

Seguridad Declarativa WS INDI (Acceso por usuario /contraseña)

GERENCIA DE INFORMÁTICA

JOSEFA VALCÁRCEL, 44
28027-MADRID



Índice General

1. INTRODUCCIÓN.....	3
1.1 DESCRIPCIÓN GENERAL.....	3
1.1 ALCANCE.....	3
2. SEGURIDAD DECLARATIVA.....	4
2.1 ALTA DEL KEYSTORE QUE USA LA APLICACIÓN EN LA CONSOLA DE WEBSHERE.....	4
2.2 CONFIGURACIÓN DE LOS ENLACES DE SEGURIDAD DE LOS CLIENTES DE SERVICIOS WEB.....	4
2.3 MODIFICAR EL CERTIFICADO DE ENLACE DE SEGURIDAD.....	11

1. Introducción

1.1 Descripción general

En estos apartados se indicarán los pasos a seguir para llevar a cabo la configuración de la seguridad declarativa para las invocaciones a la aplicación INDI, mediante texto y capturas de pantalla. Se recomienda revisar la guía de desarrollo donde se incluyen normas de obligado cumplimiento referentes a esta configuración.

1.1 Alcance

En este documento se incluye toda la información necesaria para poder realizar la seguridad a través de la consola administrativa de WebSphere para la aplicación INDI.

2. Seguridad Declarativa.

2.1 Alta del *keystore* que usa la aplicación en la consola de *Websphere*.

N/A

2.2 Configuración de los enlaces de seguridad de los clientes de servicios web

Debemos importar la siguiente política de seguridad para poder invocar a los servicios web a consumir de INDI.

- Conjunto de Políticas de Aplicación

Servicios > Conjuntos de Políticas > Conjunto de Políticas de Aplicación

Esto se puede realizar de dos maneras:

- 1) Importando el conjunto de políticas de aplicación *WSS Security Indi.zip* proporcionado en el kit de integración correspondiente, o bien, solicitándolo al equipo de desarrollo.



Ver: Todas las tareas

- Servicio
- Solicitudes pendientes
- Servidores
- Solicitudes
- Servicios
 - Propiedades de servicios
 - Clasificación de servicios
 - Conjuntos de políticas
 - Conjuntos de políticas de aplicación**
 - Conjuntos de políticas de seguridad
 - Examen del conjunto de políticas por omisión
 - Examen generalizado del conjunto de políticas del inventario
 - Examen generalizado del conjunto de políticas del cliente
- Servicio de confianza
 - Examen del nivel de seguridad
 - Estado de mensajes de texto
- Recurso
- Seguridad
- Examen
- Administración del sistema
- Operación y gestión
- Supervisión y ajuste
- Resolución de problemas
- Integración de servicios
- OTRI

Conjuntos de políticas de aplicación

Utilice este panel para gestionar o importar conjuntos de políticas de aplicación. Los conjuntos de políticas de aplicación definen las políticas de calidad del servicio para los mensajes relacionados con la empresa definidos en el WSDL. También hay disponibles conjuntos de políticas de aplicación adicionales por omisión. Puede importar estos conjuntos de políticas desde el repositorio por omisión con el botón Importar. Los conjuntos de políticas por omisión no son editables, pero puede copiarlos y modificarlos para adaptarlos a sus necesidades.

