GUÍA DE EVIDENCIAS DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES

"ECP0488_3: Gestionar incidentes de ciberseguridad"

1. ESPECIFICACIONES DE EVALUACIÓN DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES.

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 los elementos de la competencia (EC) e indicadores de calidad (IC) del ECP0488_3: Gestionar incidentes de ciberseguridad.

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 (Estándar de Competencias Profesionales (ECP) 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 gestionar incidentes de ciberseguridad, y que se indican a continuación:

Nota: A un dígito se indican las actividades profesionales expresadas en los elementos de la competencia del estándar de competencias profesionales, y dos dígitos las reflejadas en los indicadores de calidad.

1. Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos en los sistemas de

una entidad u organización según directrices ante incidentes nacionales e internacionales para los equipos de respuesta.

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 entidad, así como la determinación de la cadena de mando ante la detección de un incidente de seguridad.
1.2 La modelización de los sistemas se efectúa, seleccionando los mecanismos de registro a activar, observando las alertas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso a partir de indicadores de compromiso (IOC: "Indicator of Compromise") facilitados por equipos de respuesta ante incidentes nacionales e internacionales.
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 sospechosos, mediante un sistema de indicadores y métricas.
1.5 La instalación, configuración y actualización de los sistemas de detección de intrusos (IDS) 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, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan") definido por la organización, se verifican, comprobando que pueden ser recuperados en tiempo y forma ante un incidente grave.

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 y de la entidad responsable del sistema.

2.1 Las herramientas utilizadas para detectar intrusiones se comprueba que no han sido comprometidas ni afectadas por programas maliciosos analizándolas, siguiendo las guías y directrices de los equipos de respuesta nacionales e internacionales.
2.2 Los funcionamientos sospechosos se detectan, analizando parámetros de funcionamiento tales como conexiones no autorizadas, mensajes de alerta de los sistemas de detección de intrusiones (IDS: "Intrusion Detection System") o antimalware entre otros, usando herramientas específicas tales como sistemas de Gestión de información y eventos de seguridad (SIEM: "Security information and event management") e IDS, entre otras y estableciendo procedimientos para recoger denuncias de los usuarios acerca de ataques tales como "phising" o

comportamientos anómalos en equipos según directrices de la entidad responsable del sistema.

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 los registros de cada sistema, pruebas específicas, pruebas de estrés, entre otras 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, especificando para cada uno ítems tales como día y hora de la detección, persona que lo comunicó, sistemas implicados y acciones realizadas, entre otros.

2.6 La exposición o filtración de los datos de la organización se verifica periódicamente en función del riesgo que haya determinado la entidad responsable del sistema, consultando fuentes abiertas (OSINT: "Open Source Intelligence") según las características de la organización.

2.7 La información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales se comprueba, verificándola de manera periódica para establecer en su caso los mecanismos de seguridad recomendados en caso de exposición a las amenazas publicadas.

3. Coordinar la respuesta ante incidentes de seguridad entre las áreas implicadas, aplicando el procedimiento recogido en los protocolos de seguridad para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la entidad u organización a proteger.

3.1 Los procedimientos se activan ante la detección de un incidente de seguridad, dando aviso a los responsables de cada subsistema y aplicando los pasos recogidos en los protocolos de la normativa de seguridad de la organización.

3.2 La información para el análisis forense del sistema vulnerado se recoge, una vez aislado el sistema, capturando una imagen tan precisa como sea posible, realizando notas detalladas (incluyendo fechas y horas indicando si se utiliza horario local o UTC), recogiendo la información según el orden de volatilidad (de mayor a menor) entre otras, según los procedimientos de las normas de seguridad de la entidad.

3.3 Las características de la intrusión se determinan, analizando el sistema atacado mediante herramientas de detección de intrusos (IDS), usando las facilidades específicas de cada herramienta y 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 tales como desconexión de equipos y/o segmentos de red o cierre de puertos de comunicaciones, entre otras, y aquellas extraordinarias, que indique la

persona responsable de la seguridad, aunque no estén previamente planificadas.

