



ITAC WS-Guardian® » plataforma de seguridad y gobernabilidad SOA que permite administrar el ciclo de vida de los servicios y habilitar mecanismos de seguridad para la exposición y consumo de los mismos.

Seguridad y gobernabilidad para arquitecturas orientadas a servicios – SOA

Disponible como Virtual o Hardware Appliance



BENEFICIOS

- » Administra la seguridad en su entorno de ejecución SOA, desacoplando el modelo de seguridad del proceso de desarrollo, permitiendo a los desarrolladores hacer lo que mejor saben hacer: crear nuevas funcionalidades de SOA, sin ningún tipo de preocupación en materia de seguridad.
- » Fortalece el crecimiento acelerado, ordenado, seguro y sostenible de su infraestructura SOA.
- » Flexibiliza y facilita la configuración para el acceso seguro a los servicios SOA ofrecidos por la organización.
- » Protege la información sensible intercambiada con sus socios de negocio.
- » Gobierno y cumplimiento de las normativas de seguridad de la información.
- » Disminución de carga operativa en el proceso de administración de llaves, llaveros y certificados X.509.
- » Mejora la productividad en el desarrollo de nuevas funcionalidades requeridas por el negocio.
- » Asegura la confidencialidad, integridad y no repudio para la invocación de servicios SOA.
- » Centraliza la gobernabilidad de entornos orientados a servicios.
- » Aseguramiento de servicios SOA mediante la aplicación granular de filtros de seguridad.

CARACTERÍSTICAS TÉCNICAS Y FUNCIONALES

- » Aplicación de reglas sofisticadas de seguridad bidireccionales.
 - » Gestión de llaveros y llaves para ser usadas en cifrado, firma y verificación de mensajes o campos XML individuales.
 - » Control de acceso a los servicios expuestos por la organización basado en filtros de seguridad (calendario, horario, direcciones IP, etc.)
 - » Generación automática de documentación de los servicios en formato PDF.
 - » Políticas de seguridad semánticas avanzadas que reflejan cómo son utilizados los servicios SOA por la organización.
 - » Verificación de análisis de impacto en el momento en que las políticas de seguridad son modificadas.
 - » Integración con gestores de identidad mediante la autenticación contra sistemas LDAP.
 - » Reportes detallados de las actividades de los usuarios y uso de los servicios.
- Estándares soportados:**
- » Open WS Security standards (OASIS WS-Security 1.0/1.1, OASIS X.509, W3C XML encryption and XML signatures, WS-I BPP 1.0/1.1, SOAP with Attachments)
 - » Web Services Protocols (SOAP 1.1 & 1.2)
 - » Service Governance (WSDL 1.2, WS-Policy 1.2, UDDI)

Servicios publicados en un bus de servicios empresarial (ESB)



Servicios publicados de manera distribuida en cada sistema backend



Cuando en la arquitectura SOA está involucrado algún Enterprise Service Bus (ESB) cualquiera que sea el fabricante (Oracle, IBM, Microsoft), **ITAC WS-Guardian®** actúa como un protector de los servicios expuestos, mitigando el riesgo latente de posibles ataques maliciosos.

En este escenario, **ITAC WS-Guardian®** ayuda a asegurar los servicios que ofrece el ESB. La tarea de aseguramiento de los servicios es delegada en **ITAC WS-Guardian®** de forma que los servicios sólo se encarguen de resolver la lógica de negocio y no la lógica de seguridad.

En escenarios en los cuales la infraestructura SOA no haga uso del Enterprise Service Bus como parte de su arquitectura, **ITAC WS-Guardian®** puede interactuar directamente con los servicios o aplicaciones desplegadas en otros dominios.

Para este escenario, **ITAC WS-Guardian®** ofrece todas las posibilidades de enrutamiento inteligente del tráfico de peticiones hacia los diferentes dominios corporativos sin afectar la seguridad y escalabilidad de los mismos.

Filtros de seguridad



ITAC WS-Guardian® ofrece una gran variedad de filtros granulares de seguridad para proteger el tráfico de las peticiones.

ITAC WS-Guardian® cuenta con una serie de filtros granulares y condicionales, específicos para cifrado de mensajes, integridad de información mediante firmas digitales y control de flujo de peticiones por restricciones de direcciones IP, calendarios y horarios.

Así mismo **ITAC WS-Guardian®** puede aplicar filtros condicionales compuestos con base en el contenido del mensaje SOAP.

Gobernabilidad



Uno de los principales retos al establecer una infraestructura SOA es como controlar el ciclo de vida de los servicios generados.

ITAC WS-Guardian® ha sido diseñado para que toda organización pueda administrar de manera centralizada las políticas de seguridad, gobernar la arquitectura SOA y solucionar los inconvenientes comunes como: inventario de servicios, control de versiones, análisis de impacto en la aplicación de políticas y filtros de seguridad, y documentación.



Use su móvil para escanear el código QR.

www.wsguardian.co / info@wsguardian.co



Teléfono: (+57) 1 744-4822
info@itac.co
 Bogotá - Colombia