PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP0489_3: 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 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 "ECP0489_3: 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 protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso, garantizando la integridad y confidencialidad de la información, así como el control de acceso, para obtener comunicaciones o canales de comunicación seguros, cumpliendo las directivas del departamento responsable de la seguridad del sistema informático.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Garantizar la confidencialidad e integridad en las comunicaciones durante el tránsito a través de redes públicas, haciendo uso de redes privadas virtuales, comunicándolos al proveedor del servicio para lograr soluciones ajustadas al plan de seguridad.	☐	☐	☐	☐
1.2: Aplicar las técnicas de protección de conexiones inalámbricas disponibles en el mercado, seleccionando aquellas basadas en estándares reconocidos como confiables en el sector, para cubrir vulnerabilidades, teniendo en cuenta el principio de proporcionalidad.	☐	☐	☐	☐
1.3: Implantar los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones, diferenciando usuarios por perfiles y asignándoles permisos según ese perfil.	☐	☐	☐	☐
1.4: Proteger los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas, usando herramientas disponibles para el cifrado extremo a extremo, para garantizar la seguridad de las comunicaciones.	☐	☐	☐	☐
1.5: Garantizar la identidad de los servidores en aquellos servicios que lo soportan, usando certificados digitales, configurando las aplicaciones cliente	☐	☐	☐	☐

1: Implantar protocolos y herramientas en operaciones de intercambio de datos según las necesidades de uso, garantizando la integridad y confidencialidad de la información, así como el control de acceso, para obtener comunicaciones o canales de comunicación seguros, cumpliendo las directivas del departamento responsable de la seguridad del sistema informático.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
con el certificado raíz de confianza que garantice al usuario la autenticidad del servidor.				
1.6: Documentar las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas, incluyendo las características de las configuraciones aplicadas, ajustándolo a estándares y/o en el formato establecido en la organización.	☐	☐	☐	☐
1.7: Asegurar los servicios, cuyo nivel riesgo estime el departamento entidad responsable de la gestión de la seguridad del sistema informático que lo requieran, incorporando una autenticación de doble o triple factor basada en certificados de usuario, DNI electrónico, "token", biométricos u otros mecanismos.	☐	☐	☐	☐
1.8: Configurar los servicios en los que se utiliza autenticación basada en contraseñas, estableciendo políticas de complejidad, renovación, bloqueo, almacenamiento y/o recuperaciones.	☐	☐	☐	☐

2: Implantar el uso de sistemas de firma y certificados de persona para asegurar la autenticidad, integridad, confidencialidad y "no repudio" de los datos que intervienen en una transferencia de información personal según las necesidades de uso y dentro de las directivas del departamento responsable de la seguridad del sistema informático.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Implantar el acceso a servicios a través de la red telemática de forma que asegure la autenticación mutua de cliente y servidor, utilizando autenticación de cliente basada en certificados digitales de identidad personal cuando la política de seguridad de la organización así lo requiera.	☐	☐	☐	☐
2.2: Aplicar el proceso de obtención y verificación de certificados digitales de identidad personal, siguiendo los pasos establecidos por la entidad certificadora y con la periodicidad indicada por el departamento responsable de la seguridad del sistema.	☐	☐	☐	☐

