



PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

**CUALIFICACIÓN PROFESIONAL: OPERACIÓN DE SISTEMAS
INFORMÁTICOS**

Código: IFC300_2

NIVEL: 2

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

UNIDAD DE COMPETENCIA

**“UC0959_2: Mantener la seguridad de los subsistemas físicos y
lógicos en 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 “UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en 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 la copia de seguridad, para garantizar la integridad de los datos, según los procedimientos establecidos y el plan de seguridad.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1. Realizar las copias de seguridad, para proteger los datos del sistema, según la periodicidad, soporte y procedimiento establecidos en el plan de seguridad del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2. Verificar las copias de seguridad, para asegurar la utilización de las mismas, según los procedimientos establecidos en el plan de seguridad del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3. Realizar el almacenamiento de las copias de seguridad, para evitar pérdidas de la información, en las condiciones y según el procedimiento indicado en el plan de seguridad del sistema y las recomendaciones del fabricante del soporte.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.4. Documentar y registrar las incidencias detectadas, en el caso en que no estén ya registradas, según procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



2. Revisar los accesos al sistema informático, para asegurar la aplicación de los procedimientos establecidos y el plan de seguridad, informando de las anomalías detectadas.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1. Comprobar las herramientas de monitorización, para trazar los accesos y la actividad del sistema para asegurar su funcionamiento, según el plan de seguridad del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2. Recopilar los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para localizar la existencia de accesos o actividades no deseados.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3. Documentar y registrar las incidencias de acceso al sistema detectadas, en el caso en que no estén ya registradas, según procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4. Documentar los cambios detectados en la configuración del acceso de usuarios al sistema, para mantener el inventario actualizado, según procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Comprobar el funcionamiento de los mecanismos de seguridad establecidos informando de las anomalías detectadas a personas de responsabilidad superior.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1. Comprobar los permisos de acceso de los usuarios al sistema, para asegurar su validez, según el plan de seguridad del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2. Comprobar las políticas de seguridad de usuario, para cerciorar su validez, según el plan de seguridad del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3. Revisar los sistemas de protección antivirus y de programas maliciosos, en lo que respecta a su actualización y configuración funcional, para garantizar la seguridad del equipo, según los procedimientos establecidos por la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



3. Comprobar el funcionamiento de los mecanismos de seguridad establecidos informando de las anomalías detectadas a personas de responsabilidad superior.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.4. Documentar y registrar las incidencias detectadas, en el caso en que no estén ya registradas, según procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5. Realizar los procesos de diagnóstico en los equipos en los que se han detectado incidencias utilizando herramientas específicas y de gestión remota con el fin de solucionarlas o escalarlas siguiendo los procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Verificar que las condiciones ambientales y de seguridad se mantienen según los planes establecidos, informando de posibles anomalías.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1. Comprobar las especificaciones técnicas de los dispositivos, para asegurar que se cumplen las recomendaciones de los fabricantes, en cuanto a condiciones ambientales y de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2. Revisar la ubicación de los equipos y dispositivos físicos para asegurar que se cumplen los requisitos en cuanto a seguridad, espacio y ergonomía establecidos por la organización.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3. Documentar y registrar las incidencias detectadas, en el caso en que no estén ya registradas, según procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.4. Realizar las acciones correctivas establecidas, para solucionar determinadas incidencias detectadas, según procedimientos establecidos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>