# VINCULACIÓN AL SERVICIO CIUDADANO DIGITAL DE INTEROPERABILIDAD

BOGOTÁ, DICIEMBRE DE 2019

# Contenido

# Índice de ilustraciones

# Índice de tablas

# Interoperabilidad

La interoperabilidad tiene como propósito hacer que el estado funcione como una sola Entidad eficiente que les brinde a sus ciudadanos información oportuna, trámites y servicios en línea ágiles. Las entidades deben ser conscientes del impacto de la interoperabilidad en la sociedad, asumir con compromiso y dar el primer paso para estar digitalmente conectados y articulados. ¡Ser un solo Sistema!

La sociedad y la tecnología en constante evolución. Las relaciones entre entidades y entre éstas y el ciudadano debe estar a la par del sector público, garantizando el aprovechamiento de las TIC. Una sociedad digital debe contar con un Gobierno Digital.

El Marco de Interoperabilidad es genérico y aplicable a todas las entidades públicas y privadas en Colombia, el marco establece las condiciones básicas que se deben considerar para alcanzar la interoperabilidad tanto a nivel local, interinstitucional, sectorial, nacional o internacional y orientado a todos los involucrados en definir, diseñar, desarrollar y entregar servicios de intercambio de información, como son:

- Entidades públicas responsables de planear servicios que requieran colaboración interinstitucional.
- Entidades públicas que para mejorar su funcionamiento y relacionamiento con otras entidades a través del uso de las TIC.
- Organizaciones privadas involucradas en la ejecución y/o evolución de la estrategia de Gobierno Digital.
- Miembros de gobiernos extranjeros interesados en la interoperabilidad con entidades del Estado colombiano.
- Miembros de la comunidad académica interesados en la interoperabilidad del Gobierno Digital.

El Marco de Interoperabilidad proporciona la orientación necesaria a las entidades públicas y en general todos aquellos que quieran intercambiar información, mediante un conjunto de lineamientos sobre cómo mejorar la gobernanza de las actividades relacionadas a la interoperabilidad, permitiendo establecer relaciones entre proveedores y consumidores de información y racionalizar los procesos que dan soporte a los trámites y servicios o cualquier servicio digital prestado por las entidades, de conformidad con el marco normativo vigente y con garantía de hacerlo en un entorno de confianza digital.

## 1. Requerimientos Mínimos para la integración a la Interoperabilidad

Las entidades deberán contar como mínimo con una infraestructura tecnológica que permita desplegar un servidor virtual. Si requieren alta disponibilidad contar con dos o más nodos que permitan estar en Clúster. La entidad deberá tener la capacidad para poder desplegar la infraestructura de acuerdo con las siguientes especificaciones:

*Tabla 1 Requerimientos mínimos para la integración a la interoperabilidad*

| Ítem | Requisito | Explicación |
|---|---|---|
| **1.0** | Sistema Operativo Ubuntu 18.04 Long-Term Support (LTS), 64 bits o Red Hat RHEL7 (v7.3 o más reciente)<br>Nota: Los servidores de seguridad puede ser físicos o virtuales. | X-Road soporta únicamente estas versiones en sistemas operativos |
| **1.1** | 2 CPU Intel o AMD o compatible de doble núcleo de 64 bits; El soporte del conjunto de instrucciones AES es altamente recomendado. | El hardware del servidor (placa base, CPU, tarjetas de interfaz de red, sistema de almacenamiento) debe ser compatible con RHEL7 o Ubuntu en general. |
| **1.2** | 6 GB de RAM | Memoria RAM mínima requerida. de acuerdo con la transaccionalidad de la entidad pude aumentar la memoria RAM |
| **1.3** | 20 GB de espacio libre en disco (partición del sistema operativo)<br>20-40 GB de espacio libre en disco (/var/partición); | Almacenamiento mínimo requerido. |
| **1.4** | Para la instalación del servidor de seguridad, se requiere que el servidor instalado tenga conectividad a internet para acceder a los repositorios de instalación que se detallan en el anexo técnico. | Acceso a repositorios de instalación |
| **1.5** | Una tarjeta de interfaz de red de 1000 Mbps.<br>Enlace a GNAP dedicado, el ancho de banda del canal depende de la transaccionalidad de los servicios web. | Red mínima requerida |
| **1.6** | Posterior a la instalación, la entidad debe configurar en enlace a GNAP.<br>El servidor de seguridad puede estar separado de otras redes por un firewall y / o NAT y se deben permitir las conexiones necesarias hacia y desde el servidor de seguridad. La habilitación de los servicios auxiliares que son necesarios para el funcionamiento y la administración del sistema | Segmentación de Red y Seguridad.<br>El consumo y exposición de servicios es a través de GANP. |

| Ítem | Requisito | Explicación |
|---|---|---|
| | operativo (como DNS, NTP y SSH) se encuentran fuera del alcance de esta guía.<br>Nota: Si el servidor de seguridad tiene una dirección IP privada, se debe crear un registro NAT correspondiente en el firewall. | |