☒ Preferencias

Seleccionar	Nombre	Editable	Descripción
<input type="checkbox"/>	Kerberos V5 HTTPS default	No editable	Políticas: WSSECURITY, SSLTransport, WSAddressing <ul style="list-style-type: none">Autenticación de mensajes: utilización de señal Kerberos V5Seguridad de transporte: utilización de SSL para HTTPSeguir las especificaciones del perfil de señal de Kerberos OASIS
<input type="checkbox"/>	LTPA WSSECURITY default	No editable	Políticas: WSSECURITY, WSAddressing <ul style="list-style-type: none">Integridad de mensajes: firmar digitalmente el cuerpo, la indicación de la hora, las cabeceras de direccionamiento y la señal LTPA utilizando la firma digital RSAConfidencialidad de mensajes: cifrar cuerpo, firma y señal LTPA utilizando el cifrado RSAAutenticación de mensajes: utilización de señal LTPA
<input type="checkbox"/>	SSL WSTransaction	No editable	Políticas: WSTransaction, SSLTransport <ul style="list-style-type: none">Integridad de transacciones: propagación de contexto WS-AtomicTransaction y WS-BusinessActivity utilizando SSL
<input type="checkbox"/>	Username SecureConversation	No editable	Políticas: WSSECURITY, WSAddressing <ul style="list-style-type: none">Integridad de mensajes: firmar digitalmente el cuerpo, la indicación de la hora, la confirmación de firma, las cabeceras de direccionamiento y la señal de nombre de usuarioConfidencialidad de mensajes: cifrar cuerpo, firma, confirmación de firma y señal de nombre de usuarioAutenticación de mensajes: utilización de señal de nombre de usuarioSeguir la especificación WS-SecureConversation
<input type="checkbox"/>	Username WSSECURITY default	No editable	Políticas: WSSECURITY, WSAddressing <ul style="list-style-type: none">Integridad de mensajes: firmar digitalmente el cuerpo, la indicación de la hora, las cabeceras de direccionamiento y la señal de nombre de usuario utilizando el cifrado RSAConfidencialidad de mensajes: cifrar cuerpo, firma y señal de nombre de usuario utilizando el cifrado RSAAutenticación de mensajes: utilización de señal de nombre de usuario
<input type="checkbox"/>	WS-1.ESB	No editable	Políticas: WSReliableMessaging, WSSECURITY, WSAddressing <ul style="list-style-type: none">Mensajería fiable no persistente sin gestiones para servidores únicosIntegridad de mensajes: firmar digitalmente el cuerpo, la indicación de la hora, la confirmación de firma, las cabeceras de direccionamiento y las cabeceras de mensajería fiableConfidencialidad de mensajes: cifrar cuerpo, firma y confirmación de firmaSeguir la especificación WS-SecureConversation
<input type="checkbox"/>	WSAddressing default	No editable	Políticas: WSAddressing <ul style="list-style-type: none">Direccionamiento: utilización de WS-Addressing uniforme e independiente del transporte
<input type="checkbox"/>	WSHTTP3 default	No editable	Políticas: HTTPTransport, SSLTransport, WSAddressing <ul style="list-style-type: none">Seguridad de transporte: utilización de SSL para HTTP
<input type="checkbox"/>	WSReliableMessaging persistent	No editable	Políticas: WSAddressing, WSReliableMessaging <ul style="list-style-type: none">Envío fiable: WS-ReliableMessaging y almacenamiento persistenteDireccionamiento: utilización de WS-Addressing uniforme e independiente del transporte
<input type="checkbox"/>	WSSECURITY In4	Editable	
<input type="checkbox"/>	WSSECURITY In20	Editable	

2) Creando el conjunto de políticas de la aplicación de la siguiente manera.

Nuevo

Conjuntos de políticas de aplicación

Utilice este panel para gestionar o importar conjuntos de políticas de aplicación. Los conjuntos de políticas de aplicación definen las políticas de calidad del servicio para los mensajes relacionados con la empresa definidos en el WSDL. También hay disponibles conjuntos de políticas de aplicación adicionales por omisión. Puede importar estos conjuntos de políticas desde el repositorio por omisión con el botón Importar. Los conjuntos de políticas por omisión no son editables, pero puede copiarlos y modificarlos para adaptarlos a sus necesidades.

☒ Preferencias

- Propiedades generales → Nombre
- Políticas → Añadir → WS Security



Conjuntos de políticas de aplicación

[Conjuntos de políticas de aplicación](#) > **Nuevo**

Utilice esta página para configurar un conjunto de políticas.

Propiedades generales

* Nombre

Descripción

Políticas

Estado	Descripción
<input type="checkbox"/>	WS-Addressing
<input type="checkbox"/>	Transporte SSL
<input type="checkbox"/>	WS-Transaction
<input type="checkbox"/>	Transporte JMS
<input type="checkbox"/>	Transporte HTTP
<input checked="" type="checkbox"/>	WS-Security
<input type="checkbox"/>	WS-ReliableMessaging

WS Security → Política principal → Políticas de señal de petición → Política de señal de nombre de usuario de mensaje de petición

- Nombre de señal de nombre de usuario
- Versión de WS-Security → WS-Security 1.0

Conjuntos de políticas de aplicación

[Conjuntos de políticas de aplicación](#) > [WSS Security Prueba](#) > [WS-Security](#) > [Política principal](#) > [Políticas de señal de petición](#) > [Política de señal de nombre de usuario de mensaje de petición](#)

Se pueden definir políticas que especifiquen qué tipos de señales de seguridad están soportados así como propiedades para el tipo de señal.

* Nombre de señal de nombre de usuario

Versión de WS-Security

- Enlaces generales de conjunto de políticas del cliente

Servicios > Conjuntos de Políticas > Enlaces generales de conjunto de políticas del cliente

Esto se puede realizar de dos maneras:

1) Importando el enlace del conjunto de políticas *Indi WS-Security.zip* proporcionado en el kit de integración correspondiente, o bien, solicitándolo al equipo de desarrollo.

Enlaces generales de conjunto de políticas del cliente

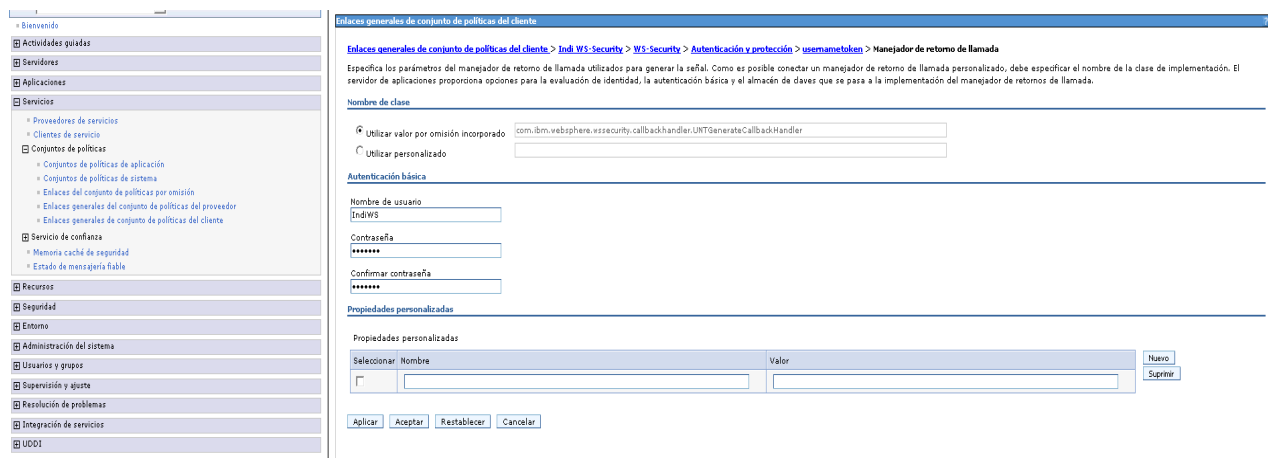
Utilice esta página para crear, copiar y gestionar enlaces del conjunto de políticas. Estos enlaces proporcionan configuración específica del sistema y se pueden reutilizar entre las conexiones del conjunto de políticas. Crear un ámbito para un enlace en un dominio de seguridad restringe las opciones de configuración a aquellas aplicables al dominio y limita el uso del enlace al dominio especificado.

Seleccionar	Nombre	Dominio de seguridad	Descripción
<input type="checkbox"/>	Client.Laetale	Seguridad global	Se trata de un ejemplo del enlace general del conjunto de políticas del cliente y sólo está disponible como punto de partida para la configuración de enlaces del cliente. Antes de utilizarlo en un entorno de producción, este enlace se debe modificar de forma que satisfaga sus requisitos.
<input type="checkbox"/>	Indi WS-Security	Seguridad global	
<input type="checkbox"/>	Inst WS-Security	Seguridad global	
<input type="checkbox"/>	Base WS-Security	Seguridad global	Conjunto de políticas de clientes de servicio web de REAP
Total 4			

En este punto deberemos configurar un usuario técnico para poder autenticarnos contra Datapower. En nuestro ejemplo tenemos puesto el usuario *IndiWS* que es el usuario creado para el entorno de Desarrollo, pero Sistemas deberá aportar el que corresponda en función del entorno (se deberá realizar una consulta a Sistemas para obtener el usuario técnico del entorno de Preproducción).

