PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

UNIDAD DE COMPETENCIA
"UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico"

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 "UC2797_2: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico".

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: Instalar sistemas de cortafuegos, 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: Asociar las zonas de seguridad a los interfaces de red del cortafuegos, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad y el resto de zonas.	☐	☐	☐	☐
1.2: Aplicar las políticas de seguridad relativas a flujos de conexiones permitidas entre redes y subredes sobre las zonas de seguridad, configurando acciones tales como: - Permitir los flujos de conexiones iniciados desde redes de mayor seguridad hacia redes de menor seguridad. - Establecer los flujos de conexiones hacia redes con vulnerabilidades intencionadas 'honeynets'. - Bloquear los flujos de conexiones iniciados desde redes de menor seguridad a redes de mayor seguridad que no estén explícitamente permitidas. - Aplicar el filtrado en el cortafuegos entre las zonas de seguridad, estableciendo las direcciones IP y puertos permitidos y no permitidos.	☐	☐	☐	☐
1.3: Aplicar la relación de políticas de filtrado de tráfico sobre los cortafuegos, estableciendo las reglas y firmas de protección específicas frente a ataques conocidos entre las zonas, tales como 'Port enumeration', 'TCP Split handshake', 'TCP SYN flood', entre otros, para protegerlas frente a ellos.	☐	☐	☐	☐
1.4: Configurar los eventos de notificación y alarmas en el cortafuegos, estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas y/o envío de paquetes de notificación mediante 'syslog', entre otros.	☐	☐	☐	☐

1: Instalar sistemas de cortafuegos, 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
1.5: Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.	☐	☐	☐	☐
1.6: 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.	☐	☐	☐	☐

2: Instalar sistemas de detección y prevención de intrusiones (IDS/IPS), 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
2.1: Conectar los cables de red de entrada y salida de datos a cada uno de los interfaces del IDS/IPS de acuerdo con especificaciones técnicas y organizativas, para posibilitar la inspección del tráfico de red.	☐	☐	☐	☐
2.2: Asociar las zonas de seguridad a los interfaces de red, estableciendo la zona de menor seguridad, generalmente conectada a Internet, la zona de mayor seguridad, la zona desmilitarizada y el resto de zonas.	☐	☐	☐	☐
2.3: Configurar los sistemas señuelo ('honeypot'), estableciendo aplicaciones y servicios trampa atractivos ante ataques, recopilando información sobre métodos y comportamientos, para la protección de la red de producción real.	☐	☐	☐	☐
2.4: Configurar las firmas de detección de ataques, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.	☐	☐	☐	☐

2: Instalar sistemas de detección y prevención de intrusiones (IDS/IPS), 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
2.5: Actualizar las firmas de detección de ataques del sistema IDS/IPS periódicamente, instalando la versión más reciente.	☐	☐	☐	☐
2.6: Configurar las reglas de detección de ataques por comportamiento, habilitándolas en el sistema IDS/IPS de acuerdo con las especificaciones técnicas y organizativas, estableciendo las acciones a realizar por el sistema IDS para cada regla relativa a la notificación y/o bloqueo de las comunicaciones, para la protección de las redes de comunicaciones.	☐	☐	☐	☐
2.7: Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.	☐	☐	☐	☐
2.8: 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.	☐	☐	☐	☐

3: Instalar sistemas de filtrado de navegación, 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
3.1: Configurar las políticas de acceso a la navegación, estableciendo las redes internas desde las que se permiten la navegación, aquellas desde las que no se permite y aquellas desde las que se permite bajo unas condiciones determinadas, para la protección de las redes.	☐	☐	☐	☐
3.2: Configurar las políticas de acceso de categorías de contenidos 'web', estableciendo aquellas categorías que son permitidas, aquellas que no son permitidas y aquellas que se permiten con cuota de acceso para la protección de la navegación web.	☐	☐	☐	☐

3: Instalar sistemas de filtrado de navegación, 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
3.3: Configurar los perfiles de acceso de navegación para cada usuario y nodo de comunicación, definiendo para cada uno de ellos las políticas de acceso de navegación, y los usuarios o direcciones IP que se deberán aplicar.	☐	☐	☐	☐
3.4: Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos 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.	☐	☐	☐	☐

4: Instalar sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM), 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
4.1: Verificar la configuración del sistema operativo para el funcionamiento de los SIEM, validando los parámetros especificados según indique la documentación técnica.	☐	☐	☐	☐
4.2: Configurar los programas de utilidad incluidos en el sistema operativo, para el uso de los SIEM, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas.	☐	☐	☐	☐
4.3: Configurar los sistemas de recolección de información en el SIEM, especificando el tipo de fuente de información, tal como sistema de protección contra el 'malware', cortafuegos, sistemas de detección de intrusión, 'honeypots', entre otros, para su registro en la herramienta.	☐	☐	☐	☐

4: Instalar sistemas de gestión de eventos de seguridad (Security Information and Event Management, SIEM), 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
4.4: Configurar las reglas de 'parseado' y normalización de eventos para cada tipo de fuente, de acuerdo con las especificaciones técnicas específicas del fabricante para cada fuente, configurando campos tales como tipo de evento, dirección IP, usuario, entre otros.	☐	☐	☐	☐
4.5: Configurar las reglas de agregado y correlación para cada caso de uso, asignando parámetros tales como ventana de agregación dirección IP u origen, usuario, tipo de evento, entre otros, para el sistema de detección de alertas del SIEM.	☐	☐	☐	☐
4.6: Configurar las reglas de generación de alertas para cada caso de uso, asignando parámetros tales como severidad, tipo de alerta, sistemas afectados, fecha y hora, entre otros, para la posterior notificación y tratamiento de la alerta.	☐	☐	☐	☐
4.7: Configurar los eventos de notificación de alertas en el SIEM, estableciendo parámetros para cada tipo de alerta y severidad, tales como correos de notificación frente a apertura de tiques en sistemas de gestión de la demanda u otros medios o sistemas válidos, para la notificación automatizada de eventos.	☐	☐	☐	☐
4.8: Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad para comprobar la funcionalidad del sistema de seguridad, siguiendo los procedimientos establecidos por la organización.	☐	☐	☐	☐
4.9: 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.	☐	☐	☐	☐

