GUÍA DE EVIDENCIAS DE LA UNIDAD DE COMPETENCIA

"UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico"

CUALIFICACIÓN PROFESIONAL: OPERACIONES DE SEGURIDAD EN SISTEMAS INFORMÁTICOS

Código: IFC300_2 NIVEL: 2

1. ESPECIFICACIONES DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA.

Dado que la evaluación de la competencia profesional se basa en la recopilación de pruebas o evidencias de competencia generadas por cada persona candidata, el referente a considerar para la valoración de estas evidencias de competencia (siempre que éstas no se obtengan por observación del desempeño en el puesto de trabajo) es el indicado en los apartados 1.1 y 1.2 de esta GEC, referente que explicita la competencia recogida en las realizaciones profesionales y criterios de realización de la UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico.

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

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

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

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

a) Especificaciones relacionadas con el “saber hacer”.

La persona candidata demostrará el dominio práctico relacionado con las actividades profesionales que intervienen en configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico, y que se indican a continuación:

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

1. Instalar sistemas de cortafuegos, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la

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

1.1 Las zonas de seguridad se asocian a los interfaces de red del cortafuegos, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad y el resto de zonas.
1.2 Las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes se aplican sobre las zonas de seguridad, configurando acciones tales como: - Permitir los flujos de conexiones iniciados desde redes de mayor seguridad hacia redes de menor seguridad. - Establecer los flujos de conexiones hacia redes con vulnerabilidades intencionadas "honeynets". - Bloquear los flujos de conexiones iniciados desde redes de menor seguridad a redes de mayor seguridad que no estén explícitamente permitidas. - Aplicar el filtrado en el cortafuegos entre las zonas de seguridad, estableciendo las direcciones IP y puertos permitidos y no permitidos.
1.3 La relación de políticas de filtrado de tráfico se aplican sobre los cortafuegos, estableciendo las reglas y firmas de protección específicas frente a ataques conocidos entre las zonas, tales como "Port enumeration", "TCP Split handshake", "TCP SYN flood", entre otros, para protegerlas frente a ellos.
1.4 Los eventos de notificación y alarmas se configuran en el cortafuegos, estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas y/o envío de paquetes de notificación mediante "syslog", entre otros.
1.5 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.
1.6 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

2. Instalar sistemas de detección y prevención de intrusiones (IDS/IPS), configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

2.1 Los cables de red de entrada y salida de datos se conectan a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas, para posibilitar la inspección del tráfico de red.
2.2 Las zonas de seguridad se asocian a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas.

2.3 Los sistemas señuelo ("honeypot") se configuran, estableciendo aplicaciones y servicios trampa atractivos ante ataques, recopilando información sobre métodos y comportamientos, para la protección de la red de producción real.
2.4 Las firmas de detección de ataques se configuran, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.
2.5 Las firmas de detección de ataques del sistema IDS/IPS se actualizan periódicamente, instalando la versión más reciente.
2.6 Las reglas de detección de ataques por comportamiento se configuran, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.
2.7 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.
2.8 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

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

3.1 Las políticas de acceso a la navegación se configuran, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes.
3.2 Las políticas de acceso de categorías de contenidos web se configuran, estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web.
3.3 Los perfiles de acceso de navegación se configuran para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar.
3.4 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.

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

4. Instalar sistemas de gestión de eventos de seguridad ("Security Information and Event Management", SIEM), configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

4.1 La configuración del sistema operativo se verifica para el funcionamiento de los SIEM, validando los parámetros especificados según indique la documentación técnica.
4.2 Los programas de utilidad incluidos en el sistema operativo, se configuran para el uso de los SIEM, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.
4.3 Los sistemas de recolección de información se configuran en el SIEM, especificando el tipo de fuente de información, tal como sistema de protección contra el "malware", cortafuegos, sistemas de detección de intrusión, "honeypot", entre otros, para su registro en la herramienta.
4.4 Las reglas de "parseado" y normalización de eventos para cada tipo de fuente se configuran, de acuerdo con las especificaciones técnicas específicas del fabricante para cada fuente, configurando campos tales como tipo de evento, dirección IP, usuario, entre otros.
4.5 Las reglas de agregado y correlación para cada caso de uso se configuran, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM.
4.6 Las reglas de generación de alertas para cada caso de uso se configuran, asignando parámetros tales como severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros, para la posterior notificación y tratamiento de la alerta.
4.7 Los eventos de notificación de alertas se configuran en el SIEM, estableciendo parámetros para cada tipo de alerta y severidad, tales como correos de notificación frente a apertura de tiques en sistemas de gestión de la demanda u otros medios o sistemas válidos, para la notificación automatizada de eventos.
4.8 La instalación se verifica, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.
4.9 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