2: Implantar el uso de sistemas de firma y certificados de persona para asegurar la autenticidad, integridad, confidencialidad y "no repudio" de los datos que intervienen en una transferencia de información personal según las necesidades de uso y dentro de las directivas del departamento responsable de la seguridad del sistema informático.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.3: Implementar los mecanismos para la transmisión cifrada del correo electrónico y otras comunicaciones, ya sea interpersonales o entre procesos y/o componentes, empleando certificados digitales para firmar y cifrar extremo a extremo el contenido de dichos mensajes, en los casos que indique la política de seguridad de la organización.	☐	☐	☐	☐
2.4: Aplicar los mecanismos de firma digital de documentos seleccionados de acuerdo con la política de seguridad del departamento responsable, incluyendo dicha firma en el momento del envío o, en su caso, al almacenar cada documento.	☐	☐	☐	☐
2.5: Implantar los sistemas de sellado digital de tiempo, aplicándolos a los documentos que requiera la seguridad de la organización, para garantizar la existencia de un documento electrónico en un instante concreto, garantizando que la información contenida no ha sido alterada por terceros.	☐	☐	☐	☐
2.6: Garantizar la integridad de los componentes en sitios "web" y del "software" interno, firmándolos mediante firma digital, según el procedimiento del sistema o herramientas de firmado.	☐	☐	☐	☐
2.7: Documentar los sistemas de firma digital implantados indicando su ámbito de aplicación, el procedimiento para su uso, la tipología de documentos, aplicaciones a firmar y el sistema de firma aplicado, entre otros, siguiendo estándares y de acuerdo con el formato establecido en la organización.	☐	☐	☐	☐

3: Implementar infraestructuras de clave pública, siguiendo instrucciones del fabricante y en función de las condiciones de uso, 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: Instalar la jerarquía de certificación configurando la herramienta que la implementa, siguiendo las instrucciones del proveedor, en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.	☐	☐	☐	☐

3: Implementar infraestructuras de clave pública, siguiendo instrucciones del fabricante y en función de las condiciones de uso, para garantizar la seguridad, según los estándares del sistema y dentro de las directivas de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.2: Redactar la declaración de prácticas de certificación y la política de certificación, definiendo los procedimientos, derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.	☐	☐	☐	☐
3.3: Instalar el sistema de autoridad de certificación, siguiendo las indicaciones del fabricante, las prácticas recomendadas del sector y la política de seguridad de la organización.	☐	☐	☐	☐
3.4: Poner a disposición de los usuarios el certificado digital de la autoridad de certificación y su política asociada, siguiendo las directrices contenidas en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.5: Almacenar la clave privada de la autoridad de certificación, manteniéndola segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.6: Emitir los certificados digitales según los usos que van a recibir los certificados y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.7: Comprobar la validez de los certificados emitidos por la autoridad de certificación, verificando que es mantenido por el servicio de revocación de certificados, según lo indicado en la declaración de prácticas de certificación.	☐	☐	☐	☐
3.8: Documentar las infraestructuras de clave pública implantadas recogiendo sus datos de configuración, ajustándose a estándares y según el formato establecido en la organización.	☐	☐	☐	☐

4: Revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos según las directrices de la entidad responsable de la gestión de la red.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1: Adaptar la topología de la red según las necesidades de seguridad, valorando su idoneidad mediante el análisis de modelos de referencia estándar,	☐	☐	☐	☐

4: Revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos según las directrices de la entidad responsable de la gestión de la red.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
seleccionando una nueva topología y añadiendo o suprimiendo dispositivos de comunicaciones para minimizar posibles riesgos.				
4.2: Segmentar la red de la organización de acuerdo con la compartimentación organizativa, la identidad de los equipos o usuarios y la política de seguridad de la entidad responsable, ya sea de forma física, mediante equipos tales como "routers", o de forma lógica utilizando VLAN ("Virtual Local Área Networks").	☐	☐	☐	☐
4.3: Establecer las reglas o pautas de filtrado perimetral entre los segmentos de la red y, en su caso, entre máquinas específicas, de acuerdo con la segmentación establecida y la política de seguridad de la organización.	☐	☐	☐	☐
4.4: Establecer los mecanismos de protección para las redes de acceso, ante elementos que rompen con el perímetro tradicional de la red corporativa, tales como redes inalámbricas, dispositivos móviles y portátiles, particulares o corporativos, con conexión a las redes de la organización identificando los dispositivos empleados, delimitando su alcance y protegiendo el acceso mediante cifrado seguro, de acuerdo con la política de seguridad de la organización.	☐	☐	☐	☐
4.5: Implementar los mecanismos para prevenir la fuga de datos (DLP: "Data Loss Prevention") mediante "hardware" o "software" al efecto, en virtud de los requisitos de seguridad de la organización, para detectar potenciales brechas en el acceso y/o transmisión de datos y prevenirlas a través del monitoreo, detección y bloqueo de información sensible.	☐	☐	☐	☐
4.6: Modificar el diseño de la red en su caso, introduciendo "hardware" y "software" que garanticen la alta disponibilidad y tolerancia a fallos, bien duplicando la red física, equipos y "software", bien mediante la virtualización de sistemas.	☐	☐	☐	☐
4.7: Configurar los equipos que proporcionan redundancia, alta disponibilidad y tolerancia a fallos en una red troncal, asegurando una transmisión de datos confiable y segura entre los distintos nodos que la conforman.	☐	☐	☐	☐
4.8: Revisar los procedimientos de salvaguarda de configuraciones modificando, en su caso, la programación de sus copias de seguridad mediante la funcionalidad habilitada en el sistema, almacenándolas en condiciones de seguridad y permitiendo una eficaz recuperación.	☐	☐	☐	☐