	INDICADORES DE AUTOEVALUACIÓN

5: Configurar 'software' de base y aplicaciones de sistemas informáticos para la protección del correo electrónico, verificando su funcionalidad y comprobando la seguridad siguiendo especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del sistema.	1	2	3	4
5.1: Verificar la configuración del sistema operativo para el funcionamiento de la protección del correo electrónico, comprobando los parámetros específicos que se indique en la documentación técnica del producto.	☐	☐	☐	☐
5.2: Instalar los programas de utilidad disponibles en el sistema operativo, verificando que son los mínimos que se necesitan para las funciones requeridas, configurándolos para su uso con los parámetros que se indiquen en la documentación o instrucciones de configuración.	☐	☐	☐	☐
5.3: Crear los usuarios imprescindibles para el funcionamiento del sistema, configurando el mínimo conjunto de privilegios para cada uno, de acuerdo a las especificaciones técnicas.	☐	☐	☐	☐
5.4: Activar los sistemas de encriptado de comunicaciones y correo electrónico se instalan o, en su caso, configurando claves o certificados para garantizar la privacidad de las transmisiones.	☐	☐	☐	☐
5.5: Verificar la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.	☐	☐	☐	☐
5.6: 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.	☐	☐	☐	☐

6: Instalar sistemas perimetrales de filtrado de correo electrónico, configurando los parámetros y acciones relacionados con su seguridad, según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
6.1: Configurar los sistemas de consulta de reputación de dominios y las acciones de filtrado de correo, estableciendo las fuentes sobre las que se realizarán las consultas, así como las acciones a tomar por el sistema de filtrado, tales como permitir, enviar a cuarentena, etiquetar o eliminar el correo	☐	☐	☐	☐

6: Instalar sistemas perimetrales de filtrado de correo electrónico, configurando los parámetros y acciones relacionados con su seguridad, según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
electrónico recibido.				
6.2: Proporcionar la información detallada que se requiere para la confección de los registros DNS tal como: - Relación de dominios desde los que se enviara el correo electrónico. - Direcciones IP públicas de los sistemas de correo electrónico con flujo saliente. - Configuración de la política SPF ('Sender Policy Framework'). - Relación de dominios de correo electrónico, y clave pública DKIM ('Domainkey Identified Mail') asociada. - Publicación de política del dominio en entradas DNS de DMARC (Domain-based Message Authentication, Reporting and Conformance). Al área responsable de la organización, para su implementación en los sistemas DNS, usando los canales de comunicación que se establezca en la entidad responsable.	☐	☐	☐	☐
6.3: Comprobar los umbrales de valoración de correos electrónicos para la determinación de correo sospechoso y no deseado, verificando que son aplicados sobre los sistemas de protección de correo electrónico, de acuerdo con las especificaciones técnicas recibidas.	☐	☐	☐	☐
6.4: Definir la relación de dominios, 'emails' y ficheros adjuntos que deben de tener un tratamiento especial en relación a la seguridad, configurando los sistemas de protección de correo electrónico y asignando acciones para cada elemento relacionado, tales como como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.	☐	☐	☐	☐
6.5: Definir los filtros de análisis semántico para la detección de contenido no deseado sobre los sistemas de protección de correo electrónico asignando acciones para cada uno de éstos tales como enviar a cuarentena, eliminar o etiquetar correo como sospechoso.	☐	☐	☐	☐
6.6: Definir el sistema de notificación de eventos y alertas frente a correos potencialmente peligrosos, configurando, entre otros, el servidor y el 'email' de notificación, para asegurar la comunicación de alertas del sistema al equipo responsable de la gestión del incidente.	☐	☐	☐	☐
6.7: 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.	☐	☐	☐	☐

7: Instalar sistemas perimetrales de prevención de fuga de información en el correo electrónico, configurándolos según especificaciones y procedimientos establecidos por la entidad responsable de la gestión del sistema para la protección del correo electrónico.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
7.1: Aplicar la relación de políticas de bloqueo de contenido sobre los sistemas de protección de correo electrónico, proporcionando para cada tipo de fichero o conjunto de información, el veredicto de bloquear, poner en cuarentena o notificar una violación de la política al usuario.	☐	☐	☐	☐
7.2: Configurar los usuarios encargados de los análisis de investigación de los casos, definiendo para cada uno de ellos el nivel de acceso a la información y la potestad de liberar, eliminar o retener los correos electrónicos.	☐	☐	☐	☐
7.3: Configurar los medios y sistemas de notificación de violación de las políticas de fuga de información en el sistema, verificando su funcionamiento, de acuerdo con las especificaciones técnicas recibidas.	☐	☐	☐	☐
7.4: Verificar la instalación, mediante pruebas de análisis del rendimiento, funcionales y de seguridad, para comprobar la funcionalidad del sistema de seguridad.	☐	☐	☐	☐
7.5: 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.	☐	☐	☐	☐