5. ***Configurar "software" de base y aplicaciones de sistemas informáticos para la protección del correo electrónico, verificando su funcionalidad y comprobando la seguridad siguiendo especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del sistema.***

    5.1 La configuración del sistema operativo se verifica para el funcionamiento de la protección del correo electrónico, comprobando los parámetros específicos que se indique en la documentación técnica del producto.
    5.2 Los programas de utilidad disponibles en el sistema operativo se instalan, verificando que son los mínimos que se necesitan para las funciones requeridas, configurándolos para su uso con los parámetros que se indiquen en la documentación o instrucciones de configuración.
    5.3 Los usuarios imprescindibles para el funcionamiento del sistema se crean, configurando el mínimo conjunto de privilegios para cada uno, de acuerdo a las especificaciones técnicas.
    5.4 Los sistemas de encriptado de comunicaciones y correo electrónico se instalan o, en su caso, se activan, configurando claves o certificados para garantizar la privacidad de las transmisiones.
    5.5 La instalación se verifica, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.
    5.6 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

6. ***Instalar sistemas perimetrales de filtrado de correo electrónico, configurando los parámetros y acciones relacionados con su seguridad, según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.***

    6.1 Los sistemas de consulta de reputación de dominios y las acciones de filtrado de correo se configuran, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido.
    6.2 La información detallada que se requiere para la confección de los registros DNS tal como: - Relación de dominios desde los que se enviara el correo electrónico. - Direcciones IP públicas de los sistemas de correo electrónico con flujo saliente. - Configuración de la política SPF ("Sender Policy Framework"). - Relación de dominios de correo electrónico, y clave pública DKIM ("Domainkey Identified Mail") asociada. - Publicación de política del dominio en entradas DNS de

DMARC ("Domain-based Message Authentication, Reporting and Conformance"). Se proporciona al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable.

6.3 Los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado se comprueban, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas.

6.4 La relación de dominios, "emails" y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad se definen, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.

6.5 Los filtros de análisis semántico para la detección de contenido no deseado se definen sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.

6.6 El sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos se define, configurando, entre otros, el servidor y el "email" de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente.

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

7. Instalar sistemas perimetrales de prevención de fuga de información en el correo electrónico, configurándolos según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.

7.1 La relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico se aplican, proporcionando para cada tipo de fichero o conjunto de información, el veredicto de bloquear, poner en cuarentena o notificar una violación de la política al usuario.

7.2 Los usuarios encargados de los análisis de investigación de los casos se configuran, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos.

7.3 Los medios y sistemas de notificación de violación de las políticas de fuga de información se configuran en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas.

7.4 La instalación se verifica, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.
7.5 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

b) Especificaciones relacionadas con el "saber".

La persona candidata, en su caso, deberá demostrar que posee los conocimientos técnicos (conceptos y procedimientos) que dan soporte a las actividades profesionales implicadas en las realizaciones profesionales de la **UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Instalación de un sistema de cortafuegos

- Zonas de seguridad en redes: zona de menor seguridad, zona de mayor seguridad, zona desmilitarizada y el resto de zonas. Asociación a interfaces de red.
- Flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad. Políticas de seguridad. Acciones de bloqueo.
- Redes con vulnerabilidades intencionadas "honeynets". Establecimiento de flujos de conexión.
- Configuración del filtrado entre zonas en cortafuegos.
- Configuración de filtrado de tráfico entre las zonas de seguridad. Parametrización de reglas y firmas de protección específicas frente a ataques conocidos entre las zonas, tales como "Port enumeration", "TCP Split handshake", "TCP SYN flood", entre otros.
- Configuración de eventos de notificación y alarmas en un cortafuegos.

2. Instalación de sistemas de detección y prevención de intrusiones (IDS/IPS)

- Conexión de cables de entrada y salida a los interfaces de un IDS/IPS según zonas de seguridad.
- Sistemas señuelo ("Honeypot").
- Configuración de firmas de detección de ataques en el sistema IDS/IPS. Reglas y acciones. Periodicidad de actualización de firmas.
- Detección de ataques por comportamiento. Reglas y acciones a realizar.

