



**Curso**

# **Introducción a la Programación Segura ante Ciberataques**

**20 Horas**

A Coruña, 26, 27 de Noviembre y 3, 4  
de Diciembre de 2018

---

[www.vitaedigital.com](http://www.vitaedigital.com)



**Vitae**

# INTRODUCCIÓN

En este Curso los y las asistentes podrán adquirir los conocimientos básicos necesarios para el desarrollo seguro de aplicaciones.

El objetivo principal del curso consiste en impartir formación a un grupo de desarrolladores de aplicaciones tanto de Backend con Java como de Frontend con Angular y JavaScript.

Se pretende impartir una formación en materia de desarrollo seguro que partiendo de un nivel introductorio facilite a los desarrolladores los conocimientos para poder implementar aplicaciones siguiendo los estándares de desarrollo seguro.

La formación inicia a los desarrolladores en la metodología y el ciclo de desarrollo seguro.

Posteriormente, se aborda el proyecto OWASP así como el ranking de los 10 tipos de vulnerabilidades más habituales en el desarrollo de software.

Se detalla técnicamente cada vulnerabilidad, los riesgos que representa, las técnicas de explotación así como las contramedidas a aplicar.

Posteriormente, se tratan en detalle las buenas prácticas de desarrollo orientadas a Java y JavaScript con Angular, así como los diferentes frameworks e integración con S-SDLC.

## Duración

Este Curso tendrá una duración de 20 horas en cuatro sesiones de 5 horas.

# TEMARIO

## **Módulo 0.- INTRODUCCIÓN**

- 1.- Introducción a la seguridad de aplicaciones
- 2.- Vulnerabilidades principales
- 3.- Ejemplos prácticos de problemas en aplicativos reales
- 4.- Introducción a la metodología de auditoría y pentesting en aplicaciones
- 5.- Identificando vulnerabilidades desde el origen

## **Módulo 1.- CICLO DE DESARROLLO SEGURO**

- 1.- Introducción S-SDLC (Secure Software Development Life Cycle)
- 2.- Modelos
  - 2.1.- CbyC, TSP Secure
  - 2.2.- Microsoft Security Development Lifecycle
  - 2.3.- NIST 800-64
  - 2.4.- OWASP CLASP (Comprehensive, Lightweight Application Security Process)
  - 2.5.- BSIMM (Building Security In Maturity Model)
- 3.- OWASP SAMM (SAMM maturity model)
- 4.- Agile con Microsoft y Cigital

## ❑ Módulo 2.- OWASP 2017 (Open Web Application Security Project) “TOP TEN”

- 1.- Injection
- 2.- Broken Authentication and Session Management
- 3.- Sensitive Data Exposure
- 4.- XML External Entities (XXE)
- 5.- Broken Access Control
- 6.- Security Misconfiguration
- 7.- Cross-Site Scripting (XSS)
- 8.- Insecure Deserialization
- 9.- Using Components with Known Vulnerabilities
- 10.- Insufficient logging & monitoring

## ❑ Módulo 3.- SECURE CODING

- 1.- Secure Coding Best Practices (Java)
- 2.- Frameworks e integración con S-SDLC
- 3.- Librerías para la validación de datos de entrada en Java
- 4.- Spring Security
- 5.- Herramientas para análisis de código estático
- 6.- Vulnerabilidades en aplicaciones web 2.0/3.0
- 7.- Vulnerabilidades en aplicaciones Angular.js

## INFORMACIÓN DEL CURSO

 Duración	20 Horas Lectivas
 Lugar	A Coruña
 Fechas	Lunes 26, Martes 27 de Noviembre y Lunes 3, Martes 4 de Diciembre de 2018
 Horario	De 16:00 a 21:00 horas
 Donde	Hotel Attica 21 Coruña C/ Enrique Mariñas, 34 Tel: 981 179 299 Parking Gratuito en el mismo Hotel

## FORMADORES

### Deepak Daswani



**Deepak Daswani** es un experto ampliamente reconocido a nivel internacional en materia de hacking ético y ciberseguridad que ha prestado servicios en entidades de referencia en el sector como INCIBE o la Firma Multinacional Deloitte.

Es ponente habitual en las principales conferencias del sector y colaborador asiduo de diversos medios de comunicación a nivel autonómico en Canarias, nacional e internacional.

Se incluye un anexo curricular, incluyendo referencias de clientes y entidades con las que ha colaborado.

Ha formado y asesorado a Clientes como DELOITTE, ROCHE, JHONSSON & JHONSSON, ORANGE, MAPFRE, etc...

## Daniel Echeverri



**Daniel Echeverri es Licenciado en Ingeniería de Sistemas y Master en Software Libre por la UOC.**

Durante 7 años trabajó en proyectos de desarrollo para importantes consultoras hasta que en 2011 se incorpora a The Hacker Way para realizar proyectos más enfocados a la Seguridad Informática y el Pentesting.

Posee las certificaciones en Seguridad SPSE, CSPA, OSCP.

En la actualidad está centrado en la labor como formador y en la divulgación mediante libros, conferencias e investigaciones.

Ha formador y asesorado a empresas y organismos como Accenture, Ibermática, PLEXUS, INCIBE, etc...



## CONDICIONES ECONÓMICAS

 <b>Tarifa por Asistente</b>	<b>290 €</b> <b>(Cuota bonificable por la Fundación Tripatita)</b>
 <b>Tarifa por asistente a partir de dos personas de la misma empresa u organización</b>	<b>250 €</b> <b>(Cuota bonificable por la Fundación Tripatita)</b>
<b>Forma de Pago:</b> <b>Por transferencia al finalizar el curso a la recepción de la factura</b> <b>Se añadirá el 21% de IVA</b>	<b>Inscripción: Marcos Carbonell</b> <b><a href="mailto:marcos@vitaedigital.com">marcos@vitaedigital.com</a></b> <b>Tlf : 986 47 21 01</b> <b>637 82 02 57</b>

Plazas limitadas, reserva de plazas por riguroso orden de inscripción