras de red (Sniffer).<br>- Manejo de herramientas de gestión centralizada de red del tipo monitorización de red.<br><br>*El umbral de desempeño competente está explicitado en la Escala C.* |

**Escala A**

| | |
|---|---|
| 5 | *La gestión del consumo de recursos en el sistema informático se ha realizado correctamente. Se ha monitorizado los recursos del sistema utilizando las mejores técnicas para detectar el consumo de estos. Se ha establecido unos límites correctos en el consumo de los recursos y se gestionan de manera eficaz las alarmas que proporcionan cuando se superan estos límites.* |
| **4** | *La gestión del consumo de recursos en el sistema informático se ha realizado correctamente. Se ha monitorizado los recursos del sistema utilizando técnicas para detectar el consumo de estos. Se ha establecido unos límites correctos en el consumo de los recursos y se gestionan de manera aceptable las alarmas que proporcionan cuando superan estos límites* |
| 3 | *La gestión del consumo de recursos en el sistema informático se ha realizado correctamente. Se ha monitorizado los recursos del sistema utilizando técnicas para detectar el consumo de estos. No se ha establecido unos límites correctos en el consumo de los recursos.* |
| 2 | *La gestión del consumo de recursos en el sistema informático no se ha realizado correctamente. No se han utilizando técnicas para detectar el consumo de estos. No se ha establecido unos límites correctos en el consumo de los recursos.* |
| 1 | *No es capaz de manejar el sistema informático. No se gestionan los recursos.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala B**

| | |
|---|---|
| 5 | *La gestión de los usuarios se ha realizado correctamente. Se ha analizado previamente los requerimientos de acceso al sistema y se han establecido unos perfiles y roles adecuados al personal de la organización. El acceso a los recursos se la limitado de manera adecuada. Se ha instalado y configurado herramientas del sistema operativo y también externas de administración de usuarios, facilitando así la gestión de los permisos.* |
| **4** | *La gestión de los usuarios se ha realizado correctamente. Se ha analizado previamente los requerimientos de acceso al sistema y se han establecido unos perfiles y roles adecuados al personal de la organización. El acceso a los recursos se la limitado de manera adecuada. Se ha instalado y configurado herramientas del sistema operativo de administración de usuarios, facilitando así la gestión de los permisos.* |
| 3 | *La gestión de los usuarios se ha realizado correctamente. Se ha analizado previamente los requerimientos de acceso al sistema y se han establecido unos perfiles y roles adecuados al personal de la organización. El acceso a los recursos se la limitado de manera incorrecta. No se ha instalado y configurado herramientas del sistema operativo de administración de usuarios.* |
| 2 | *La gestión de los usuarios se ha realizado correctamente. No se ha analizado previamente los requerimientos de acceso al sistema, aunque se han establecido unos perfiles y roles adecuados al personal de la organización. El acceso a los recursos se la limitado de manera incorrecta. No se ha instalado y configurado herramientas del sistema operativo de administración de usuarios.* |
| 1 | *La gestión de los usuarios no se ha realizado correctamente. No se ha analizado previamente los requerimientos de acceso al sistema y no se han establecido unos perfiles y roles adecuados al personal de la organización. El acceso a los recursos se la limitado de manera incorrecta. No se ha instalado y configurado herramientas del sistema operativo de administración de usuarios.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 4 de la escala.

**Escala C**

| | |
|---|---|
| 3 | *La configuración y administración de los servicios de red se ha realizado correctamente. Se ha gestionado los principales dispositivos y protocolos de red. Se ha utilizado correctamente herramientas de tipo analizador de red (Sniffer) para monitorizar la red. Se ha utilizado de manera adecuada herramientas de gestión centralizada tipo monitorización de red.* |
| **2** | *La configuración y administración de los servicios de red se ha realizado correctamente. Se ha gestionado los principales dispositivos y protocolos de red. Se ha utilizado correctamente herramientas de tipo analizador de red (Sniffer) para monitorizar la red. Se ha utilizado ocasionalmente herramientas de gestión centralizada tipo monitorización de red.* |
| 1 | *La configuración y administración de los servicios de red no se ha realizado correctamente. No se ha gestionado los principales dispositivos y protocolos de red. No se ha utilizado correctamente herramientas de tipo analizador de red (Sniffer) para monitorizar la red. No se ha utilizado de herramientas de gestión centralizada tipo monitorización de red.* |

Nota: el umbral de desempeño competente corresponde a la descripción establecida en el número 2 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.

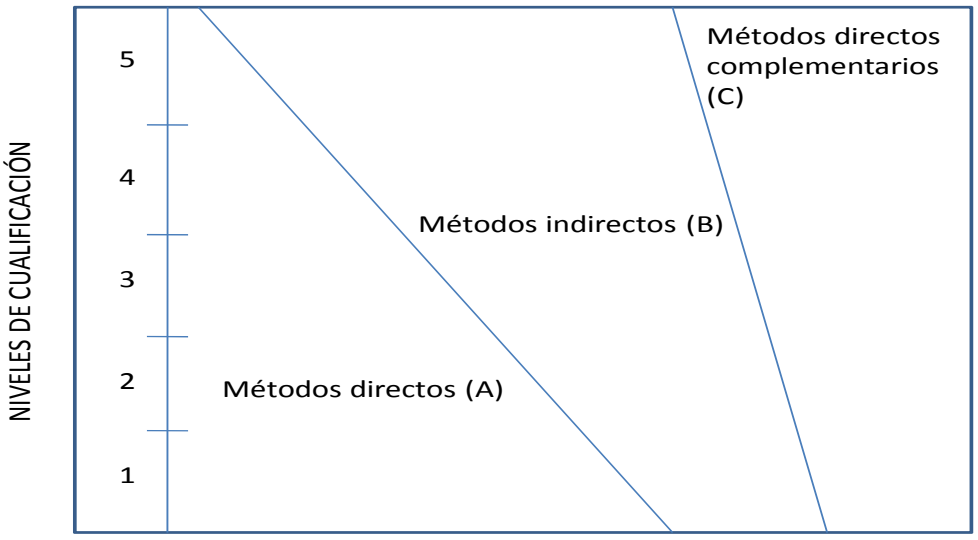
### 2.1. Métodos de evaluación y criterios generales de elección

