PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP0487_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 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 "ECP0487_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: Comprobar la seguridad de los sistemas informáticos, revisando el bastionado de las instalaciones, equipos y "software", para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada, según indicaciones del plan de seguridad de la organización auditada.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Revisar el inventariado de activos, verificando los equipos existentes y sus características, comprobando las versiones de los programas que se ejecutan, para confirmar que está actualizado y no hay equipos ni programas que no aparezcan en el mismo.	☐	☐	☐	☐
1.2: Revisar la instalación y configuración de los sistemas operativos, confirmando que el "software" instalado es legítimo, está actualizado y tanto los usuarios como las aplicaciones cuentan con los permisos de "mínimo privilegio" para desempeñar sus funciones en el sistema.	☐	☐	☐	☐
1.3: Comprobar la instalación y configuración de "software" de seguridad contra programas maliciosos tales como antivirus/antimalware, EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"), entre otros, verificando que dicho "software" es legítimo, está actualizado y tiene activas las funciones que indique el responsable de seguridad.	☐	☐	☐	☐
1.4: Revisar las aplicaciones empleadas en la organización, comprobando licencias y versiones para confirmar que son legítimas, están actualizadas y que únicamente pueden ser accedidas por el personal autorizado, y que ese acceso tenga las limitaciones que indique el responsable de seguridad, basadas en el principio de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know").	☐	☐	☐	☐

1: Comprobar la seguridad de los sistemas informáticos, revisando el bastionado de las instalaciones, equipos y "software", para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada, según indicaciones del plan de seguridad de la organización auditada.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.5: Comprobar las cuentas de usuario de la organización que son individuales, cuentan con una política de contraseñas robusta y han sido elaboradas bajo el principio de "mínimo privilegio" y segregación de funciones, modificando aquellas que no cumplen los criterios y eliminando las cuentas obsoletas o que no pertenecen a personas autorizadas.	☐	☐	☐	☐
1.6: Comprobar las instalaciones de manera presencial para asegurarse de que los equipos y la información están protegidos contra accesos físicos no autorizados, usando elementos al efecto de manera separada o combinada tales como mecanismos de apertura por usuario y contraseña, llave física, detectores biométricos entre otros, aplicando un sistema de aviso previo y bloqueando sesiones por inactividad y usando políticas de "mesas limpias".	☐	☐	☐	☐
1.7: Comprobar las instalaciones, verificando las condiciones ambientales de temperatura y humedad requeridas por el fabricante para su funcionamiento y la protección frente a desastres naturales que pueden afectar físicamente en el emplazamiento y previniendo posibles alteraciones del entorno tales como picos de electricidad o ruido eléctrico, entre otros.	☐	☐	☐	☐
1.8: Documentar las pruebas realizadas durante la auditoría, incluyendo referencias a los activos del sistema, los parches y actualizaciones instalados en los sistemas operativos y aplicaciones, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.	☐	☐	☐	☐

2: Comprobar la seguridad de la red de la organización auditada, verificando los elementos relativos indicados en el plan de seguridad, para prevenir posibles intrusiones, ataques y fugas de información.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Revisar el diseño de arquitectura de la red, mediante auditoría de caja blanca, comprobando que la red está configurada de forma que se minimice el impacto de posibles ataques del exterior: utilizando VLAN ("Virtual Local Área Networks"), cortafuegos, sistemas de detección de intrusiones (IDS) , sistemas de prevención de intrusiones (IPS), "routers" y otros dispositivo de red e instalado todos los recursos de la empresa que deben ser accesibles desde Internet tales como páginas web y correo electrónico, en una zona aislada o desmilitarizada (DMZ).	☐	☐	☐	☐

2: Comprobar la seguridad de la red de la organización auditada, verificando los elementos relativos indicados en el plan de seguridad, para prevenir posibles intrusiones, ataques y fugas de información.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.2: Revisar los dispositivos que controlan y gestionan el tráfico de la red tales como "router", "switch", "hub", cortafuegos, IDS, IPS, SIEM ("Security Information and Event Management"), entre otros, usando técnicas de caja blanca: de manera física y comprobando su configuración para verificar que únicamente aceptan el tráfico permitido y están actualizados.	☐	☐	☐	☐
2.3: Revisar los mensajes de error generados por los dispositivos de red, "routers", "switch", "hub" cortafuegos, IDS, IPS, SIEM y cualquier otro, en forma de auditoría de caja blanca para asegurar que, de forma interna, registran cualquier anomalía para facilitar la gestión de incidentes y, de forma externa en modo auditoría de caja negra, para confirmar que no aportan información que permita a un posible atacante remoto obtener información de los puertos abiertos en el sistema.	☐	☐	☐	☐
2.4: Comprobar los elementos de la red que únicamente son accedidos de forma remota por personal y bajo las condiciones de tiempo y lugar de origen, previamente autorizados en la política de seguridad y sólo a través de las VPN (Redes privadas Virtuales).	☐	☐	☐	☐
2.5: Revisar el uso de programas o herramientas en la nube, verificando que se lleva a cabo de la forma acordada con el proveedor del servicio y permitida dentro de la política de seguridad de la organización.	☐	☐	☐	☐
2.6: Comprobar las redes Wifi, verificando que utilizan protocolos seguros de cifrado y que únicamente acceden a ellas las personas autorizadas en la política de seguridad.	☐	☐	☐	☐
2.7: Comprobar la conexión a Internet por parte de los usuarios de la organización, verificando que únicamente pueden acceder a los servicios y contenidos previamente autorizados en la política de seguridad.	☐	☐	☐	☐
2.8: Verificar los sistemas anti DDoS (Denegación de servicio) de la organización que están habilitados y funcionales, comprobando si se han configurado sistemas al efecto tales como reglas de cortafuegos, sistemas de monitorización y/o servicios externos de protección, entre otros.	☐	☐	☐	☐