*Fuente: Agencia Nacional Digital*

Para Instalación, Configuración y Desarrollo Plataforma de Interoperabilidad Las entidades deberán seguir lo establecido en el documento Anexo Técnico, el cual detalla la manera de realizar la instalación y configuración de los servidores de seguridad, como también la forma de intervenir los servicios web que se encuentran desarrollados o a desarrollar en estándares REST y SOAP.

## 2. Preparación

Para la instalación del servidor de seguridad La entidad deberá configurar los siguientes requerimientos:

*Tabla 2 Configuración de requerimientos*

| Ítem | Requisito | Explicación |
|---|---|---|
| **1.0** | https://artifactory.niis.org/xroad-release-deb | Repositorio de paquetes X-Road |
| **1.1** | https://artifactory.niis.org/api/gpg/key/public | La clave del repositorio |
| **1.2** | **Conexiones entrantes** | Puerto para conexiones entrantes (desde la red externa al servidor de seguridad) |
| | TCP 5500 | Intercambio de mensajes entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la **lista blanca solo de AND IP y Nodos**). |
| | TCP 5577 | Consulta de respuestas OCSP entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (**en la lista blanca solo de AND IP y Nodos**) |
| | TCP 9011 | Puerto de escucha JMX del demonio de monitoreo de datos operativos |
| | TCP 9999 | Puerto de escucha JMX del demonio de monitoreo ambiental |
| **1.5** | **Conexiones salientes** | Puertos para conexiones salientes (desde el servidor de seguridad a la red externa) |

| Ítem | Requisito | Explicación |
|---|---|---|
| | TCP 5500 | Intercambio de mensajes entre servidores de seguridad. |
| | TCP 5577 | Consulta de respuestas OCSP entre servidores de seguridad. |
| | TCP 4001 | Comunicación con el servidor central. |
| | TCP 2080 | Puertos para conexiones salientes (desde el servidor de seguridad a la red interna)<br>Intercambio de mensajes entre el servidor de seguridad y el demonio de monitoreo de datos operativos (de forma predeterminada en localhost) |
| | TCP 80 | Descarga de la configuración global desde el servidor central. |
| | TCP 80,443 | Los servicios de OCSP y de estampa de tiempo más comunes. |
| **1.6** | TCP 4000 | Interfaz de usuario (red local). **¡No debe ser accesible desde internet!** |
| **1.7** | TCP 80, 443 | Puntos de acceso al sistema de información (en la red local). **¡No debe ser accesible desde internet!** |
| | TCP 2080 | Intercambio de mensajes entre el servidor de seguridad y el Proceso de monitoreo de datos operativos (de forma predeterminada en localhost) |
| | TCP 9011 | Puerto de escucha JMX del demonio de monitoreo de datos operacionales |
| **1.8** | Direcciones IP | Direcciones IP internas de servidor de seguridad y nombre (s) de host |
| **1.9** | Dirección Ip Servidor de Seguridad | Servidor de seguridad, dirección IP pública, dirección NAT. |
| **1.10** | <de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital> | Información sobre el certificado TLS de la interfaz de usuario. |
| **1.11** | <de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital> | Información sobre los servicios del certificado TLS. |

| Ítem | Requisito | Explicación |
|---|---|---|
| **1.12** | TCP 2552 | Puerto para comunicaciones entre los xroad-proxy y xroad-monitoring |
| **1.13** | IP PÚBLICA | Monitoreo de seguridad del servidor IP en instancia de Gobierno |

*Fuente: Agencia Nacional Digital*

Una vez se tiene el sistema operativo base, se ingresan las configuraciones de usuario, se establece la configuración regional del sistema para que posteriormente se instale paquete de plataforma X-ROAD.

Si durante la instalación se generan errores algunos de los más comunes se encuentran documentados en la guía técnica con el manejo que se le puede dar para su solución.