3. Instalación de sistemas de filtrado de navegación

- Configuración del sistema de filtrado. Redes internas y permisos de navegación. Condiciones.
- Políticas de acceso de categorías de contenidos web en un sistema de filtrado. Cuota de acceso.

- Clasificación de perfiles de acceso de navegación. Configuración en el sistema de usuarios y nodos de comunicación según políticas de acceso de navegación.
- "Proxies" transparentes.

4. Instalación de sistemas de gestión de eventos de seguridad (SIEM)

- Configuración de sistemas operativos para el funcionamiento de un SIEM.
- Configuración de programas de utilidad incluidos en el sistema operativo para el uso de los SIEM.
- Fuentes de información a registrar en el SIEM: sistema de protección contra el "malware", cortafuegos, sistemas de detección de intrusión, entre otros. Reglas de "parseado" y normalización de eventos para cada tipo de fuente. Configuración de campos tales como tipo de evento, dirección IP, usuario, entre otros.
- Reglas de agregado y correlación en el sistema de detección de alertas de un SIEM. Parámetros: ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros.
- Reglas de generación de alertas para cada caso de uso en el sistema de detección de alertas de un SIEM. Parámetros: severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros.
- Eventos de notificación de alertas en el SIEM. Notificación automatizada de eventos.

5. Configuración del "software" de base y aplicaciones para la protección del correo electrónico

- Verificación de la configuración de sistemas operativos.
- Utilidades disponibles en un sistema operativo. Instalación/desinstalación y configuración según criterios de seguridad.
- Usuarios. Perfiles y privilegios. Principios de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know").
- Encriptado de comunicaciones y correo electrónico. Certificados. Encriptado simétrico y asimétrico.
- Pruebas del sistema. Análisis del rendimiento, pruebas funcionales y pruebas de seguridad.

6. Sistemas perimetrales de filtrado de correo electrónico

- Sistemas de consulta de reputación de dominios.
- Sistema de filtrado de correo "antispam". Acciones a tomar por el sistema de filtrado.
- Confección de registros DNS. Información y parámetros relacionados: relación de dominios desde los que se enviara el correo electrónico, direcciones IP públicas de los sistemas de correo electrónico con flujo saliente, configuración del veredicto SPF ("Sender Policy Framework"), relación de dominios de correo electrónico, y clave pública DKIM ("Domainkey Identified Mail"), publicación de política del dominio en entradas DNS de DMARC ("Domain-based Message Authentication, Reporting and Conformance").
- Determinación de correo sospechoso y no deseado. Configuración de umbrales de valoración.

- Sistemas de protección de correo electrónico a relación de dominios, "emails" y ficheros adjuntos. Configuración del tratamiento en relación a la seguridad. Asignación de acciones.
- Filtros de análisis semántico para la detección de contenido no deseado. Definición de acciones.
- Sistemas de notificación de eventos y alertas frente a correos potencialmente peligrosos. Configuración de servidor y correo de notificación.

7. Sistemas perimetrales de prevención de fuga de información en el correo electrónico

- Políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico. Clasificación de contenido y acciones: bloqueo, puesta en cuarentena y/o generación de notificaciones de violación de la política.
- Usuarios encargados de los análisis de investigación de los casos. Configuración de nivel de acceso y potestad de liberar, eliminar o retener los correos electrónicos.
- Medios y sistemas de notificación de violación de las políticas de fuga de información.
- Tipos de prueba de la funcionalidad del sistema: pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad.

c) Especificaciones relacionadas con el "saber estar".

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

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

1.2. Situaciones profesionales de evaluación y criterios de evaluación.

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

Así mismo, la situación profesional de evaluación se sustenta en actividades profesionales que permiten inferir competencia profesional

respecto a la práctica totalidad de realizaciones profesionales de la Unidad de Competencia.

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

En el caso de la "UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico", se tiene una situación profesional de evaluación y se concreta en los siguientes términos:

1.2.1. Situación profesional de evaluación.

a) Descripción de la situación profesional de evaluación.