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 un candidato de bajo nivel cultural al que se le

aprecien dificultades de expresión escrita. 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 no formal y no tenga experiencia en la gestión de servicios en el sistema informático, 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/a 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.

g) En función del entorno de evaluación disponible para el desarrollo de la SPE y de la experiencia aportada por la persona candidata, la comisión de evaluación podrá elegir un entorno propietario de uso común u otro de código abierto de uso extendido.

# GLOSARIO DE TÉRMINOS UTILIZADOS EN SEGURIDAD INFORMÁTICA

**Amenaza:** Posible causa de un incidente no deseado, lo cual puede resultar en un daño a un sistema, persona u organización.

**Análisis de riesgos:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

**Análisis de vulnerabilidades:** Recopilar, analizar y sistematizar, de una forma estructurada y lógica, información sobre la vulnerabilidad de la información.

**Analizador de protocolos:** Herramienta software que nos permite analizar el tráfico, a nivel de protocolos, que discurre por una red informática.

**Appliance:** Dispositivo hardware independiente con software integrado diseñado para proporcionar un recurso específico.

**Autoridad de certificación (CA):** Entidad de confianza, responsable de emitir y revocar certificados digitales, utilizados en la firma electrónica, para lo cual se emplea en la criptografía de clave pública.

**Certificado digital:** Documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y una clave pública.

**Confidencialidad:** Propiedad de que una información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

**Demilitarized Zone (DMZ) [Zona Desmilitarizada]:** Subred, dentro de una red de área local, que permite proporcionar servicios a una red externa (normalmente internet) aislando al resto de equipos de la red local de los problemas de seguridad provenientes de la red externa.

**Domain Name System (DNS) [Sistema de Nombres de Dominio]:** Sistema de nomenclatura para sistemas informáticos que permite asociar nombres de dominio a direcciones IP.

**Dynamic Host Configuration Protocol (DHCP) [Protocolo de configuración dinámica de host]:** Protocolo de red que permite a los host obtener de forma automática los parámetros de configuración para conectarse a una red.

**Firewall [Cortafuegos]:** Dispositivo o software encargado de proteger una red permitiendo los accesos autorizados y limitando los no autorizados. Además pueden cifrar, descifrar y limitar el tráfico siguiendo un conjunto de reglas configuradas.

**Firma digital:** Esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico.

**Gateway [Pasarela]:** Dispositivo que permite la interconexión de redes con diferentes arquitecturas.

**Infraestructura de clave pública (PKI):** Conjunto de protocolos, servicios y estándares para las comunicaciones seguras mediante el uso de certificados digitales y firmas digitales.

**Internet Protocol Security (IPSec)[Seguridad del Protocolo Internet]:** Protocolo que permite la creación de VPNs asegurando las comunicaciones sobre el protocolo IP.

**Malicious software (Malware) [Software malicioso]:** Software que se infiltra en un sistema informático con el objeto de obtener información, controlar los equipos o dañar el sistema.

**Network Address Translation (NAT) [Traducción de Dirección de Red]:** Método utilizado por los routers en el que se cambia la dirección IP en la cabecera de los paquetes IP comúnmente utilizado para permitir el uso de direcciones privadas para el acceso a internet.

**Network intrusion detection system (NIDS) [Sistema de detección de intrusos en una Red]:** Sistema de detección que permite localizar anomalías como ataques de denegación de servicio o intentos de acceso indebido analizando el tráfico de red en tiempo real.

**Objetivo de punto de recuperación (RPO):** Período máximo que se permite en una organización de posible pérdida de datos. Determina la frecuencia de realización de copias de seguridad.

**Objetivo de tiempo de recuperación (RTO):** Tiempo que la organización puede permitirse tener caído un determinado servicio, antes de que esta caída le ocasione consecuencias inaceptables, relacionadas con una ruptura en la continuidad del negocio.

**Open system interconnection (OSI) [Interconexión de sistemas abiertos]:** Modelo de arquitectura utilizado como referencia para los sistemas de comunicación.

**Red Privada Virtual (VPN):** Red privada de comunicaciones, implementada sobre una infraestructura pública.

**Secure Sockets Layer (SSL) [Capa de conexión segura]:** Protocolo que proporciona conexiones seguras a través de una red.

**Seguridad de Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

**Sistema de Detección de Intrusos (IDS):** Programa usado para detectar accesos no autorizados a un ordenador o a una red.

**Sistema de Prevención de Intrusos (IPS):** Dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas informáticos de ataques y abusos.

**Virtual Private Network (VPN) [Red privada Virtual]:** Tecnología que permite estender una red de área local através de una red pública garantizando la seguridad.

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una fuente de riesgo. Debilidad de software, hardware o servicio en línea que puede ser explotada por una amenaza.