2: Comprobar la seguridad de la red de la organización auditada, verificando los elementos relativos indicados en el plan de seguridad, para prevenir posibles intrusiones, ataques y fugas de información.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.9: Documentar las pruebas realizadas durante la auditoría, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.	☐	☐	☐	☐

3: Comprobar la seguridad del sitio "web", realizando pruebas de simulación de ataques para detectar posibles fallos de seguridad.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1: Verificar la instalación y configuración de los sistemas de gestión de contenidos (CMS) y servidores web, comprobando que están instaladas las últimas versiones estables y que únicamente tienen instalados los módulos imprescindibles para su funcionamiento, revisando la documentación asociada.	☐	☐	☐	☐
3.2: Comprobar las cuentas de usuario del sitio "web", verificando que son generadas bajo el principio de "mínimo privilegio" y cuentan con una política de acceso segura.	☐	☐	☐	☐
3.3: Verificar la información generada de forma pública por el servidor "web" y/o el sistema de gestión de contenidos (CMS), comprobando que no muestre ninguna información que permita obtener fácilmente información relacionada con la configuración del sistema tal como tipo de programa empleado, versión, entre otros.	☐	☐	☐	☐
3.4: Comprobar la gestión de sesiones en el sistema, verificando que tanto las "cookies" como los "tokens" de sesión se generan de forma segura y no predecible, tal como evitando la numeración secuencial para la identificación de usuarios, para impedir que un atacante externo pueda aprovecharse de ellas para acceder al sistema de forma no autorizada.	☐	☐	☐	☐
3.5: Comprobar los formularios y puntos de acceso de información por parte del usuario, verificando que cuentan con mecanismos que impidan la entrada de caracteres que provoquen un comportamiento no deseado del sistema como la introducción de código (por inyección de SQL o XSS - "Cross-site scripting"-, entre otros) o la generación de errores en el sistema tales como desbordamiento de "buffer" por introducción de cadenas largas.	☐	☐	☐	☐

3: Comprobar la seguridad del sitio "web", realizando pruebas de simulación de ataques para detectar posibles fallos de seguridad.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.6: Comprobar la gestión de errores y excepciones del sistema, verificando que éstos son registrados y la información mostrada en el lado del cliente no revela información que pueda permitir a los usuarios una posterior explotación del fallo.	☐	☐	☐	☐
3.7: Comprobar que la información entre el cliente y el servidor se envía de forma segura, verificando que se realiza a través de protocolos tales como HTTPS y TLS, que la información enviada se cifra, siguiendo estándares actualizados.	☐	☐	☐	☐
3.8: Documentar las pruebas realizadas durante la auditoría, incluyendo referencias a los activos inspeccionados, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.	☐	☐	☐	☐

4: Comprobar la seguridad de la información tratada por la organización auditada, verificando y asegurando los elementos relativos indicados en el plan de seguridad, para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y el "no repudio" y el cumplimiento de la normativa aplicable de protección de datos.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1: Comprobar la asignación de los roles del personal responsable de la gestión, tratamiento y almacenamiento de los datos, verificando que se accede a la información requerida en cada caso y su alineación con el principio de "mínimo privilegio" y "necesidad de saber".	☐	☐	☐	☐
4.2: Comprobar las medidas de seguridad físicas y lógicas implantadas para la recogida, gestión, tratamiento, almacenamiento, intercambio y borrado de los datos, verificando que se cumple con los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio.	☐	☐	☐	☐
4.3: Comprobar el intercambio de información, verificando que se realiza únicamente a través de los canales autorizados, de la forma convenida y por las personas definidas en la normativa de la organización.	☐	☐	☐	☐
4.4: Revisar el registro de actividades del tratamiento de los datos, verificando que está completo y actualizado, comprobando que el tratamiento únicamente se efectúa por personas autorizadas en la normativa de seguridad de la organización.	☐	☐	☐	☐

4: Comprobar la seguridad de la información tratada por la organización auditada, verificando y asegurando los elementos relativos indicados en el plan de seguridad, para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y el "no repudio" y el cumplimiento de la normativa aplicable de protección de datos.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.5: Revisar los protocolos de eliminación de información, confirmando que garantizan el borrado seguro de la información, destruyendo el papel en máquinas y contenedores específicos que no permitan la recuperación de la información y, en caso de cesión de dispositivos digitales a terceros, que no se pueda acceder a la información contenida previamente en él.	☐	☐	☐	☐
4.6: Verificar la realización de copias de seguridad, comprobando que está alineado con la política de seguridad de la organización de forma que, ante una eliminación de datos por un desastre natural, o por personas de modo accidental o intencionado, es posible recuperar la información en los plazos de tiempo convenidos.	☐	☐	☐	☐
4.7: Revisar la aplicación de la normativa de seguridad por parte de los usuarios, verificando que saben cómo y dónde reportar los incidentes informáticos, no hacen uso de dispositivos no autorizados o de origen desconocido, aplican la política de "mesas limpias", bloquean el equipo si van a estar ausentes y no divulgan información asociada con su trabajo.	☐	☐	☐	☐
4.8: Elaborar el informe de la auditoría, incluyendo el alcance de la misma, la documentación revisada, las pruebas y entrevistas realizadas, los posibles obstáculos encontrados y las evidencias obtenidas, presentando especial atención a los hallazgos clasificados y no conformidades de las que también se indicará su criticidad, detallando el grado de cumplimiento legal y las medidas de mejora convenientes.	☐	☐	☐	☐