### 2.1. Instalación en Ubuntu

Para la instalación del software de seguridad X-ROAD en UBUNTU se tiene que seguir los siguientes pasos:

- Agregue la clave de firma del repositorio de X-Road a la lista de claves confiables.
- Agregue el repositorio de paquetes de X-Road.
- Instale los paquetes del servidor de seguridad.

Tras la primera instalación de los paquetes el sistema solicita información como nombre de cuenta del usuario, el nombre distinguido del propietario del certificado TLS autofirmado de la interfaz del usuario y sus nombres alternativos.

Una vez finalizada la instalación si esta se realiza correctamente se inician los servicios del sistema y la interfaz de usuario deberá estar respondiendo.

De forma opcional se puede instalar el soporte para tokens de seguridad por hardware.

### 2.2. Instalación en REDHAT

Para la instalación del software de seguridad X-ROAD en REDHAT se tiene que seguir los siguientes pasos:

- Agregue el repositorio de paquetes X-Road y los repositorios de Paquetes adicionales para Enterprise Linux (EPEL).
- Agregue la clave de firma del repositorio de X-Road a la lista de claves confiables.
- Instale los paquetes del servidor de seguridad.
- Agregar usuario del sistema a los que se otorgan todos los roles en la interfaz de usuario.

Una vez finalizada la instalación si esta se realiza correctamente se inician los servicios del sistema y la interfaz de usuario deberá estar respondiendo.

La instalación de soportes para tokens por hardware no se ha probado en este sistema por lo cual no se proporciona soporte.

## 3. Adecuación

### 3.1. Configuración del servidor

Para realizar la configuración inicial haga uso de un navegador web para iniciar sesión por primera vez, use el nombre de cuenta suministrado durante la instalación, una vez iniciada sesión se solicita el archivo de anclaje de configuración global el cual es suministrado por la agencia nacional digital AND. Si la información se descarga correctamente el sistema solicitara nueva información del miembro de propietario del servidor de seguridad.

Durante la configuración inicial del servidor de seguridad se ingresa la información de miembro del nodo X-Road del servidor y el PIN del token de software.

El anclaje de configuración es un conjunto de información que se puede utilizar para descargar y verificar información. Se proporciona un enlace a una configuración descargada. Los anclajes de configuración se distribuyen como archivos XML.

Cada entorno de X-Road tiene una configuración diferente. Utilice la configuración del entorno X-Road que va a utilizar.

Los anclajes de configuración de los tres entornos son los siguientes:

- Entorno de desarrollo: Solicitar a la Agencia Nacional Digital.
- Entorno de prueba: Solicitar a la Agencia Nacional Digital.
- Entorno de producción: Solicitarla a la Agencia Nacional Digital.

Cuando inicie sesión en su servidor web, https: // <SECURITYSERVER IP ADDRESS>: 4000 / por primera vez el sistema solicita la siguiente información:

- El archivo de anclaje de configuración global (Solicitarlo a la Agencia Nacional Digital).

Si la configuración se descarga correctamente, el sistema solicita la siguiente información:

- La clase miembro del propietario del servidor de seguridad.
- El código de miembro del propietario del servidor de seguridad, Si la clase de miembro y el código de miembro se ingresan correctamente, el sistema muestra el nombre del propietario del servidor de seguridad registrado en el centro de X-Road.

El Código de Miembro debe estar formado de la siguiente manera:

- "sigla de la Entidad-código SIGEP" - sin espacios en blanco.

Ejemplo:

- Ministerio de tecnologías de la información y las Comunicaciones (Entidad Estatal).
- Nombre de miembro: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.
- Clase de miembro: GOV.
- Código de miembro: MinTIC-0012.

Dichos requisitos del Código de miembro de GOV son necesarios para garantizar la singularidad del Código de miembro de organizaciones en X-Road. Además, los miembros del Código de miembro de X-Road deben corresponder con el campo Identificador de organización (2.5.4.97) en el perfil de certificado de sello electrónico.

