# Fundamentos de Seguridad para Servicios, Microservicios y SOA

Código: ARC-318

**Propuesta de Valor:** ARCITURA

**Duración:** 10 Horas

Este curso proporciona técnicas, patrones y tecnologías de industria esenciales que atañen al establecimiento de controles de seguridad y arquitecturas de seguridad para servicios, microservicios y soluciones orientadas a servicios.

## AUDIENCIA

- Perfiles técnicos que tienen conocimientos de programación y desarrollo de software.
- Recién graduados.

## PRE REQUISITOS

- Se recomienda realizar el curso: Conceptos de Tecnología de Servicios.

## OBJETIVOS

- Consideraciones de seguridad SOA para arquitecturas de composición y servicio.
- Implicaciones de seguridad de los principios de orientación al servicio.
- Confianza, reclamaciones, tokens, identidad, autenticación, autorización, transporte y seguridad de la capa de mensajes.
- Cifrado, hashing, firmas digitales, gestión de identidades y accesos (IAM).
- Infraestructura de clave pública (PKI), certificados digitales, autoridades de certificación, inicio de sesión único (SSO).
- Servicios REST y estándares industriales JSON.
- Marco de cifrado y firma de objetos JavaScript (JOSE), OAuth2.
- Autenticación HTTP básica y Digest, clave API, JWT con certificados X.509.
- Patrones de seguridad de interacción de servicios (confidencialidad de los datos, autenticación del origen de los datos,


Copyright © Cognos 2020 Todos los derechos reservados.

autenticación directa, autenticación intermediada).

- Servicios web y estándares de la industria XML.
- Cifrado XML, Firma XML, WS-Security, Perfiles de token, SAML.
- Consideraciones de seguridad de microservicios.
- Implementación de seguridad SOA y seguridad orientada a servicios.

## CERTIFICACIÓN DISPONIBLE

- La ruta de Especialista en Seguridad de Servicios se compone de los Módulos 1, 2, 18, 19 y 20 de SOACP.

## CONTENIDO

### 1. ESTÁNDARES DE LA INDUSTRIA PARA SERVICIOS WEB

1.1. CIFRADO XML
1.2. FIRMA XML
1.3. CANONICALIZACIÓN
1.4. TRANSFORMACIÓN DE DESCIFRADO PARA FIRMA XML
1.5. WS-SECURITY
1.6. LENGUAJE DE MARCADO DE ASERCIÓN DE SEGURIDAD (SAML)

### 2. CONCEPTOS DE SEGURIDAD

2.1. CONFIANZA
2.2. RECLAMACIÓN
2.3. TOKENS
2.4. IDENTIFICACIÓN
2.5. AUTENTICACIÓN
2.6. AUTORIZACIÓN
2.7. CONFIDENCIALIDAD
2.8. INTEGRIDAD
2.9. NO REPUDIO
2.10. TRANSPORT LAYER SECURITY
2.11. SEGURIDAD DE LA CAPA DE MENSAJES

### 3. MECANISMOS DE SEGURIDAD

3.1. CIFRADO
3.2. HASH
3.3. FIRMAS DIGITALES
3.4. GESTIÓN DE IDENTIFICACIONES Y ACCESOS (IAM)
3.5. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)
3.6. CERTIFICADOS DIGITALES
3.7. AUTORIDAD CERTIFICADORA (CA)
3.8. INICIO DE SESIÓN ÚNICO (SSO)

### 4. PATRONES DE SEGURIDAD DE INTERACCIÓN DE SERVICIOS


Copyright © Cognos 2020 Todos los derechos reservados.

4.1. CONFIDENCIALIDAD DE LOS DATOS

4.2. AUTENTICACIÓN DE ORIGEN DE DATOS

4.3. AUTENTICACIÓN DIRECTA

4.4. AUTENTICACIÓN INTERMEDIADA

### 5. TIPOS DE REGLAS DE CONTROL DE ACCESO

5.1. ACCIÓN

5.2. IDENTIDAD

5.3. RECURSO

5.4. AMBIENTE

### 6. ESTÁNDARES DE LA INDUSTRIA PARA SERVICIOS REST

6.1. JWE

6.2. JWS

6.3. JWT

6.4. OAUTH 2.0

6.5. CONEXIÓN OPENID

6.6. TLS

6.7. HTTPS

## BENEFICIOS

- Al finalizar el curso, tendrás conocimientos en seguridad y modelo arquitectónico orientado a servicios.

Cognos tiene un único cronograma virtual para todos los países de habla Hispana. Los cursos presenciales están disponibles a través de los centros franquiciados.
Copyright © Cognos 2020 Todos los derechos reservados.