PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP0488_3: Gestionar incidentes de ciberseguridad"

LEA ATENTAMENTE LAS INSTRUCCIONES

Conteste a este cuestionario de **FORMA SINCERA**. La información recogida en él tiene CARÁCTER RESERVADO, al estar protegida por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Su resultado servirá solamente para ayudarle, **ORIENTÁNDOLE** en qué medida posee la competencia profesional del "ECP0488_3: Gestionar incidentes de ciberseguridad".

No se preocupe, con independencia del resultado de esta autoevaluación, Ud. TIENE DERECHO A PARTICIPAR EN EL PROCEDIMIENTO DE EVALUACIÓN, siempre que cumpla los requisitos de la convocatoria.

Nombre y apellidos del trabajador/a: NIF:	Firma:
Nombre y apellidos del asesor/a: NIF:	Firma:

INSTRUCCIONES CUMPLIMENTACIÓN DEL CUESTIONARIO:

Las actividades profesionales aparecen ordenadas en bloques desde el número 1 en adelante. Cada uno de los bloques agrupa una serie de actividades más simples (subactividades) numeradas con 1.1., 1.2.,…, en adelante.

Lea atentamente la actividad profesional con que comienza cada bloque y a continuación las subactividades que agrupa. Marque con una cruz, en los cuadrados disponibles, el indicador de autoevaluación que considere más ajustado a su grado de dominio de cada una de ellas. Dichos indicadores son los siguientes:

1. No sé hacerlo.
2. Lo puedo hacer con ayuda.
3. Lo puedo hacer sin necesitar ayuda.
4. Lo puedo hacer sin necesitar ayuda, e incluso podría formar a otro trabajador o trabajadora.

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Localizar los procedimientos de detección y respuesta de incidentes, 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: Efectuar la modelización de los sistemas, 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: Verificar la activación de los mecanismos de registro del sistema, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.	☐	☐	☐	☐
1.4: Verificar la planificación de los mecanismos de análisis de registros, de forma que se garantice la detección de los comportamientos sospechosos, mediante un sistema de indicadores y métricas.	☐	☐	☐	☐
1.5: Verificar la instalación, configuración y actualización de los sistemas de detección de intrusos (IDS) en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.	☐	☐	☐	☐

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.6: Verificar los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan") definido por la organización, 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Comprobar las herramientas utilizadas para detectar intrusiones 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: Detectar los funcionamientos sospechosos, 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: Verificar los componentes "software" del sistema periódicamente en lo que respecta a su integridad usando programas específicos.	☐	☐	☐	☐
2.4: Verificar el funcionamiento de los dispositivos de protección física 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: Recoger los sucesos y signos extraños que pudieran considerarse una alerta, 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	☐	☐	☐	☐

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
como día y hora de la detección, persona que lo comunicó, sistemas implicados y acciones realizadas, entre otros.				
2.6: Verificar la exposición o filtración de los datos de la organización 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: Comprobar la información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales, 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1: Activar los procedimientos 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: Recoger la información para el análisis forense del sistema vulnerado, 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: Determinar las características de la intrusión, 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: Contener la intrusión 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	☐	☐	☐	☐

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
otras, y aquellas extraordinarias, que indique la persona responsable de la seguridad, aunque no estén previamente planificadas.				
3.5: Realizar la documentación del incidente, así como todas las acciones realizadas y las conclusiones obtenidas para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido, manteniendo de ésta forma un registro de lecciones aprendidas ("Lessons Learned").	☐	☐	☐	☐
3.6: Planificar las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1: Difundir las medidas de ciberseguridad definidas por la organización, usando medios tales como correo electrónico, intranet corporativa y sesiones específicas, entre otros.	☐	☐	☐	☐
4.2: Establecer la normativa de protección del puesto de trabajo, incluyendo ítems tales como escenarios y ejemplos de riesgo y medidas de seguridad, entre otros.	☐	☐	☐	☐
4.3: Definir el plan de concienciación de ciberseguridad dirigido a los empleados, elaborando material y cursos o tutoriales para su difusión o impartición y las evaluaciones a realizar y su periodicidad.	☐	☐	☐	☐
4.4: Difundir el material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados 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.	☐	☐	☐	☐

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4