PROGRAMA FORMATIVO DE LA ESPECIALIDAD FORMATIVA

DESARROLLO SEGURO

IFCD060PO

PROGRAMAS DE FORMACIÓN DIRIGIDOS PRIORITARIAMENTE A TRABAJADORES OCUPADOS

5 de abril de 2018

PROGRAMA DE LA ESPECIALIDAD FORMATIVA:

DESARROLLO SEGURO

DATOS GENERALES DE LA ESPECIALIDAD FORMATIVA

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES

Área Profesional: DESARROLLO

2. Denominación: DESARROLLO SEGURO

3. Código: **IFCD060PO**

4. Objetivo General: Sensibilizar en la importancia del cumplimiento de medidas de seguridad en los programas que se desarrollen, y asegurar que cumplen con los objetivos de seguridad informática: integridad, autenticidad, confidencialidad, disponibilidad y no repudio.

5. Número de participantes: **-**

6. Duración:

Horas totales: 25 Modalidad: Presencial

Distribución de horas:

Presencial:..... 25

Teleformación:..... 0

7. Requisitos mínimos de espacios, instalaciones y equipamiento:

7.1 Espacio formativo:

AULA POLIVALENTE:
El aula contará con las instalaciones y equipos de trabajo suficientes para el desarrollo de la acción formativa.
- Superficie: El aula deberá contar con un mínimo de 2m2 por alumno.
- Iluminación: luz natural y artificial que cumpla los niveles mínimos preceptivos.
- Ventilación: Climatización apropiada.
- Acondicionamiento eléctrico de acuerdo a las Normas Electrotécnicas de Baja Tensión y otras normas de aplicación.
- Aseos y servicios higiénicos sanitarios en número adecuado.
- Condiciones higiénicas, acústicas y de habitabilidad y seguridad, exigidas por la legislación vigente.
- Adaptabilidad: en el caso de que la formación se dirija a personas con discapacidad dispondrá de las adaptaciones y los ajustes razonables para asegurar la participación en condiciones de igualdad.
- PRL: cumple con los requisitos exigidos en materia de prevención de riesgos laborales

Cada espacio estará equipado con mobiliario docente adecuado al número de alumnos, así mismo constará de las instalaciones y equipos de trabajo suficientes para el desarrollo del curso.

7.2 Equipamientos:

Se contará con el equipamiento suficiente para el desarrollo de la acción formativa.
- Pizarra.
- Rotafolios.
- Material de aula.
- Medios audiovisuales.
- Mesa y silla para formador.
- Mesa y silla para alumnos.
- Hardware y Software necesarios para la impartición de la formación.
- Conexión a Internet.

Se entregará a los participantes los manuales y el material didáctico necesarios para el adecuado desarrollo de la acción formativa

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.
En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

8. Requisitos necesarios para el ejercicio profesional:

(Este epígrafe sólo se cumplimentará si existen requisitos legales para el ejercicio de la profesión)

9. Requisitos oficiales de los centros:

(Este epígrafe sólo se cumplimentará si para la impartición de la formación existe algún requisito de homologación / autorización del centro por parte de otra administración competente.

10. CONTENIDOS FORMATIVOS:

1. FUNDAMENTOS DE PROGRAMACION SEGURA
1.1. Contexto
1.2. Secciones críticas de una aplicación:
1.2.1. Motivos de seguridad y consecuencias por falta de seguridad
1.2.2. Autenticación
1.2.3. Autorización
1.2.4. Gestión de sesiones
1.2.5. Validación de entradas y Riesgos de inyección
1.2.6. Controles criptográficos
1.2.7. Registro de eventos
1.2.8. Funcionalidades
1.2.9. Gestión de memoria
1.2.10. Gestión de la información sensible

2. INTRODUCCIÓN: SEGURIDAD EN JAVA
2.1. Principios básicos: Encapsulación, Mutabilidad, Serialización
2.2. Clonación.
2.3. 12 reglas de oro.
2.4. Descompiladores y ofuscadores

3. ERRORES DE INYECCIÓN
3.1. Inyección en servidor.
3.1.1. Inyección de comandos del SO.
3.1.2. Inyección SQL y Blind SQL Injection.
3.1.3. Inyección Xpath.
3.1.4. Redirecciones y reenvíos no validados.

3.2. Inyección en cliente.
3.2.1. Inyección HTML.
3.2.2. Cross Site Scripting (XSS).
3.2.3. Cross Frame Scripting (XFS).
3.2.4. Cross Site Request Forgery (CSRF).
3.2.5. HTTP Response Split.

4. CONTROL DE ACCESO A RECURSOS
4.1. Condiciones de carrera (race conditions = RC).

5. AUTENTIFICACIÓN
5.1. Autenticación/Autorización.
5.2. Http Básica y avanzada (HTTP Basic, HTTP Digest).
5.3. Autenticación HTTP basada en formulario.
5.4. Certificado (HTTPS Client).

6. CONTROL DE ACCESOS
6.1. Control de acceso declarativo.
6.2. Control de acceso programático

7. CIFRADO
7.1. Encriptación.

7.2. Keystores/Trustores.
7.3. Gestión programática en java.
7.4. SSL.
7.5. JSSE.

8. CONTROL DE SESIONES
8.1. Id de sesión.
8.2. Gestión de sesiones.
8.3. Session Hijacking.
8.4. Session Fixation.

9. FUGA DE DATOS
9.1. Control de autorización insuficiente.
9.2. Revelación de información en mensajes de error.
9.2.1. Path Traversal.