

# Seguridad de aplicaciones basadas en tecnología Java. (JSG-150)

## Objetivos:

- Conocer el modelo de seguridad de Java 2, así como las vulnerabilidades y medidas a tomar para hacer las aplicaciones web seguras.

## Dirigido:

- Desarrolladores y analistas que deseen tener una visión global de los distintos aspectos que ofrece la tecnología Java, en cuanto a seguridad de aplicaciones se refiere.

## Requisitos iniciales:

- Conocimientos programación Java en general y de desarrollo de aplicaciones basadas en componentes Web.

## Contenidos:

- Introducción.
- Criptografía en java:
  - × Introducción.
  - × Servicios criptográficos.
  - × Proveedores.
  - × Clases motor (engine classes).
  - × Claves criptográficas.
  - × Encriptación.
  - × Message digest.
  - × Firma digital.
- Infraestructura PKI con java:
  - × ¿Qué es un certificado?
  - × Autoridades certificadoras.
  - × X.509.
  - × ¿Qué aplicaciones usan certificados?.
  - × Listas de anulación de certificados (crls).
  - × ¿Cómo se obtiene un certificado?
  - × ¿Qué API de java se usa para acceder y gestionar certificados?
  - × Key and certificate management tool (keytool).
- Control de acceso :
  - × Evolución del modelo de seguridad.
  - × Security manager.
  - × Ficheros de políticas de seguridad (policy files).
  - × Java authentication and authorization service (jaas).
- Aplicaciones con java SSL:
  - × Panorámica de SSL.
  - × Extensión de socket seguro de java (JSSE).
  - × Keystores.
  - × Truststores.
  - × RMI sobre SSL.
- Seguridad en Aplicaciones Web:
  - × Seguridad declarativa en aplicaciones web.
  - × Seguridad programática en aplicaciones web.
  - × Configuración de aspectos de seguridad en apache tomcat.
  - × Configuración de aspectos de seguridad en oracle ias 10g.
  - × Principales vulnerabilidades para las aplicaciones web.
  - × Dimensiones de la seguridad web.
  - × Seguridad en los mensajes.
  - × Xml encryption: confidencialidad en los mensajes.
  - × Xml signature: integridad, autenticación y no repudio en los mensajes.
  - × WS-security: extensión de SOAP para seguridad en mensajes.
  - × Certificados x.509.
  - × Firma.
  - × Cifrado.
  - × Especificaciones de JCP.