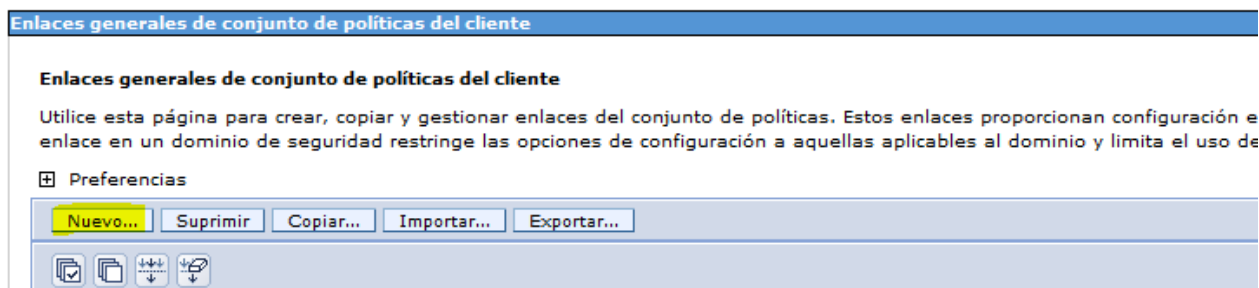
El cambio se deberá realizar en la siguiente pantalla:

Enlaces generales de conjunto de políticas del cliente > Indi WS-Security > WS-Security > Autenticación y protección > usernametoken > Manejador de retorno de llamada



2) Creando el conjunto de políticas de la siguiente manera.

Nuevo



- Nombre de configuración de enlaces
- Añadir → WS- Security



Enlaces generales de conjunto de políticas del cliente

Enlaces generales de conjunto de políticas del cliente > Nuevo

Utilice esta página para crear un enlace de cliente que se puede reutilizar entre los conjuntos de políticas y las aplicaciones. Utilice el botón Añadir para seleccionar los enlaces de política y, a continuación, asegúrese de proporcionar la configuración. Los enlaces vacíos se suprimen. Crear un ámbito para un enlace en un dominio de seguridad restringe las opciones de configuración a aquellas aplicables al dominio y limita el uso del enlace al dominio especificado.

* Nombre de configuración de enlaces
[Prueba WS-Security]

Dominio de seguridad:
Seguridad global

Descripción

Añadir Suprimir

Transporte SSL	
Transporte JMS	
Transporte HTTP	
WS-Security	
WS-ReliableMessaging	

WS-Security → Autenticación y protección → Señales de autenticación → Nueva señal →
Generador de señales

Enlaces generales de conjunto de políticas del cliente

Enlaces generales de conjunto de políticas del cliente > Nuevo > WS-Security > Autenticación y protección

Pueden añadirse a los enlaces por omisión señales y protecciones adicionales para las partes de mensaje.

☐ Inhabilitar la protección implícita para la confirmación de firma

Señales de protección

Nueva señal Suprimir

Seleccionar	Nombre de señal de protección	Uso
Ninguno		
Total 0		

Señales de autenticación

Nueva señal Suprimir

Generador de señales

Consumidor de señales

Seleccionar	Nombre de señal de autenticación	Uso
Ninguno		
Total 0		

Protección de cifrado y firma de mensaje de petición

Nueva firma... Nuevo cifrado... Suprimir Subir Bajar

Seleccionar	Nombre	Protección	Orden
Ninguno			
Total 0			

Protección de cifrado y firma de mensaje de respuesta

Nueva firma... Nuevo cifrado... Suprimir

Seleccionar	Nombre	Protección
Ninguno		
Total 0		

- Nombre
- Tipo de señal → Señal de nombre de usuario v1.0
- Inicio de sesión JAAS → wss.generate.unt
- 'Aplicar'



Enlaces generales de conjunto de políticas del cliente

[Enlaces generales de conjunto de políticas del cliente](#) > [Prueba WS-Security](#) > [WS-Security](#) > [Autenticación y protección](#) > [usenameToken](#)

Las señales de autenticación se envían en mensajes para probar o declarar una identidad.