3.5 La documentación del incidente, así como todas las acciones realizadas y las conclusiones obtenidas se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido, manteniendo de esta forma un registro de lecciones aprendidas ("Lessons Learned").

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 entidad a proteger.

4. Implantar planes de prevención y concienciación en ciberseguridad, para facilitar la previsión de ciberincidentes y su respuesta, en caso de producirse, según los requisitos de servicio y dentro de las directivas de la organización o entidad a proteger.

4.1 Las medidas de ciberseguridad definidas por la organización se difunden, usando medios tales como correo electrónico, intranet corporativa y sesiones específicas, entre otros.

4.2 La normativa de protección del puesto de trabajo se establece, incluyendo ítems tales como escenarios y ejemplos de riesgo y medidas de seguridad, entre otros.

4.3 El plan de concienciación de ciberseguridad dirigido a los empleados se define, elaborando material y cursos o tutoriales para su difusión o impartición y las evaluaciones a realizar y su periodicidad.

4.4 El material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados se difunde o en su caso se imparte de forma periódica, usando los mecanismos disponibles en la entidad, tales como correo electrónico, plataformas web de difusión, aulas y canales de vídeo para cursos, entre otros, capacitando a los empleados ante ciberataques, para detectar los métodos y vectores más habituales.

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 los elementos de la competencia del ECP**0488_3: Gestionar incidentes de ciberseguridad**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Prevención de incidentes de ciberseguridad y preparación de la respuesta

- Documentación de procedimientos de detección y respuesta de incidentes. Roles y responsabilidades de seguridad.
- Mecanismos de registro de sistemas. Activación: indicadores y métricas. Alertas (parámetros de utilización de la red, inventariado de archivos a vigilar, indicadores de compromiso -IOC: "Indicator of Compromise"-).
- Procedimientos de detección de los comportamientos no habituales. Análisis de registros, indicadores y métricas.
- Procedimientos de instalación, configuración y actualización de los sistemas de detección de intrusos (IDS).
- Verificación de los procedimientos de restauración del sistema informático. Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan").
- Normativa aplicable de protección de datos.
- Estándares específicos de la tecnología afectada.

2. Detección de incidentes de ciberseguridad

- Herramientas de detección de intrusiones, (IDS: "Intrusion Detection System"). "Antimalware". Ámbito de aplicación y características.
- Tipología de ataques y programas maliciosos.
- Repositorios de guías y directrices nacionales e internacionales para la detección y prevención de intrusiones.
- Procedimientos de comprobación de integridad en herramientas de detección de intrusiones.
- Herramientas específicas de análisis y detección de parámetros de funcionamiento sospechosos. Sistemas de Gestión de información y eventos de seguridad (SIEM: "Security Information and Event Management").
- Herramientas específicas de verificación de integridad de componentes "software" del sistema.
- Dispositivos de protección física. Mecanismos de verificación: registros del sistema, pruebas específicas, pruebas de estrés, entre otras.
- Procedimientos de detección, análisis y registro de sucesos y signos anormales.
- Fuentes abiertas (OSINT: "Open Source Intelligence").
- Centros de respuesta ante incidentes nacionales y/o internacionales.

3. Respuesta ante incidentes de ciberseguridad

- Aislamiento del sistema Mecanismos de contención de intrusiones
- Orquestación, organización, automatización y respuesta de la seguridad (SOAR)
- Recogida de información
- Análisis forense.

4. Prevención y concienciación en ciberseguridad

- Medios de difusión. Correo electrónico, intranet corporativa, listas de distribución y sesiones específicas, entre otros.
- Protección de puestos de trabajo. Escenarios y ejemplos de riesgo y medidas de seguridad.
- Plan de concienciación de ciberseguridad. Cursos y tutoriales.

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:

- Demostrar un buen hacer profesional.
- 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.
- Respetar los procedimientos y normas internas de la organización.
- 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 del Estándar de Competencias Profesionales implicado.

Así mismo, la situación profesional de evaluación se sustenta en actividades profesionales que permiten inferir competencia profesional respecto a la práctica totalidad de elementos de la competencia del Estándar de Competencias Profesionales.

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 del "ECP0488_3: Gestionar incidentes de ciberseguridad", se tiene una situación profesional de evaluación y se concreta en los siguientes términos:

1.2.1. Situación profesional de evaluación.

a) Descripción de la situación profesional de evaluación.

En esta situación profesional, la persona candidata demostrará la competencia requerida para gestionar incidentes de ciberseguridad, 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. Implantar los procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos.

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

3. Coordinar la respuesta ante incidentes de seguridad entre las áreas implicadas.

4. Implantar planes de prevención y concienciación en ciberseguridad.

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***
Eficacia en la implantación de los procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos.	- Verificación de los procedimientos de detección y respuesta de incidentes. - Realización de la modelización de los sistemas a partir de indicadores de compromiso (IOC: "Indicator of Compromise"). - Verificación de la activación de los mecanismos de registro del sistema.

	- Verificación de la planificación de los mecanismos de análisis de registros para detección de los comportamientos sospechosos. - Verificación de la instalación, configuración y actualización de los sistemas de detección de intrusos (IDS). - Verificación de los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan"). *El umbral de desempeño competente está explicitado en la Escala A*
Eficiencia en la detección de incidentes de seguridad de forma activa y preventiva.	- Comprobación de las herramientas utilizadas para detectar intrusiones. - Detección de funcionamientos sospechosos. - Verificación periódica de la integridad de los componentes "software" del sistema. - Verificación del funcionamiento de los dispositivos de protección física. - Recogida de los sucesos y signos extraños que pudieran considerarse una alerta en el informe. - Verificación periódica de la exposición o filtración de los datos de la organización en función del riesgo. - Comprobación de la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales. *El umbral de desempeño competente está explicitado en la Escala B*
Eficiencia en la coordinación de la respuesta ante incidentes de seguridad entre las áreas implicadas.	- Aviso a los responsables de cada subsistema ante la detección de un incidente de seguridad. - Recogida de la información para el análisis forense del sistema vulnerado. - Determinación de las características de la intrusión se determinan mediante herramientas de detección de intrusos (IDS). - Contención de la intrusión. - Documentación del incidente, así como todas las acciones realizadas y las conclusiones obtenidas. - Planificación de las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado. *El umbral de desempeño competente está explicitado en la Escala C*

Eficacia en la implantación de planes de prevención y concienciación en ciberseguridad.	- Difusión las medidas de ciberseguridad definidas por la organización. - Establecimiento la normativa de protección del puesto de trabajo. - Definición del plan de concienciación de ciberseguridad dirigido a los empleados. - Difusión del material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados. *El umbral de desempeño competente está explicitado en la Escala D*
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 implantar, los procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos, verifica los procedimientos de detección y respuesta de incidentes, realiza la modelización de los sistemas a partir de indicadores de compromiso (IOC: "Indicator of Compromise"), verifica la activación de los mecanismos de registro del sistema, verifica la planificación de los mecanismos de análisis de registros para detección de los comportamientos sospechosos, verifica la instalación, configuración y actualización de los sistemas de detección de intrusos (IDS), verifica los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan").*
3	***Para implantar los procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos, verifica los procedimientos de detección y respuesta de incidentes, realiza la modelización de los sistemas a partir de indicadores de compromiso (IOC: "Indicator of Compromise"), verifica la activación de los mecanismos de registro del sistema, verifica la planificación de los mecanismos de análisis de registros para detección de los comportamientos sospechosos, verifica la instalación, configuración y actualización de los sistemas de detección de intrusos (IDS), verifica los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan"), aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para implantar los procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos, verifica los procedimientos de detección y respuesta de incidentes, realiza la modelización de los sistemas a partir de indicadores de compromiso (IOC: "Indicator of Compromise"), verifica la*

activación de los mecanismos de registro del sistema, verifica la planificación de los mecanismos de análisis de registros para detección de los comportamientos sospechosos, verifica la instalación, configuración y actualización de los sistemas de detección de intrusos (IDS), verifica los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan"), pero comete amplias irregularidades que alteran el resultado final.

1

No implanta los procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos, verifica los procedimientos de detección y respuesta de incidentes, realiza la modelización de los sistemas a partir de indicadores de compromiso (IOC: "Indicator of Compromise"), verifica la activación de los mecanismos de registro del sistema, verifica la planificación de los mecanismos de análisis de registros para detección de los comportamientos sospechosos, verifica la instalación, configuración y actualización de los sistemas de detección de intrusos (IDS), verifica los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan").

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

Escala B

4

Para detectar, incidentes de seguridad de forma activa y preventiva, comprueba las herramientas utilizadas para detectar intrusiones, detecta funcionamientos sospechosos, verifica periódicamente la integridad de los componentes "software" del sistema, verifica el funcionamiento de los dispositivos de protección física, recoge los sucesos y signos extraños que pudieran considerarse una alerta en el informe, verifica periódicamente la exposición o filtración de los datos de la organización en función del riesgo, comprueba la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales.

3

Para detectar incidentes de seguridad de forma activa y preventiva, comprueba las herramientas utilizadas para detectar intrusiones, detecta funcionamientos sospechosos, verifica periódicamente la integridad de los componentes "software" del sistema, verifica el funcionamiento de los dispositivos de protección física, recoge los sucesos y signos extraños que pudieran considerarse una alerta en el informe, verifica periódicamente la exposición o filtración de los datos de la organización en función del riesgo, comprueba la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales, aunque comete ligeras irregularidades que no alteran el resultado final.

2

Para detectar incidentes de seguridad de forma activa y preventiva, comprueba las herramientas utilizadas para detectar intrusiones, detecta funcionamientos sospechosos, verifica periódicamente la integridad de los componentes "software" del sistema, verifica el funcionamiento de los dispositivos de protección física, recoge los sucesos y signos extraños que pudieran considerarse una alerta en el informe, verifica periódicamente la exposición o filtración de los datos de la organización en función del riesgo, comprueba la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales, pero comete amplias irregularidades que alteran el resultado final.

1

	No detecta incidentes de seguridad de forma activa y preventiva, comprueba las herramientas utilizadas para detectar intrusiones, detecta funcionamientos sospechosos, verifica periódicamente la integridad de los componentes "software" del sistema, verifica el funcionamiento de los dispositivos de protección física, recoge los sucesos y signos extraños que pudieran considerarse una alerta en el informe, verifica periódicamente la exposición o filtración de los datos de la organización en función del riesgo, comprueba la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales.

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

Escala C

4	*Para coordinar, la respuesta ante incidentes de seguridad entre las áreas implicadas, avisa a los responsables de cada subsistema ante la detección de un incidente de seguridad, recoge la información para el análisis forense del sistema vulnerado, determina las características de la intrusión se determinan mediante herramientas de detección de intrusos (IDS), contiene la intrusión, documentar el incidente, así como todas las acciones realizadas y las conclusiones obtenidas, planifica las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado.*
3	***Para coordinar la respuesta ante incidentes de seguridad entre las áreas implicadas, avisa a los responsables de cada subsistema ante la detección de un incidente de seguridad, recoge la información para el análisis forense del sistema vulnerado, determina las características de la intrusión se determinan mediante herramientas de detección de intrusos (IDS), contiene la intrusión, documentar el incidente, así como todas las acciones realizadas y las conclusiones obtenidas, planifica las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para coordinar la respuesta ante incidentes de seguridad entre las áreas implicadas, avisa a los responsables de cada subsistema ante la detección de un incidente de seguridad, recoge la información para el análisis forense del sistema vulnerado, determina las características de la intrusión se determinan mediante herramientas de detección de intrusos (IDS), contiene la intrusión, documentar el incidente, así como todas las acciones realizadas y las conclusiones obtenidas, planifica las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado, pero comete amplias irregularidades que alteran el resultado final.*
1	*No coordina la respuesta ante incidentes de seguridad entre las áreas implicadas, avisa a los responsables de cada subsistema ante la detección de un incidente de seguridad, recoge la información para el análisis forense del sistema vulnerado, determina las características de la intrusión se determinan mediante herramientas de detección de intrusos (IDS), contiene la intrusión, documentar el incidente, así como todas las acciones realizadas y las conclusiones obtenidas, planifica las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado.*

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

Escala D

4	*Para implantar, planes de prevención y concienciación en ciberseguridad, difunde las medidas de ciberseguridad definidas por la organización, establecer la normativa de protección del puesto de trabajo, define el plan de concienciación de ciberseguridad dirigido a los empleados, difunde el material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados.*
3	***Para implantar planes de prevención y concienciación en ciberseguridad, difunde las medidas de ciberseguridad definidas por la organización, establecer la normativa de protección del puesto de trabajo, define el plan de concienciación de ciberseguridad dirigido a los empleados, difunde el material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados, aunque comete ligeras irregularidades que no alteran el resultado final.***
2	*Para implantar planes de prevención y concienciación en ciberseguridad, difunde las medidas de ciberseguridad definidas por la organización, establecer la normativa de protección del puesto de trabajo, define el plan de concienciación de ciberseguridad dirigido a los empleados, difunde el material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados, pero comete amplias irregularidades que alteran el resultado final.*
1	*No implanta planes de prevención y concienciación en ciberseguridad, difunde las medidas de ciberseguridad definidas por la organización, establecer la normativa de protección del puesto de trabajo, define el plan de concienciación de ciberseguridad dirigido a los empleados, difunde el material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados.*

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

2. MÉTODOS DE EVALUACIÓN DEL ESTÁNDAR DE COMPETENCIAS PROFESIONALES 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 del estándar de competencias profesionales, 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.

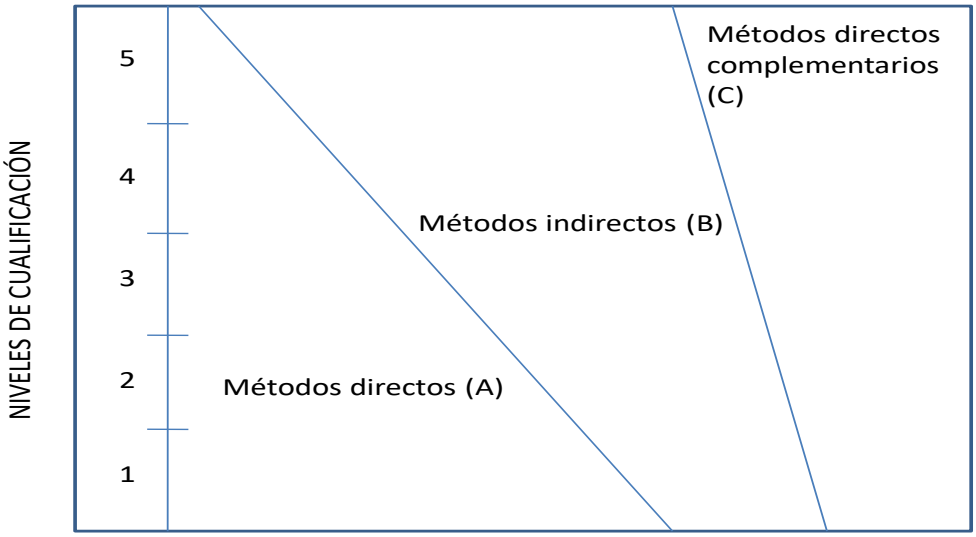
Los métodos que pueden ser empleados en la evaluación de la competencia profesional adquirida por las personas a través de la

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 del ECP. 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 Gestionar incidentes de ciberseguridad, 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 el ECP, 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 los elementos de la competencia 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) 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.