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

1. ***Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e***

internacionales.

1.1. Los procedimientos de detección y respuesta de incidentes se localizan, verificando que están documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la organización.

1.2. La modelización de los sistemas se realiza seleccionando los mecanismos de registro a activar, observando las alarmas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso.

1.3. La activación de los mecanismos de registro del sistema se verifica, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

1.4. La planificación de los mecanismos de análisis de registros se verifica, de forma que se garantice la detección de los comportamientos no habituales mediante un sistema de indicadores y métricas.

1.5. La instalación, configuración y actualización de los sistemas de detección de intrusos se verifica en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

1.6. Los procedimientos de restauración del sistema informático se verifican para la recuperación del mismo ante un incidente grave dentro de las necesidades de la organización.

2. Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.

2.1. Las herramientas utilizadas para detectar intrusiones se analizan para determinar que no han sido comprometidas ni afectadas por programas maliciosos.

2.2. Los parámetros de funcionamiento sospechoso se analizan con herramientas específicas según la normativa de seguridad.

2.3. Los componentes software del sistema se verifican periódicamente en lo que respecta a su integridad usando programas específicos.

2.4. El funcionamiento de los dispositivos de protección física se verifica por medio de pruebas según las normas de la organización y/o normativa aplicable de seguridad.

2.5. Los sucesos y signos extraños que pudieran considerarse una alerta se recogen en el informe para su posterior análisis en función de la gravedad de los mismos y la política de la organización.

3. Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el

incidente según los requisitos de servicio y dentro de las directivas de la organización.

3.1. Los procedimientos recogidos en los protocolos de la normativa de seguridad de la organización se activan ante la detección de un incidente de seguridad.

3.2. La información para el análisis forense del sistema vulnerado se recoge una vez aislado el sistema según los procedimientos de las normas de seguridad de la organización y/o normativa aplicable.

3.3. El sistema atacado se analiza mediante herramientas de detección de intrusos según los procedimientos de seguridad de la organización.

3.4. La intrusión se contiene mediante la aplicación de las medidas establecidas en las normas de seguridad de la organización y aquellas extraordinarias necesarias aunque no estén previamente planificadas.

3.5. La documentación del incidente se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido.

3.6. Las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado se planifican a partir de la determinación de los daños causados, cumpliendo los criterios de calidad de servicio y el plan de explotación 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 **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. Gestión de incidentes de seguridad.

- Justificación de la necesidad de gestionar incidentes de seguridad.
- Identificación y caracterización de los datos de funcionamiento del sistema.
- Sistemas de detección de intrusos: sistemas basados en equipo (HIDS); sistemas basados en red (NIDS); sistemas de prevención de intrusiones (IPS); señuelos.

2. Respuesta ante incidentes de seguridad.

- Recolección de información.
- Análisis y correlación de eventos.
- Verificación de la intrusión.
- Organismos de gestión de incidentes: nacionales (IRIS-CERT, esCERT); Internacionales (CERT, FIRST).

3. Análisis forense informático.

- Objetivos del análisis forense.
- Principio de Lockard.
- Recogida de evidencias.
- Principio de indeterminación: evidencias volátiles; evidencias no volátiles; etiquetado de evidencias; cadena de custodia.
- Análisis de evidencias: ficheros y directorios ocultos; información oculta en el sistema de ficheros, Slack-space; recuperación de ficheros borrados; herramientas de análisis forense.
- Análisis de programas maliciosos: desensambladores; entornos de ejecución controlada.

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:

- Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
- Tratar al cliente con cortesía, respeto y discreción.
- Proponerse objetivos retadores que supongan un nivel de rendimiento y eficacia superior al alcanzado previamente.
- Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
- Interpretar y ejecutar instrucciones de trabajo.
- Actuar con rapidez en situaciones problemáticas y no limitarse a esperar.
- Demostrar flexibilidad para entender los cambios.

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.

4. Proponer actuaciones en función de la información recopilada.

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. - Testeo de que los sistemas se modelan de forma que se detecten signos de comportamiento malicioso. - 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. - Comprobación de que los sistemas de detección de intrusos están instalados, actualizados y configurados en función de las especificaciones de seguridad. - Verificación de que los procedimientos de restauración del sistema informático permiten la recuperación del mismo. *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. - Análisis de los parámetros. - Verificación periódica de los componentes software. - Prueba del funcionamiento de los dispositivos de protección física. - Redacción del informe diario de actividad. *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. - Aislamiento del sistema vulnerado y recogida de información. - Análisis el sistema atacado. - Contención de la intrusión. - Documentación del incidente. - Determinación de los daños causados. - Planificación de las acciones a tomar. *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.

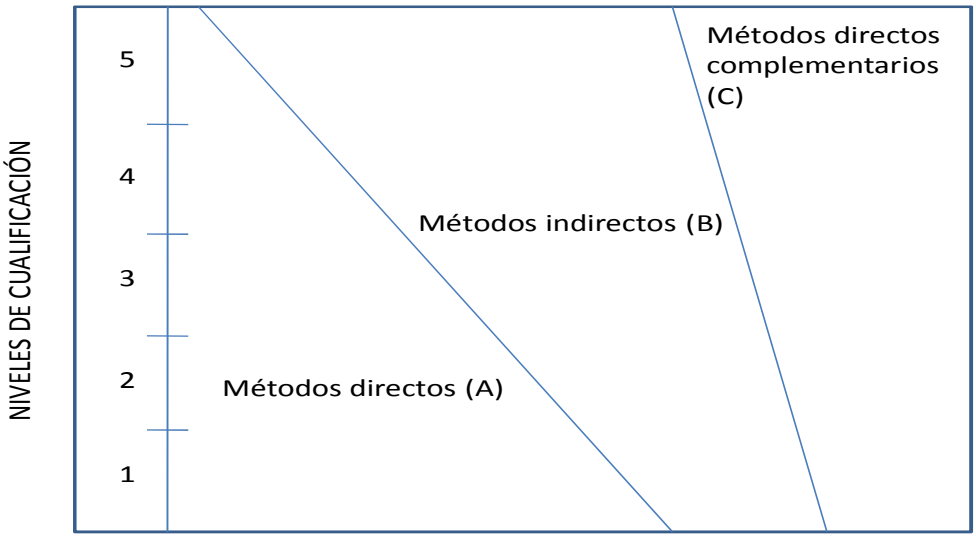
2.1. Métodos de evaluación y criterios generales de elección

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 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) 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.