PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP2798_2: Responder ante eventos de ciberseguridad"

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 "ECP2798_2: Responder ante eventos de ciberseguridad".

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: Implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Parametrizar los eventos de sistemas recolectados en el sistema de monitorización configurándolos de modo que se asegure que la información que proporciona es completa y precisa para facilitar su posterior tratamiento.	☐	☐	☐	☐
1.2: Implementar las reglas de tratamiento de los eventos normalizados, configurándolas en función de su severidad para la generación de alertas.	☐	☐	☐	☐
1.3: Implementar las reglas de correlación entre eventos normalizados y alertas, configurándolas en función de su severidad para la generación de alertas.	☐	☐	☐	☐
1.4: Implementar las reglas de agregación de eventos normalizados y alertas, configurando métricas y elementos para su agrupación.	☐	☐	☐	☐
1.5: Implementar los mecanismos de remediación automática o semiautomática de las alertas, de acuerdo con las condiciones de remediación.	☐	☐	☐	☐
1.6: Confeccionar la documentación de las alertas y reglas de normalización, agregación y correlación realizados, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones	☐	☐	☐	☐

1: Implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
aplicadas y archivándola para su control, trazabilidad y uso posterior.				

2: Ejecutar procedimientos frente alertas de seguridad, identificando parámetros, origen y condiciones y comunicando a las personas responsables de su gestión, para subsanar incidencias de seguridad, según normas y procedimientos de la entidad responsable.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Seleccionar el procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización, interpretando cada alerta y consultando el maestro de alertas y procedimientos establecido por la organización.	☐	☐	☐	☐
2.2: Aplicar los procedimientos de seguridad, de acuerdo con las condiciones de entorno de la alerta específica, identificando parámetros relacionados tales como direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros.	☐	☐	☐	☐
2.3: Ejecutar el escalado de alertas, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos.	☐	☐	☐	☐
2.4: Cerrar las alertas gestionadas, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación.	☐	☐	☐	☐
2.5: Confeccionar la documentación relativa a las alertas gestionadas, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.	☐	☐	☐	☐

	INDICADORES DE AUTOEVALUACIÓN

3: Colaborar en la definición de procedimientos de respuesta a alertas de seguridad, recabando requisitos, condiciones de entorno y objetivos, definiéndolos y registrándolos, para preparar la respuesta ante incidencias, según normas y procedimientos de la entidad responsable.	1	2	3	4
3.1: Marcar las alertas sin procedimiento asociado en la documentación para su uso posterior, utilizando el maestro de alertas y procedimientos operativos e identificando aquellas alertas no recogidas en él.	☐	☐	☐	☐
3.2: Recabar los requisitos, condiciones de entorno y objetivos de remediación para cada alerta, previa identificación, documentándolos según modelos internos establecidos por la organización, para su control, uso y trazabilidad.	☐	☐	☐	☐
3.3: Redactar los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable, indicando las acciones a realizar y prestando especial atención a los requisitos de continuidad de negocio definidas por la organización.	☐	☐	☐	☐
3.4: Probar los procedimientos de seguridad, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización.	☐	☐	☐	☐
3.5: Confeccionar la documentación de los procesos realizados, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.	☐	☐	☐	☐