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 "UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos"

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 "UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos"

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 políticas de seguridad y cifrado de información en operaciones de intercambio de datos para obtener conexiones seguras según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1. Realizar las comunicaciones con otras compañías o a través de canales inseguros haciendo uso de redes privadas virtuales para garantizar la confidencialidad e integridad de dichas conexiones durante el tránsito a través de redes públicas según las especificaciones de la normativa aplicable de seguridad y el diseño de redes de la organización.	☐	☐	☐	☐
1.2. Seleccionar los requerimientos para implantar la solución de red privada virtual y comunicar al operador de telefonía para lograr soluciones adecuadas al plan de seguridad.	☐	☐	☐	☐
1.3. Evaluar las técnicas de protección de conexiones inalámbricas disponibles en el mercado seleccionar aquellas más idóneas, teniendo en cuenta el principio de proporcionalidad y las normas de seguridad de la organización.	☐	☐	☐	☐
1.4. Implantar los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones según parámetros de la normativa de seguridad de la organización.	☐	☐	☐	☐

1. Implantar políticas de seguridad y cifrado de información en operaciones de intercambio de datos para obtener conexiones seguras según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.5. Activar la encapsulación, o encriptación extremo a extremo para aquellos servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas para garantizar la seguridad de las comunicaciones.	☐	☐	☐	☐
1.6. Emplear los servicios que incorporan soporte para certificados digitales para identificación del servidor, para garantizar al usuario la identidad del servidor.	☐	☐	☐	☐
1.7. Documentar las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas en el formato establecido en la organización.	☐	☐	☐	☐
1.8. Los servicios que incorporan una autenticación de doble o triple factor, validación con certificados de usuario, DNI electrónico, 'token', biométricos u otros dispositivos.	☐	☐	☐	☐

2. Implantar sistemas de firma digital para asegurar la autenticidad, integridad y confidencialidad de los datos que intervienen en una transferencia de información utilizando sistemas y protocolos criptográficos según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1. Implantar el acceso a servicios a través de la red telemática de forma que utilice la autenticación basada en certificados digitales de identidad personal.	☐	☐	☐	☐
2.2. Aplicar el proceso de obtención y verificación de firmas, en caso de ser necesario, según los requerimientos del sistema informático y los procesos de negocio.	☐	☐	☐	☐

2. Implantar sistemas de firma digital para asegurar la autenticidad, integridad y confidencialidad de los datos que intervienen en una transferencia de información utilizando sistemas y protocolos criptográficos según las necesidades de uso y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.3. Asegurar la utilización de certificados digitales para firmar y cifrar su contenido en la transmisión de mensajes de correo electrónico.	☐	☐	☐	☐
2.4. Emplear el perfil de firma digital de documentos estándar asegurando que es el más adecuado al uso que se va a realizar.	☐	☐	☐	☐
2.5. Implantar los sistemas de sellado digital de tiempo, para garantizar la existencia de un documento en una determinada fecha, según las normas de seguridad de la organización.	☐	☐	☐	☐
2.6. Firmar digitalmente los componentes web de forma que se pueda garantizar la integridad de dichos componentes.	☐	☐	☐	☐
2.7. Documentar los sistemas de firma digital implantados en el formato establecido en la organización.	☐	☐	☐	☐

3. Implementar infraestructuras de clave pública para garantizar la seguridad según los estándares del sistema y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1. Diseñar la jerarquía de certificación en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.	☐	☐	☐	☐
3.2. Redactar la declaración de prácticas de certificación y la política de certificación de forma que definen los procedimientos y derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.	☐	☐	☐	☐

3. Implementar infraestructuras de clave pública para garantizar la seguridad según los estándares del sistema y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.3. Instalar el sistema de autoridad de certificación siguiendo las indicaciones del fabricante.	☐	☐	☐	☐
3.4. Poner a disposición de los usuarios el certificado digital de la autoridad de certificación y su política asociada, en la forma y modo necesario, siguiendo las directrices contenidas en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.5. Mantener la clave privada de la autoridad de certificación segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.6. Realizar la emisión de certificados digitales según los usos que va a recibir el certificado y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.7. Mantener accesible la información sobre validez de los certificados emitidos por la autoridad de certificación, según lo indicado en la declaración de prácticas de certificación, mediante el servicio de revocación de certificados.	☐	☐	☐	☐
3.8. Documentar las infraestructuras de clave pública implantadas en el formato establecido en la organización.	☐	☐	☐	☐