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: GESTIÓN DE SISTEMAS INFORMÁTICOS

Código: IFC152_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 profesionales expresadas en las realizaciones profesionales de la unidad de competencia, y a dos dígitos las reflejadas en los criterios de realización.

1. ***Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.***

1.1. El plan de implantación del sistema informático de la organización se analiza comprobando que incorpora:
   - Información referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones, entre otros.
   - Referencias de posibilidades de utilización de los equipos y restricciones de los mismos.
   - Protecciones contra agresiones de virus y otros elementos no deseados, entre otros.

1.2. Los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema se asignan (provisionan) por medio de las herramientas correspondientes según el Plan de Implantación y el de seguridad del sistema informático.

1.3. La confidencialidad e integridad de la conexión en el acceso a servidores se garantiza según las normas de seguridad de la organización.

1.4. Las políticas de usuario se analizan verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.

1.5. La política de seguridad se transmite a los usuarios, asegurándose de su correcta y completa comprensión.

1.6. Las tareas realizadas se documentan según los procedimientos de la organización.

1.7. Las informaciones afectadas por la normativa aplicable de protección de datos se tratan verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.

2. ***Configurar servidores para protegerlos de accesos no deseados según las necesidades de uso y dentro de las directivas de la organización.***

2.1. El servidor se ubica en la red en una zona protegida y aislada según las normas de seguridad y el plan de implantación de la organización.

2.2. Los servicios que ofrece el servidor se activan y configuran desactivando los innecesarios según la normativa aplicable de seguridad y plan de implantación de la organización.

2.3. Los accesos y permisos a los recursos del servidor por parte de los usuarios se configuran en función del propósito del propio servidor y de

la normativa de seguridad de la organización.

2.4. Los mecanismos de registro de actividad e incidencias del sistema se activan y se habilitan los procedimientos de análisis de dichas informaciones, de forma que permitan sacar conclusiones a posteriori.

2.5. La utilización de los módulos adicionales del servidor se decide en base a sus funcionalidades y riesgos de seguridad, llegando a una solución de compromiso.

2.6. Los mecanismos de autenticación se configuran para que ofrezcan niveles de seguridad e integridad en la conexión de usuarios de acuerdo con la normativa de seguridad de la organización.

2.7. Los roles y privilegios de los usuarios se definen y asignan siguiendo las instrucciones que figuren en las normas de seguridad y el plan de explotación de la organización.

3. Instalar y configurar elementos de seguridad (cortafuegos, equipos trampa, Sistemas de Prevención de Intrusión o Firewalls, entre otros) en equipos y servidores para garantizar la seguridad ante los ataques externos según las necesidades de uso y dentro de las directivas de la organización.

3.1. La topología del cortafuegos se selecciona en función del entorno de implantación.

3.2. Los elementos hardware y software del cortafuegos se eligen teniendo en cuenta factores económicos y de rendimiento.

3.3. Los cortafuegos se instalan y configuran según el nivel definido en la política de seguridad.

3.4. Las reglas de filtrado y los niveles de registro y alarmas se determinan, configuran y administran según las necesidades dictaminadas por la normativa de seguridad de la organización.

3.5. Los cortafuegos se verifican con juegos de pruebas, asegurando que superan las especificaciones de la normativa de seguridad de la organización.

3.6. La instalación y actualización del cortafuegos y los procedimientos de actuación con el mismo se documentan según las especificaciones de la organización.

3.7. Los sistemas de registro se definen y configuran para la revisión y estudio de los posibles ataques, intrusiones y vulnerabilidades.

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. ***Gestión de la seguridad y riesgos.***

- Seguridad: objetivo de la seguridad; amenazas; atacante externo e interno; tipos de ataque; mecanismos de protección.
- Riesgos: proceso de gestión de riesgos; métodos de identificación y análisis de riesgos; reducción del riesgo.

2. ***Seguridad Física***

- Protección del sistema informático.
- Protección de los datos.

3. ***Seguridad lógica del sistema.***

- Sistemas de ficheros.
- Permisos de archivos.
- Listas de control de acceso (ACLs) a ficheros.
- Registros de actividad del sistema.
- Autenticación de usuarios: sistemas de autenticación débiles; sistemas de autenticación fuertes; sistemas de autenticación biométricos.
- Introducción a la Criptografía y Establecimiento de Políticas de Contraseñas.