Adicionalmente en esta configuración inicial del servidor de seguridad tendrá que realizar lo siguiente:

- Agregar gestión de servicios de estampa cronológica de tiempo.
- Generar una clave de firma haciendo uso del certificado digital.
- Generar clave de autenticación.
- Generación de solicitud de certificado para clave de autenticación.
- Importar un certificado de firma desde un sistema de archivos local.
- Importar un certificado de firma desde un dispositivo criptográfico.
- Importar un certificado de autenticación de un sistema de archivos local.
- Registro del servidor de seguridad en la administración de X-Road.
- Agregar un certificado de prueba a la lista de prueba de OCSP.
- Estados de disponibilidad de dispositivos clave, claves y certificados.
- Condiciones de registro de certificados.
- Propietario y cliente del servidor de seguridad.
- Adicionar un cliente al servidor de seguridad.
- Registro del cliente del servidor de seguridad en la administración de PDI.
- Administración de servicios de datos.
- Activar y desactivar Servicios Web.
- Adición de un certificado TLS de red interna.
- Gestionando el Certificado Intranet TLS.
- Cambiar la clave TLS y el certificado para la intranet.
- Sujetos de derechos de acceso.
- Gestión de derechos de acceso.
- Cambiar los derechos de acceso al servicio.
- Añadir un cliente de servicio.
- Cambio de los derechos de acceso del cliente de servicio.
- Grupos con derechos de acceso locales y globales.
- Añadiendo un grupo local.

- Ver y editar miembros del grupo local.
- Cambiar la descripción del grupo local.
- Copia de seguridad de la configuración del servidor de seguridad.
- Cargar y eliminar un archivo de copia de seguridad de configuración.
- Restaurar la configuración de la interfaz de usuario.
- Transferencia de archivos de un servidor de seguridad.

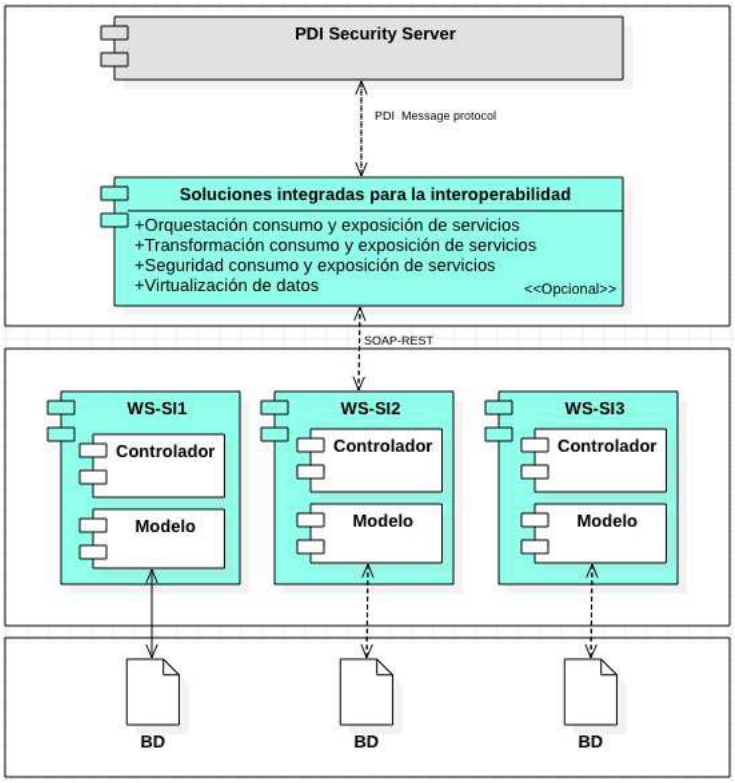
## 4. Integrar servicios WEB

### 4.1. Intervención de los servicios

Para la intervención de los servicios se debe tener en cuenta si la entidad va a exponer y/o consumir servicios. Nativamente la plataforma de interoperabilidad soporta tecnología REST y protocolo SOAP. Los servicios web en tecnología REST no requieren la intervención cuando estos son de exposición.

El marco de interoperabilidad describe una arquitectura de referencia orientada a la integración de servicios de exposición o consumo en la plataforma de interoperabilidad.

*Ilustración 1 Arquitectura de referencia plataforma de interoperabilidad*




*Fuente: Agencia Nacional Digital*

la arquitectura ilustrada muestra el componente de soluciones integradas para interoperabilidad como un componente que tendrá la capacidad de:

- Orquestar los servicios de consumo y exposición.
- Transformar servicios de consumo y exposición.
- Brindar seguridad en el consumo y exposición de servicios.
- Virtualizar datos.

Este componente servirá para agregar los encabezados que se requieren en los servicios web sin necesidad de intervenir estos directamente en su estructura. Este puede ser implementado por diferentes medios como, por ejemplo: un Bus de servicios (ESB Enterprise Service Bus), o un API y es opcional para las entidades dependiendo de la arquitectura interna.