En esta situación profesional, la persona candidata demostrará la competencia requerida para configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico, cumpliendo la normativa relativa a protección medioambiental, planificación de la actividad preventiva y aplicando estándares de calidad. Esta situación comprenderá al menos las siguientes actividades:

1. Instalar sistemas de cortafuegos; sistemas de detección y prevención de intrusiones (IDS/IPS) y sistemas de filtrado de navegación.

2. Instalar sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM); sistemas perimetrales de filtrado de correo electrónico y sistemas perimetrales de prevención de fuga de información en el correo electrónico.

3. Configurar 'software' de base y aplicaciones de sistemas informáticos para la protección del correo electrónico

Condiciones adicionales:

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

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

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

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

Cada criterio de evaluación está formado por un criterio de mérito significativo, así como por los indicadores y escalas de desempeño competente asociados a cada uno de dichos criterios.

En la situación profesional de evaluación, los criterios de evaluación se especifican en el cuadro siguiente:

Criterios de mérito	***Indicadores de desempeño competente***
Destreza en la instalación de sistemas de cortafuegos; de sistemas de detección y prevención de intrusiones (IDS/IPS) y de sistemas de filtrado de navegación.	- Asociación de las zonas de seguridad a los interfaces de red del cortafuegos. - Aplicación de las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad y de la relación de políticas de filtrado de tráfico sobre los cortafuegos. - Configuración de los eventos de notificación y alarmas en el cortafuegos. - Verificación de la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos establecidos. - Conexión de los cables de red de entrada y salida de datos a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas. - Asociación de las zonas de seguridad a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas. - Configuración de los sistemas señuelo ('honeypot'). - Configuración de las firmas de detección de ataques, habilitándolas en el sistema IDS/IPS. - Actualización de las firmas de detección de ataques del sistema IDS/IPS periódicamente, instalando la versión más reciente. - Configuración de las reglas de detección de ataques por comportamiento, habilitándolas en el sistema IDS/IPS. - Configuración de las políticas de acceso a la navegación,

	estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes. - Configuración de las políticas de acceso de categorías de contenidos 'web', estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web. - Configuración de los perfiles de acceso de navegación para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar. *El umbral de desempeño competente está explicitado en la Escala A.*
Precisión en la instalación de sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM); de sistemas perimetrales de filtrado de correo electrónico y de sistemas perimetrales de prevención de fuga de información en el correo electrónico.	- Verificación de la configuración del sistema operativo para el funcionamiento de los SIEM. - Configuración de los programas de utilidad incluidos en el sistema operativo, para el uso de los SIEM. - Configuración de los sistemas de recolección de información en el SIEM, especificando el tipo de fuente de información para su registro en la herramienta. - Configuración de las reglas de 'parseado' y normalización de eventos para cada tipo de fuente. - Configuración de las reglas de agregado y correlación para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM. - Configuración de las reglas de generación de alertas para cada caso de uso. - Configuración de los eventos de notificación de alertas en el SIEM. - Verificación de la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización. - Configuración de los sistemas de consulta de reputación de dominios y las acciones de filtrado de correo, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema

	de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido. - Proporción de la información detallada que se requiere para la confección de los registros DNS al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable. - Comprobación de los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas. - Definición de la relación de dominios, 'emails' y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. - Definición de los filtros de análisis semántico para la detección de contenido no deseado sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. - Definición del sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, configurando, entre otros, el servidor y el 'email' de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente. - Aplicación de la relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico. - Configuración de los usuarios encargados de los análisis de investigación de los casos, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos. - Configuración de los medios y sistemas de notificación de violación de las políticas de fuga de información en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas. *El umbral de desempeño competente está explicitado en la Escala B.*
Eficacia en la configuración del 'software' de base y aplicaciones de	- Verificación de la configuración del sistema operativo para el funcionamiento de la protección del correo

sistemas informáticos para la protección del correo electrónico	electrónico. - Instalación de los programas de utilidad disponibles en el sistema operativo, verificando que son los mínimos que se necesitan para las funciones requeridas. - Creación de los usuarios imprescindibles para el funcionamiento del sistema, configurando el mínimo conjunto de privilegios para cada uno. - Instalación de los sistemas de encriptado de comunicaciones y correo electrónico. - Verificación de la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad. - Confección de la documentación de los procesos realizados, siguiendo los modelos internos establecidos. *El umbral de desempeño competente está explicitado en la Escala C.*
Cumplimiento del tiempo asignado, considerando el que emplearía un o una profesional competente.	
El desempeño competente requiere el cumplimiento, en todos los criterios de mérito, de la normativa aplicable en materia de prevención de riesgos laborales, protección medioambiental	

