# PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

# CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

## ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP0959_2: Configurar la ciberseguridad en equipos finales"

### 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 "ECP0959_2: Configurar la ciberseguridad en equipos finales".

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:<br><br>NIF: | Firma: |
| Nombre y apellidos del asesor/a:<br><br>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 protección frente a 'malware' en equipos finales ('end point'), configurando los parámetros de protección, 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: Verificar la configuración del sistema operativo para el funcionamiento de la protección frente a 'malware', validando los parámetros especificados según indique la documentación técnica. | ☐ | ☐ | ☐ | ☐ |
| 1.2: Configurar los programas de utilidad incluidos en el sistema operativo para el uso de la protección frente a 'malware', previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas. | ☐ | ☐ | ☐ | ☐ |
| 1.3: Definir la seguridad relativa al 'software' no deseado en el sistema de protección frente a 'malware', asignando parámetros tales como extensiones de programas y ficheros no permitidas, carpetas de especial protección, listas blancas de ficheros, actuación frente a ficheros no firmados digitalmente o con firma desconocida o caducada, junto con el veredicto de bloquear, enviar a cuarentena, permitir o aplicación de cualquier otro filtro para proteger al sistema frente a 'malware' y 'software' no deseado. | ☐ | ☐ | ☐ | ☐ |
| 1.4: Configurar los eventos de notificación y alarmas en el sistema de protección frente a 'malware', estableciendo parámetros tales como correos de notificación frente a alertas críticas y altas, envío de paquetes de notificación mediante 'syslog' u otros. | ☐ | ☐ | ☐ | ☐ |

| ***1: Instalar sistemas de protección frente a 'malware' en equipos finales ('end point'), configurando los parámetros de protección, 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: Configurar los paquetes de instalación del 'software' cliente para equipos y servidores en el sistema, definiendo parámetros tales como versión de sistema operativo, carpetas de exclusión y/o exclusión de aplicación o programas particulares, entre otros. | ☐ | ☐ | ☐ | ☐ |
| 1.6: Configurar las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema de protección frente a 'malware', estableciendo las condiciones de actualización de todos los equipos. | ☐ | ☐ | ☐ | ☐ |
| 1.7: Configurar las opciones anti 'tampering' para la protección contra la desactivación y desinstalación del 'software' cliente de protección frente a 'malware', estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección. | ☐ | ☐ | ☐ | ☐ |
| 1.8: Verificar la instalación, mediante pruebas de análisis del rendimiento, pruebas funcionales y pruebas de seguridad, para comprobar la funcionalidad del sistema de seguridad. | ☐ | ☐ | ☐ | ☐ |
| 1.9: 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. | ☐ | ☐ | ☐ | ☐ |

| ***2: Instalar sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response'), configurando los parámetros de protección, 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: Configurar los paquetes de instalación del software cliente de protección frente a amenazas avanzadas para equipos y servidores en el sistema, definiendo parámetros tales como versión de sistema operativo, datos | ☐ | ☐ | ☐ | ☐ |

| ***2: Instalar sistemas avanzados de detección y respuesta (EDR: 'Endpoint Detection and Response'), configurando los parámetros de protección, 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 |
| específicos de suscripción a la plataforma de nube, y datos de conexión. | | | | |
| 2.2: Definir las alertas avanzadas de detección de intrusión en el sistema, estableciendo parámetros tales como tácticas, técnicas y procedimientos empleados por atacantes, programas y utilidades frecuentemente utilizadas, direcciones IP de comunicación, empleo de credenciales de administradores, entre otras, asignando la severidad de las alertas para la detección y notificando los eventos detectados por la plataforma. | ☐ | ☐ | ☐ | ☐ |
| 2.3: Configurar los eventos de notificación y alarmas en el sistema de protección frente a amenazas avanzadas, estableciendo parámetros tales como correos frente a alertas críticas y altas, envío de paquetes de notificación mediante 'syslog', entre otros. | ☐ | ☐ | ☐ | ☐ |
| 2.4: Configurar las frecuencias de escaneos activos de memoria, escaneos completos de sistemas de ficheros, actualización de políticas de seguridad y actualización de patrones de firmas en el sistema, estableciéndolas en todos los equipos. | ☐ | ☐ | ☐ | ☐ |
| 2.5: Configurar las opciones anti 'tampering' para la protección de desactivación y desinstalación del 'software' cliente de protección, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o protección de la carpeta raíz del cliente de protección. | ☐ | ☐ | ☐ | ☐ |
| 2.6: 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. | ☐ | ☐ | ☐ | ☐ |
| 2.7: 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. | ☐ | ☐ | ☐ | ☐ |

| | INDICADORES DE AUTOEVALUACIÓN |
|---|---|

| ***3: Instalar sistemas de cifrado de información en disco, 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.*** | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 3.1: Verificar la configuración del sistema operativo para el funcionamiento del cifrado, validando los parámetros especificados según indique la documentación técnica. | ☐ | ☐ | ☐ | ☐ |
| 3.2: Configurar los programas de utilidad incluidos en el sistema operativo, para el uso del cifrado, previa instalación en su caso y verificando que son únicamente los imprescindibles para la funcionalidad que se pretende, de acuerdo con especificaciones técnicas. | ☐ | ☐ | ☐ | ☐ |
| 3.3: Definir el almacenamiento seguro de información, configurándolo mediante la asignación de parámetros tales como tamaño, permisos de accesos, claves de protección para el almacenamiento de claves y certificados de descifrado de los clientes. | ☐ | ☐ | ☐ | ☐ |
| 3.4: Aplicar la relación de políticas de cifrado de información en el sistema, estableciendo parámetros tales como unidades de disco a cifrar, algoritmos de cifrado (AES, DES, entre otros), longitud de clave, secuencia de encendido de equipos, elemento de paso del cifrado (clave, certificado, pin, entre otros) o número máximo de intentos de descifrado, según cada tipo de equipo y servidor. | ☐ | ☐ | ☐ | ☐ |
| 3.5: Configurar las opciones anti 'tampering' de protección de desactivación y desinstalación del 'software' cliente de cifrado en el sistema, estableciendo parámetros de seguridad tales como contraseña o pin de desinstalación, notificación a la consola central tras desinstalación y/o desactivación del producto del cliente. | ☐ | ☐ | ☐ | ☐ |
| 3.6: 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. | ☐ | ☐ | ☐ | ☐ |
| 3.7: 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. | ☐ | ☐ | ☐ | ☐ |