# PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

**CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA**

**Código**: **IFC153_3** **NIVEL: 3**

# CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

## UNIDAD DE COMPETENCIA "UC0488_3: Detectar y responder ante incidentes de seguridad"

### 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 "UC0488_3: Detectar y responder ante incidentes de seguridad"

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. Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.*** | INDICADORES DE AUTOEVALUACIÓN | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1.1. Localizar los procedimientos de detección y respuesta de incidentes, verificando que están documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la organización. | ☐ | ☐ | ☐ | ☐ |
| 1.2. Realizar la modelización de los sistemas seleccionando los mecanismos de registro a activar, observando las alarmas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso. | ☐ | ☐ | ☐ | ☐ |
| 1.3. Verificar la activación de los mecanismos de registro del sistema, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas. | ☐ | ☐ | ☐ | ☐ |
| 1.4. Verificar la planificación de los mecanismos de análisis de registros, de forma que se garantice la detección de los comportamientos no habituales mediante un sistema de indicadores y métricas. | ☐ | ☐ | ☐ | ☐ |

| ***1. Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.*** | INDICADORES DE AUTOEVALUACIÓN | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1.5. Verificar la instalación, configuración y actualización de los sistemas de detección de intrusos en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas. | ☐ | ☐ | ☐ | ☐ |
| 1.6. Verificar los procedimientos de restauración del sistema informático para la recuperación del mismo ante un incidente grave dentro de las necesidades de la organización. | ☐ | ☐ | ☐ | ☐ |

| ***2. Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.*** | INDICADORES DE AUTOEVALUACIÓN | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 2.1. Analizar las herramientas utilizadas para detectar intrusiones para determinar que no han sido comprometidas ni afectadas por programas maliciosos. | ☐ | ☐ | ☐ | ☐ |
| 2.2. Analizar los parámetros de funcionamiento sospechoso con herramientas específicas según la normativa de seguridad. | ☐ | ☐ | ☐ | ☐ |
| 2.3. Verificar los componentes software del sistema periódicamente en lo que respecta a su integridad usando programas específicos. | ☐ | ☐ | ☐ | ☐ |
| 2.4. Verificar el funcionamiento de los dispositivos de protección física por medio de pruebas según las normas de la organización y/o normativa aplicable de seguridad. | ☐ | ☐ | ☐ | ☐ |
| 2.5. Recoger los sucesos y signos extraños que pudieran considerarse una alerta en el informe para su posterior análisis en función de la gravedad de los mismos y la política de la organización. | ☐ | ☐ | ☐ | ☐ |

| ***3. Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la organización.*** | INDICADORES DE AUTOEVALUACIÓN | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 3.1. Activar los procedimientos recogidos en los protocolos de la normativa de seguridad de la organización ante la detección de un incidente de seguridad. | ☐ | ☐ | ☐ | ☐ |
| 3.2. Recoger la información para el análisis forense del sistema vulnerado una vez aislado el sistema según los procedimientos de las normas de seguridad de la organización y/o normativa aplicable. | ☐ | ☐ | ☐ | ☐ |
| 3.3. Analizar el sistema atacado mediante herramientas de detección de intrusos según los procedimientos de seguridad de la organización. | ☐ | ☐ | ☐ | ☐ |
| 3.4. Contener la intrusión mediante la aplicación de las medidas establecidas en las normas de seguridad de la organización y aquellas extraordinarias necesarias aunque no estén previamente planificadas. | ☐ | ☐ | ☐ | ☐ |
| 3.5. Realizar la documentación del incidente para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido. | ☐ | ☐ | ☐ | ☐ |
| 3.6. Planificar las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado a partir de la determinación de los daños causados, cumpliendo los criterios de calidad de servicio y el plan de explotación de la organización. | ☐ | ☐ | ☐ | ☐ |