



PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUALIFICACIÓN PROFESIONAL: GESTIÓN DE SISTEMAS INFORMÁTICOS

Código: IFC152_3

NIVEL: 3

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

UNIDAD DE COMPETENCIA “UC0486_3: Asegurar equipos 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 “UC0486_3: Asegurar equipos 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:

Cada **actividad profesional principal (APP)** se compone de **varias actividades profesionales secundarias (APS)**.

Lea atentamente cada APP y a continuación sus APS. En cada APS marque con una cruz el indicador de autoevaluación que considere más ajustado a su grado de dominio de las APS. 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.

<i>APP1: Asignar políticas de seguridad en el acceso de los usuarios siguiendo las necesidades de uso y condiciones de seguridad.</i>	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
APS1.1: Verificar la existencia de procedimientos de instalación y actualización de equipos, de copias de respaldo, de detección de errores, de restricción de equipos y de protección contra virus y elementos no deseados a partir del plan de implantación del sistema informático de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS1.2: Establecer los permisos de acceso a los recursos del sistema según el plan de seguridad y la normativa de implantación.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS1.3: Verificar la integridad de la conexión y la confidencialidad en el acceso a servidores siguiendo las normas de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS1.4: Comprobar la inclusión de usos y restricciones de equipos y usuarios, los servicios de red permitidos y restringidos y el ámbito de responsabilidades en la utilización de los equipos informáticos en las políticas de usuario según las especificaciones.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS1.5: Transmitir la política de seguridad a los usuarios asegurando su correcta interpretación.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS1.6: Documentar las tareas realizadas aplicando los procedimientos de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS1.7: Comprobar el cumplimiento de la legislación de protección de datos en la información afectada por ella siguiendo el plan de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



APP2: Preparar servidores protegiéndolos frente a accesos no deseados y siguiendo las necesidades de uso y las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
APS2.1: Ubicar el servidor en la red en una zona protegida y aislada cumpliendo el plan de seguridad y la normativa de implantación del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS2.2: Configurar los servicios que ofrece el servidor según el plan de seguridad y la normativa de implantación del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS2.3: Configurar los accesos y permisos a los recursos del servidor según el propósito del mismo y cumpliendo la política de seguridad de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS2.4: Activar los mecanismos de registro de actividad e incidencias del sistema y sus procedimientos de análisis permitiendo analizar dicha información.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS2.5: Determinar una solución de compromiso entre funcionalidades y riesgos para los módulos adicionales del servidor a partir del análisis del mismo.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS2.6: Configurar los mecanismos de autenticación según la normativa de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS2.7: Crear los roles y privilegios de los usuarios según la normativa de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

APP3: Implantar cortafuegos en equipos y servidores teniendo en cuenta las necesidades de uso y las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
APS3.1: Seleccionar la topología del cortafuegos para el entorno de implantación en base a las necesidades planteadas.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



APP3: Implantar cortafuegos en equipos y servidores teniendo en cuenta las necesidades de uso y las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
APS3.2: Elegir los elementos hardware y software del cortafuegos según factores económicos y de rendimiento.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS3.3: Efectuar la puesta en marcha de los cortafuegos según el nivel exigido por la política de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS3.4: Configurar las reglas de filtrado y los niveles de registro y alarmas cumpliendo la normativa de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS3.5: Verificar los cortafuegos asegurando el cumplimiento de lo especificado en la normativa de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS3.6: Documentar la instalación, actualización y procedimientos de actuación del cortafuegos según las especificaciones de la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APS3.7: Configurar los sistemas de registro de forma que permitan su análisis en busca de problemas de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>