PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP0486_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 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 "ECP0486_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:

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: Configurar equipos informáticos siguiendo los procedimientos establecidos en el plan de seguridad de la organización para protegerlos de la pérdida, manipulación y sustracción de información no autorizada.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Definir los tipos de usuarios, estableciendo los privilegios de acceso a los recursos (aplicaciones software, carpetas, entre otros), según las funciones desempeñadas dentro de la organización.	☐	☐	☐	☐
1.2: Crear las cuentas de usuario, utilizando las herramientas específicas del sistema operativo, dándoles un nombre de usuario, una contraseña y asignándolas a los tipos de usuarios definidos en el sistema informático.	☐	☐	☐	☐
1.3: Configurar la política de contraseñas, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.	☐	☐	☐	☐
1.4: Establecer el control de acceso al equipo informático, configurando parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.	☐	☐	☐	☐
1.5: Reforzar la seguridad del equipo informático ante ataques externos, configurando un cortafuegos según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.	☐	☐	☐	☐
1.6: Revisar la seguridad de la información del equipo informático (integridad, accesos, entre otros) frente a riesgos de ataque malicioso, comprobando la instalación y configuración del software de protección adecuado (EDP	☐	☐	☐	☐

1: Configurar equipos informáticos siguiendo los procedimientos establecidos en el plan de seguridad de la organización para protegerlos de la pérdida, manipulación y sustracción de información no autorizada.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
(EndPoint Detection and Response), anti-ransomware, anti-malware, entre otros).				
1.7: Revisar la recopilación, tratamiento y eliminación de la información por parte de los usuarios, documentando detalladamente los protocolos a seguir según el grado de confidencialidad de la información.	☐	☐	☐	☐
1.8: Transmitir la política de seguridad de la organización a los usuarios, publicando informaciones tales como restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos.	☐	☐	☐	☐

2: Configurar equipos servidores, aplicando los mecanismos de protección establecidos en el plan de seguridad de la organización para protegerlos de accesos indebidos.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Configurar los servicios que ofrece el servidor (correo, web, servicio de impresión, entre otros), haciendo uso de los entornos específicos de cada servicio, estableciendo valores a sus parámetros de configuración, conforme a las medidas de bastionado establecidas por la organización, si procede.	☐	☐	☐	☐
2.2: Desactivar los servicios del sistema operativo preinstalados no necesarios (NFS, DNS, entre otros) en el servidor, borrándolos del sistema, garantizando así que no pueden ser activados.	☐	☐	☐	☐
2.3: Asegurar la comunicación con el servidor (autentificación de usuarios, intercambio de información), activando y configurando protocolos de seguridad tales como TLS (TLS, SSH, entre otros).	☐	☐	☐	☐
2.4: Activar los mecanismos de registro de actividad e incidencias del servidor, configurando el registro de eventos del sistema y parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).	☐	☐	☐	☐
2.5: Activar los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor, configurando y parametrizando, según el servicio, valores tales como tamaño de los ficheros logs, rotación, nivel de detalle (dirección IP, fecha, usuario, entre otros).	☐	☐	☐	☐

2: Configurar equipos servidores, aplicando los mecanismos de protección establecidos en el plan de seguridad de la organización para protegerlos de accesos indebidos.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.6: Documentar las configuraciones realizadas e incidencias producidas, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas software, entre otros).	☐	☐	☐	☐

3: Eliminar información en soportes y sistemas de almacenamiento de equipos informáticos, de forma segura, aplicando procedimientos de borrado seguro y destrucción física de información, siguiendo los procedimientos establecidos en la política de seguridad de la organización para prevenir la fuga de información confidencial.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1: Revisar los métodos de destrucción física (trituración, desintegración, incineración, entre otros), comprobando que el método utilizado se corresponde con el tipo de soporte de información.	☐	☐	☐	☐
3.2: Interpretar el protocolo de retención de datos, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.	☐	☐	☐	☐
3.3: Borrar la información almacenada en los equipos informáticos y en los soportes de información, utilizando herramientas software de borrado seguro de datos.	☐	☐	☐	☐
3.4: Registrar el procedimiento realizado, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del hardware, entre otras.	☐	☐	☐	☐

4: Aplicar medidas de seguridad física a equipos servidores, comprobando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras, siguiendo el plan de seguridad de la organización para evitar interrupciones en la prestación de servicios del sistema.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1: Revisar la ubicación física de los servidores, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.	☐	☐	☐	☐
4.2: Comprobar las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.	☐	☐	☐	☐
4.3: Revisar el Sistema de Alimentación Ininterrumpida (SAI), comprobando que está operativo a través de su sistema de alertas y reportando su estado en caso de anomalías de funcionamiento.	☐	☐	☐	☐

5: Verificar la realización de copias de seguridad, comprobando la información a respaldar, la frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
5.1: Comprobar la información del equipo informático, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde al plan de copias de seguridad.	☐	☐	☐	☐
5.2: Verificar el plan de copias de seguridad, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.	☐	☐	☐	☐
5.3: Comprobar los dispositivos de almacenamiento de copias de seguridad (cintas, discos externos, entre otros), verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en el plan de copias de seguridad.	☐	☐	☐	☐
5.4: Verificar los procedimientos de obtención y verificación de copias de seguridad, realizando pruebas de funcionamiento de los mismos.	☐	☐	☐	☐