Escala A

4	*Para instalar sistemas de cortafuegos; sistemas de detección y prevención de intrusiones (IDS/IPS) y sistemas de filtrado de navegación, asocia las zonas de seguridad a los interfaces de red del cortafuegos. Aplica las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad y de la relación de políticas de filtrado de tráfico sobre los cortafuegos. Configura los eventos de notificación y alarmas en el cortafuegos. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos. Conecta los cables de red de entrada y salida de datos a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas. Asocia las zonas de seguridad a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas. Configura los sistemas señuelo ('honeypot'). Configura las firmas de detección de ataques, habilitándolas en el sistema IDS/IPS. Actualiza las firmas de detección de ataques del sistema IDS/IPS periódicamente, instalando la versión más reciente. Configura de las reglas de detección de ataques por comportamiento, habilitándolas en el sistema IDS/IPS. Configura las políticas de acceso a la navegación, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes. Configura las políticas de acceso de categorías de contenidos 'web', estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web. Configura los perfiles de acceso de navegación para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las*

políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar.

3

Para instalar sistemas de cortafuegos; sistemas de detección y prevención de intrusiones (IDS/IPS) y sistemas de filtrado de navegación, asocia las zonas de seguridad a los interfaces de red del cortafuegos. Aplica las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad y de la relación de políticas de filtrado de tráfico sobre los cortafuegos. Configura los eventos de notificación y alarmas en el cortafuegos. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos. Conecta los cables de red de entrada y salida de datos a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas. Asocia las zonas de seguridad a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas. Configura los sistemas señuelo ('honeypot'). Configura las firmas de detección de ataques, habilitándolas en el sistema IDS/IPS. Actualiza las firmas de detección de ataques del sistema IDS/IPS periódicamente, instalando la versión más reciente. Configura de las reglas de detección de ataques por comportamiento, habilitándolas en el sistema IDS/IPS. Configura las políticas de acceso a la navegación, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes. Configura las políticas de acceso de categorías de contenidos 'web', estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web. Configura los perfiles de acceso de navegación para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar, pero comete ciertas irregularidades que no alteran el resultado final.

2

Para instalar sistemas de cortafuegos; sistemas de detección y prevención de intrusiones (IDS/IPS) y sistemas de filtrado de navegación, asocia las zonas de seguridad a los interfaces de red del cortafuegos. Aplica las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad y de la relación de políticas de filtrado de tráfico sobre los cortafuegos. Configura los eventos de notificación y alarmas en el cortafuegos. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos. Conecta los cables de red de entrada y salida de datos a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas. Asocia las zonas de seguridad a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas. Configura los sistemas señuelo ('honeypot'). Configura las firmas de detección de ataques, habilitándolas en el sistema IDS/IPS. Actualiza las firmas de detección de ataques del sistema IDS/IPS periódicamente, instalando la versión más reciente. Configura de las reglas de detección de ataques por comportamiento, habilitándolas en el sistema IDS/IPS. Configura las políticas de acceso a la navegación, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes. Configura las políticas de acceso de categorías de contenidos 'web', estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web. Configura los perfiles de acceso de navegación para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar, pero comete ciertas irregularidades que alteran el resultado final.

1	*No instala sistemas de cortafuegos; ni sistemas de detección y prevención de intrusiones (IDS/IPS) ni sistemas de filtrado de navegación.*

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

Escala B

4	*Para instalar sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM); sistemas perimetrales de filtrado de correo electrónico y sistemas perimetrales de prevención de fuga de información en el correo electrónico, verifica la configuración del sistema operativo para el funcionamiento de los SIEM. Configura los programas de utilidad incluidos en el sistema operativo, para el uso de los SIEM. Configura los sistemas de recolección de información en el SIEM, especificando el tipo de fuente de información para su registro en la herramienta. Configura las reglas de 'parseado' y normalización de eventos para cada tipo de fuente. Configura las reglas de agregado y correlación para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM. Configura las reglas de generación de alertas para cada caso de uso. Configura los eventos de notificación de alertas en el SIEM. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización. Configura los sistemas de consulta de reputación de dominios y las acciones de filtrado de correo, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido. Proporciona la información detallada que se requiere para la confección de los registros DNS al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable. Comprueba los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas. Define la relación de dominios, 'emails' y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. Define los filtros de análisis semántico para la detección de contenido no deseado sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. Define el sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, configurando, entre otros, el servidor y el 'email' de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente. Aplica la relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico. Configura los usuarios encargados de los análisis de investigación de los casos, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos. Configuración de los medios y sistemas de notificación de violación de las políticas de fuga de información en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas.*
3	***Para instalar sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM); sistemas perimetrales de filtrado de correo electrónico y sistemas perimetrales de prevención de fuga de información en el correo electrónico, verifica la***