Generador de señales

* Nombre
usenameToken

* Tipo de señal
Señal de nombre de usuario v1.0 ▼

* Parte local
<http://docs.oasis-open.org/ws/2004/01/oasis-200401-ws-username-token-profile-1.0#UsernameToken>

URI de espacio de nombres

Inicio de sesión JAAS
ws.generate.unt (Seguridad global) ▼ [Nuevo inicio de sesión de aplicación](#)

Propiedades personalizadas

Seleccionar	Nombre	Valor	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Nuevo Suprimir

Enlaces adicionales

Las propiedades adicionales estarán disponibles cuando se guarden o se apliquen las propiedades generales de este elemento.

* [Manejador de retorno de llamada](#)

[Aplicar](#) [Aceptar](#) [Restablecer](#) [Cancelar](#)

Manejador de retorno de llamada

URI de espacio de nombres

Inicio de sesión JAAS
ws.generate.x309 (Seguridad global) ▼ [Nuevo inicio de sesión de aplicación](#)

Propiedades personalizadas

Seleccionar	Nombre	Valor	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Nuevo Suprimir

Enlaces adicionales

* [Manejador de retorno de llamada](#)

[Aplicar](#) [Aceptar](#) [Restablecer](#) [Cancelar](#)

- Nombre de usuario → (Usuario técnico, para Preproducción solicitar al departamento de Sistemas)
- Contraseña → (Usuario técnico, para Preproducción solicitar al departamento de Sistemas)



[Enlaces generales de conjunto de políticas del cliente](#) > [Prueba WS-Security](#) > [WS-Security](#) > [Autenticación y protección](#) > [usnametoken](#) > [Manejador de retorno de llamada](#)

Especifica los parámetros del manejador de retorno de llamada utilizados para generar la señal. Como es posible conectar un manejador de retorno de llamada personalizado, debe especificar el nombre de la clase de implementación. El servidor de aplicaciones proporciona opciones para la evaluación de identidad, la autenticación básica y el almacén de claves que se pasa a la implementación del manejador de retornos de llamada.

Nombre de clase

- ☒ Utilizar valor por omisión incorporado
- ☐ Utilizar personalizado

Autenticación básica

Nombre de usuario

Contraseña

Confirmar contraseña

Propiedades personalizadas

Propiedades personalizadas

Seleccionar	Nombre	Valor	Nuevo	Suprimir
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Nuevo"/>	<input type="button" value="Suprimir"/>

-Conjuntos de políticas y enlaces del cliente de servicio.

Aplicaciones > Tipos de aplicación > Aplicaciones de empresa de WebSphere > [NUESTRA_APLICACION] > Propiedades de servicios Web > Conjuntos de políticas y enlaces del cliente de servicio

En este punto deberemos correlacionar la llamada a el/los servicio/s de INDI de nuestra aplicación con las políticas anteriormente creadas.

Primero conectamos el conjunto de políticas de cliente a el/los servicio/s de INDI de nuestra aplicación:

[Aplicaciones de empresa](#) > [\[NUESTRA_APP\]](#) > [Conjuntos de políticas y enlaces del cliente de servicio](#)

Define la configuración de la política y del enlace para la aplicación, sus referencias de servicios, puntos finales u operaciones. Acceda al enlace de políticas aplicadas para indicar si se debe utilizar y cómo adquirir la política del proveedor de servicios. Complete la conexión proporcionando la configuración específica del sistema cuando asigne el enlace apropiado.

Preferencias

Conectar conjunto de políticas de cliente ▾ Desconectar conjunto de políticas de cliente Asignar enlace ▾				
<input type="checkbox"/>	Kerberos V5 HTTPS default			
<input type="checkbox"/>	LTPA WSSecurity default			
<input type="checkbox"/>	SSL WSTransaction			
<input type="checkbox"/>	Username SecureConversation	nto final/Operaciones ▾	Conjunto de políticas de cliente conectado ▾	Políticas aplicadas ▾
<input type="checkbox"/>	Username WSSecurity default			
<input type="checkbox"/>	WS-I RSP	guientes:		
<input type="checkbox"/>	WSAddressing default		Ninguna	Ninguna
<input type="checkbox"/>	WSHTTPS default			No se aplica
<input type="checkbox"/>	WSReliableMessaging persistent	olucionWS	Ninguna	Ninguna
<input type="checkbox"/>	WSS Security Indt	evolucionWSPort_v7	Ninguna	No se aplica
<input type="checkbox"/>	WSS Security Ivpt			
<input type="checkbox"/>	WSS Security Reap	evolucionWSPort_v7	Ninguna	No se aplica
<input type="checkbox"/>	anotarExpedienteDevolucion		Ninguna	No se aplica
<input type="checkbox"/>	anotarExpedienteDevolucion		Ninguna	No se aplica
<input type="checkbox"/>	anotarSolicitudDevolucion		Ninguna	No se aplica
<input type="checkbox"/>	anotarSolicitudDevolucion		Ninguna	No se aplica