4: Revisar el "hardware" y el diseño de la red de área local, aplicando adaptaciones para garantizar la seguridad de las comunicaciones y la protección de los datos según las directrices de la entidad responsable de la gestión de la red.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.9: Elaborar la documentación de configuración de seguridad incluyendo todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.	☐	☐	☐	☐

5: Revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, actualizándolo, añadiendo o suprimiendo elementos y/o modificando configuraciones, para garantizar la seguridad de las comunicaciones y la protección de los datos, según las directrices de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
5.1: Evaluar el "software" de comunicaciones que se ejecuta en los dispositivos de red, valorando su compatibilidad, teniendo en cuenta su funcionalidad y su idoneidad para el diseño a corto y medio plazo, comprobando su integridad, legitimidad y grado de actualización para corregir problemas de seguridad.	☐	☐	☐	☐
5.2: Incluir los productos "software" de comunicaciones relacionados con su seguridad, tales como cortafuegos ("firewalls"), o "proxies" en el diseño de la red, comparando prestaciones y características e interpretando la documentación técnica asociada.	☐	☐	☐	☐
5.3: Revisar los procedimientos de salvaguarda del "software", modificando en su caso la programación de los "backup", almacenándolos en condiciones de seguridad y permitiendo una eficaz recuperación.	☐	☐	☐	☐
5.4: Revisar los medios de identificación de accesos a la red y a la administración de los equipos tales como autenticación 802.1x, servidores Radius, usuarios, perfiles, roles u otros, ajustándolos de forma que garanticen la seguridad, la trazabilidad de los parámetros y las definiciones de configuración, estableciendo protocolos para el cambio cíclico de contraseñas fijas que no caducan, estableciendo mecanismos de control de acceso del equipo de red de forma que sólo puedan ser modificados desde puntos permitidos y por administradores autorizados.	☐	☐	☐	☐
5.5: Aplicar la configuración de seguridad en el ámbito de red garantizando el funcionamiento de puntos críticos, tales como la seguridad de puerto y configurando los mecanismos de control de tormentas de difusión, tales como el protocolo de árbol de expansión ("spanning-tree"), protocolos de redundancia	☐	☐	☐	☐

5: Revisar el "software" de comunicaciones en red y el control de acceso de manera periódica, actualizándolo, añadiendo o suprimiendo elementos y/o modificando configuraciones, para garantizar la seguridad de las comunicaciones y la protección de los datos, según las directrices de la organización.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
("Parallel Redundancy Protocol" -PRP-) y "Highly-available Seamless Redundancy" (HSR), entre otros.				
5.6: Elaborar la documentación del "software" de seguridad incluyendo productos, referencias y todos los valores de configuración implantados, ajustándolo a estándares y según el formato establecido en la organización.	☐	☐	☐	☐