	configuración del sistema operativo para el funcionamiento de los SIEM. Configura los programas de utilidad incluidos en el sistema operativo, para el uso de los SIEM. Configura los sistemas de recolección de información en el SIEM, especificando el tipo de fuente de información para su registro en la herramienta. Configura las reglas de 'parseado' y normalización de eventos para cada tipo de fuente. Configura las reglas de agregado y correlación para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM. Configura las reglas de generación de alertas para cada caso de uso. Configura los eventos de notificación de alertas en el SIEM. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización. Configura los sistemas de consulta de reputación de dominios y las acciones de filtrado de correo, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido. Proporciona la información detallada que se requiere para la confección de los registros DNS al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable. Comprueba los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas. Define la relación de dominios, 'emails' y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. Define los filtros de análisis semántico para la detección de contenido no deseado sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. Define el sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, configurando, entre otros, el servidor y el 'email' de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente. Aplica la relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico. Configura los usuarios encargados de los análisis de investigación de los casos, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos. Configuración de los medios y sistemas de notificación de violación de las políticas de fuga de información en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas, pero comete ciertas irregularidades que no alteran el resultado final.
2	*Para instalar sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM); sistemas perimetrales de filtrado de correo electrónico y sistemas perimetrales de prevención de fuga de información en el correo electrónico, verifica la configuración del sistema operativo para el funcionamiento de los SIEM. Configura los programas de utilidad incluidos en el sistema operativo, para el uso de los SIEM. Configura los sistemas de recolección de información en el SIEM, especificando el tipo de fuente de información para su registro en la herramienta. Configura las reglas de 'parseado' y normalización de eventos para cada tipo de fuente. Configura las reglas de agregado y correlación para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM. Configura las reglas de generación de alertas para cada caso de uso. Configura los eventos de notificación de alertas en el SIEM. Verifica la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización. Configura los sistemas de consulta*

	de reputación de dominios y las acciones de filtrado de correo, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo electrónico recibido. Proporciona la información detallada que se requiere para la confección de los registros DNS al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable. Comprueba los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas. Define la relación de dominios, 'emails' y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. Define los filtros de análisis semántico para la detección de contenido no deseado sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso. Define el sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, configurando, entre otros, el servidor y el 'email' de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente. Aplica la relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico. Configura los usuarios encargados de los análisis de investigación de los casos, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos. Configuración de los medios y sistemas de notificación de violación de las políticas de fuga de información en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas, pero comete ciertas irregularidades que alteran el resultado final.
1	*No instala sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM); ni sistemas perimetrales de filtrado de correo electrónico y ni sistemas perimetrales de prevención de fuga de información en el correo electrónico.*

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

Escala C

4	*Para configurar 'software' de base y aplicaciones de sistemas informáticos para la protección del correo electrónico, verifica la configuración del sistema operativo para el funcionamiento de la protección del correo electrónico. Instala los programas de utilidad disponibles en el sistema operativo, verificando que son los mínimos que se necesitan para las funciones requeridas. Crea los usuarios imprescindibles para el funcionamiento del sistema, configurando el mínimo conjunto de privilegios para cada uno. Instala los sistemas de encriptado de comunicaciones y correo electrónico. Verifica la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos.*
3	***Para configurar 'software' de base y aplicaciones de sistemas informáticos para la protección del correo electrónico, verifica la configuración del sistema operativo para el funcionamiento de la protección del correo electrónico. Instala los programas de utilidad disponibles en el sistema operativo, verificando que son los mínimos que se necesitan para las funciones requeridas. Crea los usuarios imprescindibles para el funcionamiento del sistema,***