Segundo conectamos el enlace a el/los servicio/s de INDI de nuestra aplicación:

[Aplicaciones de empresa](#) > [\[NUESTRA_APP\]](#) > [Conjuntos de políticas y enlaces del cliente de servicio](#)

Defina la configuración de la política y del enlace para la aplicación, sus referencias de servicios, puntos finales u operaciones. Acceda al enlace de políticas aplicadas para indicar si se debe utilizar y cómo adquirir la política del proveedor de servicios. Complete la conexión proporcionando la configuración específica del sistema cuando asigne el enlace apropiado.

⊞ Preferencias

Conectar conjunto de políticas de cliente ▾ Desconectar conjunto de políticas de cliente ▾ Asignar enlace ▾

Valor por omisión
 Nuevo enlace específico de la aplicación...
 Client sample

Seleccionar: Aplicación/Servicio/Punto final/Operaciones ⚙ Conjunto de políticas de cliente ▾ **Indi WS-Security** Políticas aplicadas ⚙ Enlace ⚙

Puede administrar los recursos siguientes:

<input checked="" type="checkbox"/>	ExpedientesDevolucionWS	WSS Security Indi	Sólo cliente	Valor por omisión
<input type="checkbox"/>	ExpedientesDevolucionWSPort_v7	WSS Security Indi (heredado)	Sólo cliente (heredado)	Valor por omisión (heredado)
<input type="checkbox"/>	ExpedientesDevolucionWSPort_v7	WSS Security Indi (heredado)	Sólo cliente (heredado)	Valor por omisión (heredado)
<input type="checkbox"/>	anotarExpedienteDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Valor por omisión (heredado)
<input type="checkbox"/>	anotarExpedienteDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Valor por omisión (heredado)
<input type="checkbox"/>	anotarSolicitudDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Valor por omisión (heredado)
<input type="checkbox"/>	anotarSolicitudDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Valor por omisión (heredado)




Finalmente se debe quedar de esta manera:

[Aplicaciones de empresa](#) > [\[NUESTRA_APP\]](#) > [Conjuntos de políticas y enlaces del cliente de servicio](#)

Defina la configuración de la política y del enlace para la aplicación, sus referencias de servicios, puntos finales u operaciones. Acceda al enlace de políticas aplicadas para indicar si se debe utilizar y cómo adquirir la política del proveedor de servicios. Complete la conexión proporcionando la configuración específica del sistema cuando asigne el enlace apropiado.

⊞ Preferencias

Conectar conjunto de políticas de cliente ▾ Desconectar conjunto de políticas de cliente ▾ Asignar enlace ▾

Seleccionar: Aplicación/Servicio/Punto final/Operaciones ⚙ Conjunto de políticas de cliente conectado ⚙ Políticas aplicadas ⚙ Enlace ⚙

Puede administrar los recursos siguientes:

<input type="checkbox"/>	ExpedientesDevolucionWS	WSS Security Indi	Sólo cliente	Indi WS-Security
<input type="checkbox"/>	ExpedientesDevolucionWSPort_v7	WSS Security Indi (heredado)	Sólo cliente (heredado)	Indi WS-Security (heredado)
<input type="checkbox"/>	ExpedientesDevolucionWSPort_v7	WSS Security Indi (heredado)	Sólo cliente (heredado)	Indi WS-Security (heredado)
<input type="checkbox"/>	anotarExpedienteDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Indi WS-Security (heredado)
<input type="checkbox"/>	anotarExpedienteDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Indi WS-Security (heredado)
<input type="checkbox"/>	anotarSolicitudDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Indi WS-Security (heredado)
<input type="checkbox"/>	anotarSolicitudDevolucion	WSS Security Indi (heredado)	Sólo cliente (heredado)	Indi WS-Security (heredado)

2.3 Modificar el certificado de enlace de seguridad

N/A