PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

Código: **IFC153_3** **NIVEL: 3**

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

UNIDAD DE COMPETENCIA "UC0487_3: Auditar redes de comunicación y sistemas informáticos"

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 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Su resultado servirá solamente para ayudarle, **ORIENTÁNDOLE** en qué medida posee la competencia profesional de la "UC0487_3: Auditar redes de comunicación y sistemas informáticos"

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. Realizar análisis de vulnerabilidades, mediante programas específicos para controlar posibles fallos en la seguridad de los sistemas según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1. Seleccionar las herramientas y los tipos de pruebas de análisis de vulnerabilidades, adecuándolas al entorno a verificar según las especificaciones de seguridad de la organización y el sector al que pertenece la misma.	☐	☐	☐	☐
1.2. Actualizar los programas y las pruebas para realizar ensayos consistentes con los posibles fallos de seguridad de las versiones de hardware y software instaladas en el sistema informático.	☐	☐	☐	☐
1.3. Analizar los resultados de las pruebas, documentándolos conforme se indica en las normas de la organización.	☐	☐	☐	☐
1.4. Comprobar los sistemas de acceso por contraseña mediante herramientas específicas según las especificaciones de la normativa de seguridad.	☐	☐	☐	☐

1. Realizar análisis de vulnerabilidades, mediante programas específicos para controlar posibles fallos en la seguridad de los sistemas según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.5. Documentar el análisis de vulnerabilidades, incluyendo referencias exactas a las aplicaciones y servicios que se han detectado funcionando en el sistema, el nivel de los parches instalados, vulnerabilidades de negación de servicio, vulnerabilidades detectadas y mapa de la red.	☐	☐	☐	☐

2. Verificar el cumplimiento de las normativas, buenas prácticas y requisitos legales aplicables para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1. Comprobar la asignación de responsable de seguridad a todos los ficheros con datos de carácter personal según la normativa aplicable.	☐	☐	☐	☐
2.2. Verificar el estado del listado de personas autorizadas a acceder a cada fichero, comprobando que está actualizado según la normativa aplicable.	☐	☐	☐	☐
2.3. Comprobar el control de accesos a los ficheros siguiendo el procedimiento establecido en la normativa de seguridad de la organización.	☐	☐	☐	☐
2.4. Auditar la gestión del almacenamiento de los ficheros y sus copias de seguridad, comprobando que se realiza siguiendo la normativa aplicable y las normas de la organización.	☐	☐	☐	☐
2.5. Auditar el acceso telemático a los ficheros, comprobando que se realiza utilizando mecanismos que garanticen la confidencialidad e integridad cuando así lo requiera la normativa.	☐	☐	☐	☐

2. Verificar el cumplimiento de las normativas, buenas prácticas y requisitos legales aplicables para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.6. Elaborar el informe de la auditoría, incluyendo la relación de ficheros con datos de carácter personal, las medidas de seguridad aplicadas y aquellas pendientes de aplicación (no conformidades) así como puntos fuertes y puntos de mejora.	☐	☐	☐	☐

3. Comprobar el cumplimiento de la política de seguridad establecida para afirmar la integridad del sistema según las necesidades de uso y dentro de las directivas de la organización y teniendo en cuenta la normativa aplicable nacional e internacional.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1. Desarrollar y revisar los procedimientos de detección y gestión de incidentes de seguridad, comprobando que están incluidos en la normativa de seguridad de la organización y que incluyen todo lo necesario para administrar de forma eficiente las posibles incidencias que pueden afectar a la organización.	☐	☐	☐	☐
3.2. Testear los puntos de acceso de entrada y salida de la red comprobando que su uso se circunscribe a lo descrito en la normativa de seguridad de la organización.	☐	☐	☐	☐
3.3. Comprobar la activación y actualización de los programas de seguridad y protección de sistemas, viendo que corresponden a las especificaciones de los fabricantes.	☐	☐	☐	☐
3.4. Validar los puntos de entrada y salida de la red adicionales, verificando que se autorizan y controlan en base a las especificaciones de seguridad y al plan de implantación de la organización.	☐	☐	☐	☐

3. Comprobar el cumplimiento de la política de seguridad establecida para afirmar la integridad del sistema según las necesidades de uso y dentro de las directivas de la organización y teniendo en cuenta la normativa aplicable nacional e internacional.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.5. Revisar los procesos de auditoría informática, tanto los de carácter interno, como aquellos realizados por personal externo a la organización, comprobando que se encuentran activados, actualizados y con los parámetros especificados en las normas de la organización.	☐	☐	☐	☐
3.6. Verificar el cumplimiento de los procedimientos de las políticas de seguridad por parte de los usuarios de forma que se detecte su correcta aplicación y adecuación a las necesidades de la organización en materia de seguridad.	☐	☐	☐	☐