	configurando el mínimo conjunto de privilegios para cada uno. Instala los sistemas de encriptado de comunicaciones y correo electrónico. Verifica la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos, pero comete ciertas irregularidades que no alteran el resultado final.
2	*Para configurar 'software' de base y aplicaciones de sistemas informáticos para la protección del correo electrónico, verifica la configuración del sistema operativo para el funcionamiento de la protección del correo electrónico. Instala los programas de utilidad disponibles en el sistema operativo, verificando que son los mínimos que se necesitan para las funciones requeridas. Crea los usuarios imprescindibles para el funcionamiento del sistema, configurando el mínimo conjunto de privilegios para cada uno. Instala los sistemas de encriptado de comunicaciones y correo electrónico. Verifica la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad. Confecciona la documentación de los procesos realizados, siguiendo los modelos internos establecidos, pero comete ciertas irregularidades que alteran el resultado final.*
1	*No configura el 'software' de base y aplicaciones de sistemas informáticos para la protección del correo electrónico.*

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

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

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

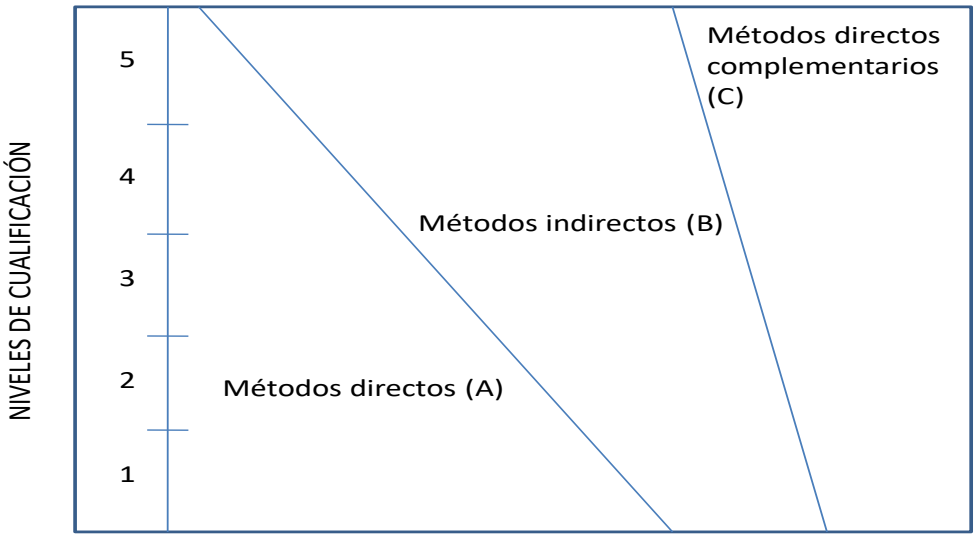
2.1. Métodos de evaluación y criterios generales de elección.

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

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

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

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



Fuente: Leonard Mertens (elaboración propia)

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

La consideración de las características personales de la persona candidata, debe basarse en el principio de equidad. Así, por este principio, debe priorizarse la selección de aquellos métodos de carácter complementario que faciliten la generación de evidencias válidas. En este orden de ideas, nunca debe aplicarse una prueba de conocimientos de carácter escrito a una persona candidata a la que se le aprecien dificultades de expresión escrita, ya sea por razones basadas en el desarrollo de las competencias básicas o factores de integración cultural, entre otras. Una conversación profesional que genere confianza sería el método adecuado.

Por último, indicar que las evidencias de competencia indirectas debidamente contrastadas y valoradas, pueden incidir decisivamente, en cada caso particular, en la elección de otros métodos de evaluación para obtener evidencias de competencia complementarias.

2.2. Orientaciones para las Comisiones de Evaluación y Evaluadores.

a) Cuando la persona candidata justifique sólo formación formal y no tenga experiencia en el proceso de Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico, se le someterá, al menos, a una prueba profesional de evaluación y a una entrevista profesional estructurada sobre la dimensión relacionada con el "saber" y "saber estar" de la competencia profesional.

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

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

d) Si se aplica una prueba práctica, se recomienda establecer un tiempo para su realización, considerando el que emplearía un o una profesional competente, para que el evaluado trabaje en condiciones de estrés profesional.

e) Por la importancia del “saber estar” recogido en la letra c) del apartado 1.1 de esta Guía, en la fase de evaluación se debe comprobar la

competencia de la persona candidata en esta dimensión particular, en los aspectos considerados.

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

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

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

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

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

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