4. ***Acceso remoto al sistema.***

- Mecanismos del sistema operativo para control de accesos.
- Cortafuegos de servidor: filtrado de paquetes; cortafuegos de nivel de aplicación; registros de actividad del cortafuegos.

a) 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:

- Mantener el área de trabajo con el grado apropiado de orden y limpieza.
- Demostrar creatividad en el desarrollo del trabajo que realiza.
- Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.
- Interpretar y ejecutar instrucciones de trabajo.
- Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.

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. - Comprobación de que los sistemas de protección contra virus y malware y de los sistemas de registro garantizan la seguridad de los sistemas informáticos. - Establecimiento de permisos de acceso a recursos de acuerdo con el plan de seguridad. - Comprobación de la integridad de las conexiones y del acceso confidencial según el plan de seguridad. - Configuración de restricciones en equipos y usuarios siguiendo las especificaciones dadas. - Verificación de los documentos de seguridad y el acceso a la información según la normativa de protección de datos. - Documentación de los procedimientos llevados a cabo siguiendo las indicaciones dadas. *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. - Configuración de enrutamiento y acceso remoto. - Configuración de filtros. - Configuración de servicios y puertos. - Implantación de sistemas de seguridad en el acceso y las conexiones a la VPN. - Ajuste de los niveles de registro. *El umbral de desempeño competente está explicitado en la escala A.*
Configuración de la DMZ.	- Selección del firewall. - Configuración IP de los routers, hosts y servidores. - Inicialización del firewall. - Configuración de las interfaces del firewall. - Configuración de NAT en el firewall. - Documentación del esquema de la DMZ configurada. *El umbral de desempeño competente está explicitado en la escala B.*

Escala A

5	*El servidor VPN de acceso remoto se configura en base a las especificaciones facilitadas proponiendo medidas adicionales de seguridad y protección. 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.

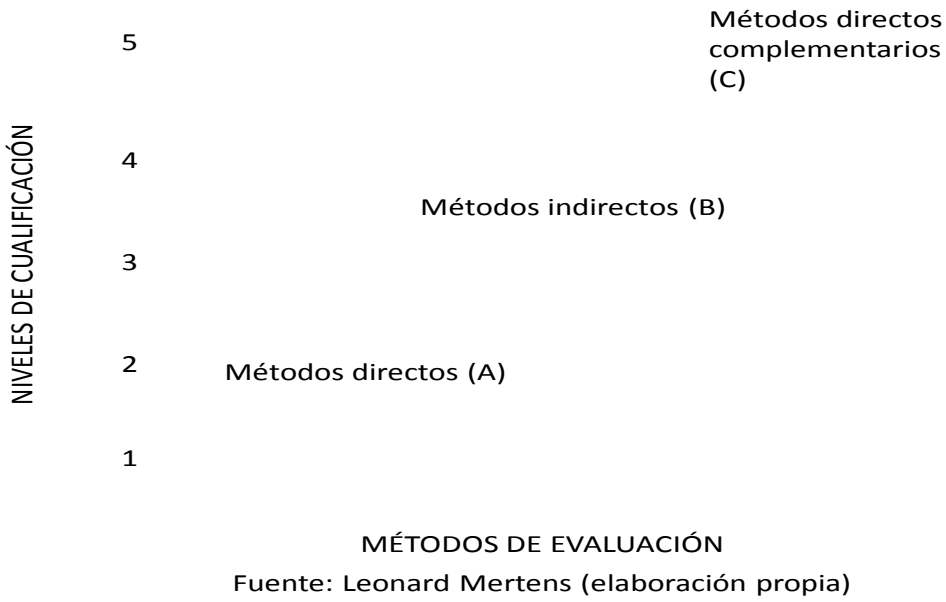
2.1. Métodos de evaluación y criterios generales de elección

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 y en sus competencias más significativas tienen mayor relevancia las destrezas cognitivas y actitudinales. Por las características de estas competencias, la persona candidata ha de movilizar principalmente las destrezas cognitivas aplicándolas de forma competente en 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, en su caso, 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.