Los encabezados deben tener una estructura y un espacio de nombres correctos, es por esto por lo que los servicios SOAP y REST (consumo) tienen que ser intervenidos para que los siguientes campos obligatorios de X-Road sean agregados:

- Client: campo que identifica al cliente que inició la solicitud, que se describe con los siguientes elementos:

  - xRoadInstance

  - memberClass

  - memberCode

  - subsystemCode

- Service: es el campo que especifica el servicio de datos que se utilizará. Ademas de agregar los elementos descriptivos del campo < client > se adicionan los siguientes elementos:

  - (xRoadInstance, memberClass, memberCode y subsystemCode)

  - serviceCode

  -serviceVersion (Opcional)

## 4.2. Creación de subsistemas

En la plataforma de interoperabilidad, los servicios de intercambio de datos son consumidos a través de subsistemas sobre los cuales se conceden los permisos de acceso a cada uno de los clientes.

Las entidades pueden configurar quienes pueden consumir sus servicios a través de la gestión de derechos de acceso.

Hay dos formas de administrar los derechos de acceso en un servidor de seguridad.

- La gestión de derechos de acceso basada en servicios: permite abrir o cerrar un servicio para múltiples clientes de servicios.
- Administración de derechos de acceso basada en el cliente: si necesita abrir o cerrar varios servicios para un cliente de servicio.

## 4.3. Adicionar servicios WEB

### 4.3.1. SOAP

Cuando se agrega un nuevo archivo WSDL, el servidor de seguridad lee la información del servicio y muestra la información en la tabla de servicios. El código de servicio, el título y la dirección se leen del WSDL.

Para agregar un WSDL, siga estos pasos:

- En el menú “Configuration”, seleccione “Security Server Clients”, seleccione un cliente de la tabla y haga clic en el icono “Services”.
- Haga clic en “ADD WSDL”, ingrese la dirección WSDL en la ventana que se abre y haga clic en Aceptar. Una vez que se cierra la ventana, el WSDL y la información sobre los servicios que contiene se agregan a la tabla. Por defecto, el WSDL se agrega en estado deshabilitado.

Para ver una lista de servicios contenidos en el WSDL haga clic en el símbolo " + " delante de la fila WSDL para expandir la lista.

### 4.3.2. REST

Cuando se agrega un nuevo servicio REST, el servidor de seguridad muestra la url y el código de servicio proporcionado.

Para agregar un servicio REST, siga estos pasos:

- En el menú “Configuration”, seleccione “Security Server Clients”, seleccione un cliente de la tabla y haga clic en el icono “Services”.
- Haga clic en “ADD REST”, ingrese la url y el código de servicio en la ventana que se abre y haga clic en Aceptar. Una vez que se cierra la ventana, la url y el código de servicio se agregan a la tabla. Por defecto, la API REST se agrega en estado deshabilitado.

Para ver el servicio el servicio REST haga clic en el símbolo " + " delante de la fila REST para expandir la descripción del servicio.

## 5. Uso y apropiación

Una vez finalizado la integración de la entidad a la plataforma de interoperabilidad PDI, la decisión de que este pase a etapa de producción está en manos de la entidad, para ello la agencia nacional digital AND recomienda tener en cuenta lo siguiente:

- La entidad debe estar certificada en nivel 3 de lenguaje común de intercambio.
- La entidad comprende el marco de interoperabilidad para gobierno digital el cual se fundamenta en un modelo de madurez basado en aspectos legales, técnicos y organizacionales que permite el desarrollo progresivo de los servicios de intercambio de información al interior de las entidades, estos dominios son:

  - **Dominio Político – legal:** Consiste en garantizar que las entidades públicas realizan el intercambio de información ajustado al marco jurídico vigente, las políticas y estrategias pueden trabajar juntas y no se obstaculiza o impide la interoperabilidad.

  - **Dominio Organizacional:** se refiere al modo en que las misiones, políticas, procesos y expectativas interactúan con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y mutuamente beneficiosas, a través del intercambio de información.

  - **Dominio Semántico**: permite garantizar que, en el momento de intercambiar datos, el significado de la información sea exacto y el mismo para todas las partes interesadas. De igual manera, permite que las entidades del Estado colombiano puedan estandarizar, gestionar y administrar su información.

  - **Dominio Técnico**: hace referencia a las aplicaciones e infraestructuras que conectan sistemas de información, a través de los servicios de intercambio de información. Incluye aspectos como especificaciones de interfaz, protocolos de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros.