

# Manual de uso

## 2024

Fecha de publicación:

Última revisión:

Generado por: Florencia Gonzalez

Área responsable: Análisis funcional

# Índice

Índice.....	2
Restricciones .....	4
TABLA DE REVISIÓN.....	4
INTRODUCCIÓN .....	4
PROPOSITO .....	5
<b>Definición de un Sistema de Interoperabilidad .....</b>	<b>6</b>
<b>Motivos para Implementar X-Road .....</b>	<b>6</b>
<b>Visión General del Sistema X-Road.....</b>	<b>7</b>
<b>Ejemplo de Aplicación.....</b>	<b>7</b>
COMPONENTES Y FUNCIONAMIENTO .....	8
Responsabilidades y Funciones Clave .....	8
<b>Operador del Sistema de Interoperabilidad .....</b>	<b>9</b>
<b>Proveedores de Servicios de Confianza (TSP).....</b>	<b>9</b>
<b>Organizaciones Miembro (OM) .....</b>	<b>9</b>
<b>Diseño de la Arquitectura del Sistema.....</b>	<b>10</b>
<b>Componentes Principales: .....</b>	<b>11</b>
<b>Cómo Funciona el Intercambio de Datos: .....</b>	<b>13</b>
<b>Beneficios de esta Arquitectura:.....</b>	<b>14</b>
INFRAESTRUCURA EN AWS .....	14
Componentes Clave de la Infraestructura en AWS.....	14
VPC (Virtual Private Cloud): .....	14
Instancias EC2:.....	14
Grupos de Seguridad y Configuración de Puertos:.....	15
Health Checks y Failover:.....	15
Security Server (Servidor de Seguridad):.....	15
Base de Datos en Amazon Aurora:.....	15
Seguridad Adicional con AWS WAF: .....	15
Bastion (Jump Box) para Acceso Seguro: .....	16
Alta Disponibilidad y Recuperación Ante Desastres (DR) .....	16
Beneficios de la Infraestructura en AWS .....	16
Comparación con Infraestructuras Locales.....	17
Conclusión .....	17

PROCESO DE INTEGRACIÓN AL SISTEMA X-ROAD .....	18
Registrarse como Organización Miembro.....	18
<b>Organizaciones Públicas:</b> .....	18
<b>Organizaciones Privadas:</b> .....	20
SERVIDOR DE SEGURIDAD .....	22
INSTALACION DEL SERVIDOR DE SEGURIDAD .....	23
<i><b>Componentes de configuración del servidor de seguridad</b></i> .....	28

# Manual de Usuario para el Sistema X-Road: Implementación en el Gobierno de Córdoba

Clasificación de la información: Interno

## Restricciones

Los contenidos de este documento son propiedad de South Hive y son confidenciales sólo para uso interno. Queda estrictamente prohibido cualquier reproducción total o parcial sin la autorización escrita por parte de South Hive.

Este documento está sujeto a cambios. Los comentarios o dudas deberán ser enviados a sus autores.

Audiencia	Propósito
Equipo South Hive	Conocimiento del estado actual del sistema y su uso.

## TABLA DE REVISIÓN

La siguiente tabla enlista las revisiones realizadas a este documento.

Versión	Fecha	Cambio	Autor	Revisión
1.0	28/11/2024	Creación del documento	Florencia Gonzalez	

## INTRODUCCIÓN

El sistema de interoperabilidad X-Road es una plataforma de intercambio de datos segura y eficiente, diseñada para facilitar la conexión entre diferentes sistemas y entidades públicas y privadas. A través de X-Road, los organismos gubernamentales, entidades privadas y otros actores clave pueden compartir información de manera automatizada, garantizando la integridad, confidencialidad y disponibilidad de los datos en cada transacción.

En el contexto de la Provincia de Córdoba, X-Road representa un avance significativo en la modernización de la administración pública. Su implementación responde a la necesidad de optimizar los procesos administrativos, reducir la duplicación de trámites y agilizar la entrega de servicios a los ciudadanos, a la vez que asegura el cumplimiento de normativas de seguridad y privacidad.

Este manual está destinado a guiar a los usuarios en la configuración, operación y mantenimiento del sistema X-Road implementado en la infraestructura de Amazon Web Services (AWS). En él se detallan los pasos necesarios para integrar servicios, gestionar las configuraciones técnicas y administrar los certificados digitales esenciales para las transacciones seguras. Además, se proporcionan instrucciones claras sobre el monitoreo del sistema y la resolución de posibles incidencias, de manera que los responsables de la administración puedan garantizar un funcionamiento eficiente y sin contratiempos.

La implementación de X-Road en Córdoba tiene como objetivo transformar la manera en que las organizaciones interactúan con los datos, permitiendo una mayor transparencia, eficiencia y colaboración entre los sectores público y privado. A lo largo de este documento, los usuarios encontrarán no solo los aspectos técnicos, sino también ejemplos prácticos que faciliten la comprensión de los beneficios del sistema en la práctica.

## **PROPOSITO**

El propósito de este manual es proporcionar a los usuarios un conjunto de directrices claras para la implementación, uso y mantenimiento del sistema X-Road en el Gobierno de la Provincia de Córdoba, utilizando la infraestructura de Amazon Web Services (AWS). Este documento está diseñado para garantizar que todos los usuarios, desde administradores hasta técnicos y organismos miembros, comprendan cómo interactuar con el sistema de interoperabilidad de manera segura y eficiente.

El manual tiene como objetivo principal facilitar el proceso de integración entre las entidades públicas y privadas en la provincia, asegurando que todos los servicios digitales se intercambien de forma automatizada y con los más altos estándares de seguridad. A través de esta plataforma, se busca optimizar los procesos administrativos, reducir la carga burocrática y mejorar la experiencia de los ciudadanos al acceder a servicios gubernamentales.

Además, el manual proporciona instrucciones detalladas sobre la configuración del sistema, la gestión de servicios, y la implementación de los certificados digitales necesarios para la autenticación y firma de transacciones. De esta manera, se pretende que los usuarios sean capaces de integrar sus servicios en la red de interoperabilidad de forma autónoma y efectiva, manteniendo la seguridad, privacidad y trazabilidad de las transacciones en todo momento.

A lo largo del documento, se incluyen ejemplos prácticos, procedimientos paso a paso y directrices sobre las mejores prácticas para la gestión y monitoreo del sistema. Esto permitirá a los responsables de la administración y operación de X-Road garantizar el correcto funcionamiento del sistema a medida que se expanda y se integren nuevos servicios.

## **Definición de un Sistema de Interoperabilidad**

Un sistema de interoperabilidad es un entorno diseñado para permitir el intercambio fluido, seguro y eficiente de información entre diferentes sistemas y entidades, independientemente de las tecnologías y plataformas que utilicen. Su propósito principal es establecer estándares comunes y mecanismos seguros que faciliten la comunicación sin importar las diferencias técnicas, lo que optimiza la cooperación entre distintas organizaciones.

Es esencial que estos sistemas sean flexibles y adaptables, capaces de evolucionar con los avances tecnológicos y los cambios en las normativas, mientras aseguran la seguridad, privacidad y protección de los datos. De esta manera, se promueve la transparencia, se automatizan los procesos administrativos y se mejora la experiencia de los ciudadanos al interactuar con los servicios públicos.

Este tipo de sistemas permite optimizar el intercambio de datos, contribuyendo al fortalecimiento de los procesos de toma de decisiones y reduciendo los costos operativos mediante la automatización de trámites y la mejora de la accesibilidad a la información entre diferentes actores gubernamentales y privados.

## **Motivos para Implementar X-Road**

La modernización del sector público en Córdoba es una prioridad, con el objetivo de facilitar el acceso a los servicios gubernamentales y reducir la carga burocrática que enfrentan tanto los ciudadanos como las instituciones. Aunque se han logrado avances en la digitalización de ciertos procesos, aún persisten sistemas aislados que requieren que los ciudadanos presenten documentación repetidamente y gestionen trámites en plataformas dispares.

La implementación de X-Road responde a esta necesidad de integración, permitiendo que diversas entidades puedan compartir información en tiempo real y de forma segura, lo que reduce duplicidades y mejora la eficiencia operativa. A través de este sistema, los organismos públicos y privados podrán colaborar en un ecosistema digital interconectado, optimizando el uso de los recursos, acelerando los procesos administrativos y brindando a los ciudadanos servicios más rápidos y eficaces.

El proyecto X-Road tiene como finalidad contribuir al proceso de transformación digital de la Provincia de Córdoba, estableciendo las bases para la Plataforma de Interoperabilidad Provincial y avanzando hacia un Ecosistema Digital Integrado de Córdoba (EDI-X).

## **Visión General del Sistema X-Road**

X-Road es una plataforma que permite la conexión segura entre entidades públicas y privadas mediante servicios web estandarizados. Este sistema garantiza la integridad y confidencialidad de la información en cada transacción, favoreciendo la colaboración entre organismos, optimizando los recursos y mejorando la transparencia en los procesos administrativos.

En el contexto de Córdoba, la gestión de X-Road estará a cargo de la Secretaría de Innovación e Infraestructura de la Gestión (SIIG), que establecerá las normativas y directrices técnicas para asegurar su correcta implementación y funcionamiento. A través de este sistema, se busca mejorar la accesibilidad y la calidad de los servicios gubernamentales, brindando una experiencia más eficiente y menos burocrática para los ciudadanos.

Este proyecto tiene un impacto significativo en la administración pública, ya que no solo contribuye a ahorrar tiempo y reducir costos para los ciudadanos, sino que también transforma la relación entre el sector público y privado, promoviendo una administración más ágil y accesible.

## **Ejemplo de Aplicación**

### **Situación Actual en Córdoba:**

Imagina que un ciudadano de Córdoba necesita realizar múltiples trámites relacionados con su propiedad, como la inscripción en el Registro de la Propiedad y la solicitud de un permiso de obra en la municipalidad. Actualmente, el proceso podría ser así:

1. El ciudadano debe llevar su escritura pública al Registro de la Propiedad para obtener un certificado que valide la titularidad.
2. Con el certificado del Registro, debe ir a la municipalidad para presentar nuevamente la escritura y otros documentos, como un plano de la obra.
3. Si necesita solicitar un crédito hipotecario, el banco también le pedirá los mismos documentos.

En cada institución, el ciudadano debe presentar los mismos papeles repetidamente. Este sistema no solo es ineficiente, sino que también aumenta la probabilidad de errores, demoras y pérdida de documentos.

### **Cómo X-Road Mejoraría el Proceso:**

Con X-Road, las instituciones públicas y privadas en Córdoba estarían conectadas mediante una plataforma de interoperabilidad. Lo cual provee las siguientes características:

**Unificación de Datos:** Una vez que la escritura está registrada en el Registro de la Propiedad, esta información queda disponible para la municipalidad, el banco, y cualquier otra entidad autorizada.

**Acceso Seguro y Automático:** Al momento de iniciar un trámite en la municipalidad o el banco, el funcionario no necesita pedir la escritura al ciudadano. En su lugar, accede de manera segura a los datos del Registro a través de X-Road.

**Reducción de Pasos:** Para el ciudadano, esto significa menos viajes, menos papeles y un proceso mucho más rápido. Todo esto se hace garantizando la seguridad y privacidad de la información mediante certificados digitales y registros de auditoría.

De esta manera y con este sencillo ejemplo, se puede apreciar que no solo se beneficia al ciudadano ahorrándole tiempo y recursos ya que no debe presentar los mismos documentos en cada institución, sino que también las instituciones públicas y privadas pueden optimizar la gestión de recursos porque se comparten los datos en tiempo real, reduciendo el tiempo de procesamiento.

## **COMPONENTES Y FUNCIONAMIENTO**

### **Responsabilidades y Funciones Clave**

El ecosistema de X-Road se sustenta en tres figuras clave que garantizan su funcionamiento: el operador, los proveedores de confianza y las entidades participantes, conocidas como Organizaciones Miembro (OM). Cada una desempeña un papel fundamental para asegurar la seguridad y eficiencia en el intercambio de datos.



## **Operador del Sistema de Interoperabilidad**

El operador actúa como el administrador central, encargado de establecer las políticas y normativas que rigen el sistema. Este rol incluye tareas como:

- Definir regulaciones y directrices operativas.
- Monitorear el desempeño del sistema y aplicar mejoras.
- Aprobar nuevas organizaciones para que formen parte del sistema.
- Brindar soporte técnico y gestionar la infraestructura central.

## **Proveedores de Servicios de Confianza (TSP)**

Estos proveedores aseguran la integridad de las transacciones al proporcionar servicios esenciales como:

**Certificados de Autenticación:** Que garantizan la identidad y la seguridad de las conexiones entre los diferentes nodos. Se encuentra lo siguiente:

**Time Stamping Service:** Se encarga de sellar el momento en que se realizó la transacción.

**Certificados de Firma Digital:** Que aseguran que los mensajes enviados no han sido alterados y permiten rastrear su origen, evitando cualquier tipo de negación por parte del emisor. Se encuentra lo siguiente:

**Certification Authority OSCP Service:** Sellar digitalmente cual fue la organización en la transacción.

## **Organizaciones Miembro (OM)**

Las OM son las entidades que, a través de sus servidores, ofrecen o consumen servicios dentro de la red. Estas pueden ser públicas o privadas y deben cumplir con ciertos requisitos para garantizar la seguridad del sistema.

Ventajas para las OM:

- Mayor agilidad en el intercambio de información.
- Optimización de procesos administrativos.
- Mejora en los servicios brindados al público.

Obligaciones al ser parte de X-BA:

- Cumplimiento de estándares de seguridad y privacidad
- Garantía de ética y privacidad en el uso de la información
- Mantenimiento actualizado de la infraestructura tecnológica

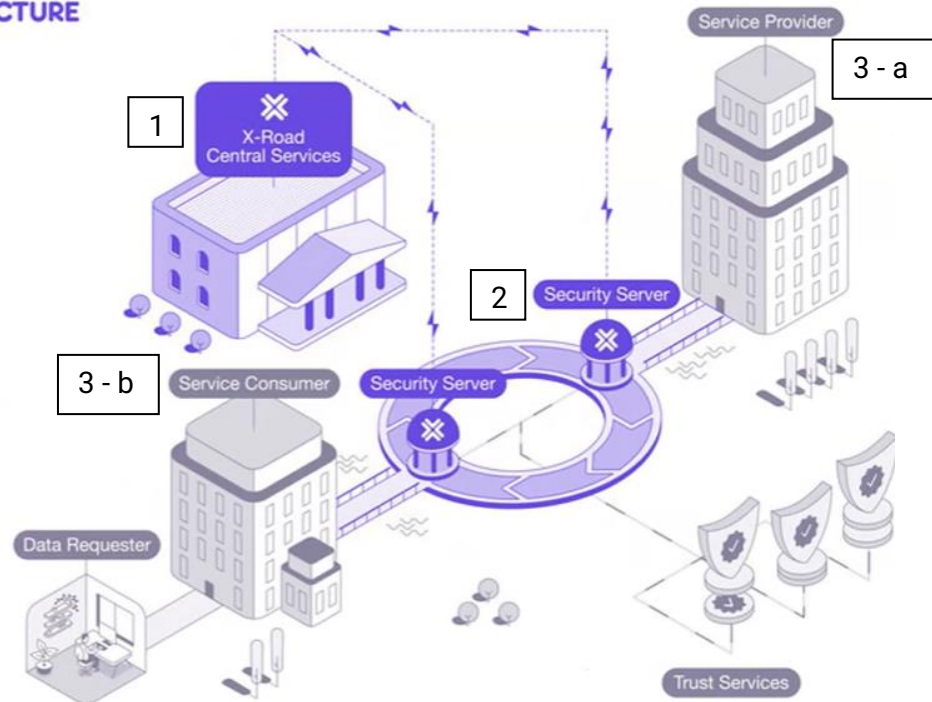
- Aseguramiento del correcto funcionamiento del sistema en su totalidad
- Cumplimiento de requisitos para evitar suspensiones por incompatibilidades

Es importante destacar que, frente a la detección de incompatibilidades conforme a estas obligaciones, el operador del sistema tiene la potestad de suspender a Organizaciones Miembro que formen parte del sistema de interoperabilidad.

## **Diseño de la Arquitectura del Sistema**

X-Road utiliza una arquitectura distribuida que garantiza una comunicación segura entre diferentes entidades a través de servicios web. A diferencia de los sistemas centralizados, donde todas las comunicaciones dependen de un único punto de control, X-Road elimina el riesgo de que una falla en ese punto comprometa todo el ecosistema debido a que el intercambio de información se hace entre instituciones, permitiendo una mayor resiliencia y continuidad en el intercambio de información.

Es importante mencionar que es centralmente administrado, porque en la arquitectura depende de un servidor central que realiza la gestión de los miembros al ecosistema y su configuración. Además, es el vínculo directo del establecimiento de la relación con los servicios de confianza, lo cual es una estructura de servicios que incluye sellado digital de tiempo, sellado mediante certificado digital de firma y autenticación, y validaciones de configuraciones mediante un proxy de configuración.

**X-ROAD ARCHITECTURE****Componentes Principales:**

- **Servidor Central (1):** Coordina y supervisa todas las transacciones, autentica a los participantes y lleva registros de auditoría. Es el punto de referencia para la entrada de organizaciones que formen parte del ecosistema.
- **Servidores de Seguridad (2):** Actúan como puntos de conexión para cada organización, protegiendo los datos durante su transferencia. Es importante resaltar que cada organización debe contar con uno, debido a que es entre estos servidores que se realiza la transferencia de datos de manera cifrada, y se debe realizar una carga de configuraciones globales desde el servidor central. Pueden ser Físicos o Virtuales:

Aspecto	Servidor Físico	Servidor Virtual
<b>Costo inicial</b>	<b>Elevado:</b> requiere la compra del hardware, espacio físico y mantenimiento.	<b>Bajo:</b> se paga solo por los recursos usados en una plataforma de virtualización o nube.
<b>Escalabilidad</b>	<b>Limitada:</b> agregar capacidad implica adquirir más hardware físico.	<b>Alta:</b> se puede aumentar o reducir la capacidad fácilmente según las necesidades.

<b>Implementación</b>	<b>Más lento:</b> requiere instalación física y manual de configuración.	<b>Más rápido:</b> puede implementarse en minutos en entornos virtualizados como AWS, Azure o VMware.
<b>Mantenimiento</b>	<b>Manual:</b> necesita personal técnico para actualizaciones y soporte físico.	<b>Automatizado:</b> las plataformas de nube ofrecen herramientas para mantenimiento y actualizaciones automáticas.
<b>Seguridad Física</b>	<b>Alta:</b> control físico directo del equipo.	<b>Depende del proveedor:</b> la seguridad de la nube debe cumplir con los estándares internacionales.
<b>Resiliencia</b>	<b>Moderada:</b> los fallos de hardware pueden requerir tiempo para su reparación.	<b>Alta:</b> puede configurarse con alta disponibilidad (HA) y recuperación ante desastres.
<b>Flexibilidad</b>	<b>Limitada:</b> difícil de reubicar o modificar su propósito.	<b>Alta:</b> fácil de migrar o reconfigurar según los requerimientos.

Una vez configurado cada uno de los servidores se necesitan 2 llaves básicas para su funcionamiento:

Una llave de autenticación para que se pueda asegurar de que es miembro activo del ecosistema de X-Road

Una llave de firma para que se firme digitalmente cada transacción.

Subsistemas (3): Son los servicios específicos que cada entidad ofrece o consume, registrados en el sistema central. Se pueden clasificar en:

Proveedores (a)

Consumidores (b)

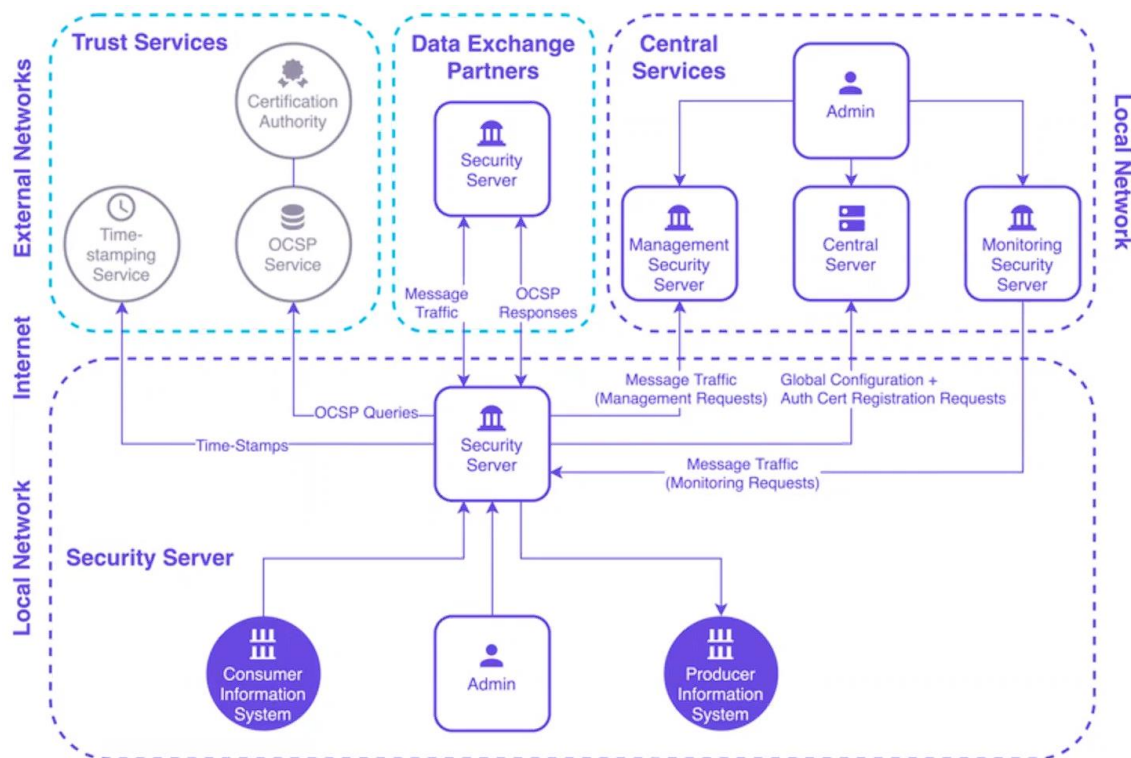
Servicios Web: Cada servicio se define técnicamente y se publica para su acceso por otros subsistemas autorizados.

- **Derechos de acceso:** Se deben realizar acuerdos formales que especifiquen las condiciones bajo las que los servicios pueden ser utilizados. Definen la autorización y restricciones de uso.

- **Seguridad y autenticación:** El sistema cuenta con una seguridad sólida, utilizando certificados digitales para autenticar y autorizar a los miembros y subsistemas. Cada transacción que se realiza en el sistema es sellada mediante un servicio de sellado de tiempo que registra el momento exacto en el que se realiza la transacción y firmada de manera digital garantizando el no repudio, armando un registro de

auditoria que es almacenado en el servidor central (ACLARACIÓN: Lo que se registra es la transacción, no los datos que se han transferido).

## Cómo Funciona el Intercambio de Datos:



- 1) **Verificación:** El sistema valida la identidad del subsistema que solicita acceso mediante su certificado digital.
- 2) **Solicitud:** La entidad consumidora envía una petición al proveedor de servicios.
- 3) **Autorización:** El servidor central revisa si el solicitante tiene los permisos necesarios.
- 4) **Respuesta:** El proveedor procesa la solicitud y envía la información solicitada.
- 5) **Registro de Auditoría:** Cada paso del proceso es registrado para mantener la trazabilidad y seguridad.

## **Beneficios de esta Arquitectura:**

- **Seguridad:** Todas las transacciones están cifradas y autenticadas.
- **Flexibilidad:** El sistema permite la integración de múltiples participantes y servicios, adaptándose a diversas necesidades.
- **Eficiencia:** Optimiza el uso de recursos y facilita la colaboración entre entidades.
- **Gobernanza:** Su estructura descentralizada permite que la fuente auténtica de los datos tenga control sobre los accesos a sus servicios.
- **Trazabilidad:** Registra todas las transacciones para auditoría y seguimiento.

## **INFRAESTRUCURA EN AWS**

La infraestructura de X-Road en Amazon Web Services (AWS) está diseñada para ser altamente flexible, escalable y segura, asegurando que el sistema de interoperabilidad del Gobierno de la Provincia de Córdoba funcione de manera eficiente y confiable. Esta arquitectura sigue las mejores prácticas establecidas por AWS para garantizar alta disponibilidad, resiliencia y seguridad en todas las operaciones.

AWS proporciona una plataforma en la nube ideal para alojar X-Road, permitiendo que el sistema se adapte rápidamente a las necesidades cambiantes del gobierno y los ciudadanos, al mismo tiempo que asegura un entorno seguro y rentable para todos los datos intercambiados.

## **Componentes Clave de la Infraestructura en AWS**

### VPC (Virtual Private Cloud):

Toda la infraestructura de X-Road está aislada en una VPC (Virtual Private Cloud), que crea un entorno privado y seguro en la nube para los recursos de AWS, protegiendo los datos y servicios del sistema.

### Instancias EC2:

3 instancias t3.large distribuidas en 3 Zonas de Disponibilidad (AZs) para asegurar que el sistema esté siempre disponible, incluso en caso de fallo de alguna de las zonas.

Estas instancias ejecutan los servidores centrales y los servidores de seguridad de X-Road, que son responsables de gestionar la conectividad y los servicios entre las entidades públicas y privadas.

### Grupos de Seguridad y Configuración de Puertos:

Los grupos de seguridad están configurados para permitir solo el tráfico necesario, con puertos específicos abiertos para cada tipo de servicio. Por ejemplo:

Puerto 4000: Gestión de la interfaz de administración.

Puerto 4001: Gestión de claves y certificados.

Puerto 4002: Interfaz de servicios.

### Health Checks y Failover:

Se implementan Health Checks en Route 53 para monitorear la salud de las instancias de EC2. Si alguna instancia no está disponible, el tráfico se redirige automáticamente a las instancias saludables para asegurar que el sistema siga funcionando sin interrupciones.

### Security Server (Servidor de Seguridad):

El sistema incluye un Security Server en cada zona de disponibilidad, encargado de asegurar las transacciones y la autenticación entre los participantes del sistema. Este servidor utiliza TLS passthrough a través de un Application Load Balancer (ALB), lo que permite redirigir el tráfico de manera segura y eficiente.

### Base de Datos en Amazon Aurora:

Para almacenar la información de X-Road, se utiliza Amazon Aurora PostgreSQL, una base de datos relacional que ofrece replicación entre regiones, lo que asegura la alta disponibilidad y la recuperación ante desastres. Esto significa que, si una región de AWS falla, los datos siguen siendo accesibles desde otra región.

### Seguridad Adicional con AWS WAF:

Para proteger el sistema de posibles ataques, se implementa AWS Web Application Firewall (WAF), que ayuda a defenderse contra ataques DDoS y de



inyección SQL, garantizando que la infraestructura de X-Road se mantenga segura frente a amenazas externas.

### Bastion (Jump Box) para Acceso Seguro:

Para gestionar el acceso a los servidores, se utiliza una instancia Bastion (t3.micro) que permite acceder de manera segura a la infraestructura solo desde direcciones IP específicas, asegurando que el acceso remoto se mantenga controlado.

### Alta Disponibilidad y Recuperación Ante Desastres (DR)

Una de las ventajas clave de utilizar AWS para X-Road es la capacidad de recuperación ante desastres (DR). Para garantizar que el sistema esté siempre disponible, incluso en el caso de fallos en la infraestructura principal, se ha configurado un entorno de staging en una segunda región. Esto permite que, en caso de una caída en la región principal, el sistema pueda conmutar automáticamente a la segunda región sin afectar la operativa del sistema. Esta configuración se realiza a través de Route 53 con Fileover, que dirige el tráfico a la región secundaria si la principal no está disponible.

### Beneficios de la Infraestructura en AWS

**Escalabilidad Automática:** AWS permite ajustar los recursos del sistema de manera automática a medida que aumenta la demanda, lo que asegura que X-Road pueda manejar una mayor carga de trabajo sin problemas.

**Seguridad de Primer Nivel:** AWS proporciona herramientas de seguridad avanzadas, como cifrado de datos, autenticación de múltiples factores y monitoreo de actividad, que garantizan que los datos intercambiados a través de X-Road estén siempre protegidos.

**Optimización de Costos:** Gracias al modelo de pago por uso de AWS, los recursos se ajustan de manera dinámica, lo que permite reducir costos operativos al solo pagar por lo que realmente se utiliza.

**Alta Disponibilidad:** Con la configuración de instancias distribuidas en múltiples Zonas de Disponibilidad y la replicación de bases de datos entre regiones, la infraestructura de X-Road es resiliente y garantiza que el sistema esté siempre disponible, incluso en situaciones de fallo.



## Comparación con Infraestructuras Locales

Optar por AWS frente a infraestructuras físicas o centros de datos locales presenta varias ventajas significativas:

**Escalabilidad:** AWS permite aumentar o disminuir recursos según sea necesario, sin la necesidad de adquirir nuevo hardware, lo que es un proceso costoso y lento en infraestructuras físicas.

**Reducción de Costos:** El uso de servicios de nube elimina los costos iniciales y operativos relacionados con el mantenimiento de hardware, personal de gestión de servidores y actualizaciones de infraestructura.

**Mayor Resiliencia:** A diferencia de los centros de datos tradicionales, que pueden depender de una única ubicación física, AWS ofrece redundancia geográfica y recuperación automática ante fallos, lo que mejora la continuidad del servicio.

## Conclusión

La infraestructura de X-Road en AWS proporciona un entorno seguro, eficiente y escalable para el intercambio de datos entre entidades públicas y privadas en la Provincia de Córdoba. Gracias a los servicios avanzados de AWS, el sistema garantiza alta disponibilidad, seguridad y flexibilidad para adaptarse a las necesidades cambiantes del gobierno y de los ciudadanos. Además, la arquitectura está diseñada para ser rentable y fácil de gestionar, asegurando una implementación exitosa y sin interrupciones

# **PROCESO DE INTEGRACIÓN AL SISTEMA**

## **X-ROAD**

### **Registrarse como Organización Miembro**

Teniendo en cuenta la siguiente diferenciación:

<b>Organización Pública</b>	<b>Organización Privada</b>
Son entidades gubernamentales (municipios, ministerios, organismos descentralizados) que gestionan datos de interés público y ofrecen servicios esenciales a los ciudadanos.	Empresas, ONGs o instituciones educativas que participan en el ecosistema para consumir o proveer servicios digitales relacionados con actividades específicas.
Priorizan la interoperabilidad entre instituciones estatales y deben cumplir estrictamente con las normativas gubernamentales.	Su participación puede estar motivada por acuerdos con el gobierno o necesidades del sector privado.
Debe garantizar el acceso público a datos no confidenciales bajo normativas como leyes de transparencia.	Acceso limitado a servicios y datos sensibles según acuerdos de nivel de servicio (SLA).
Responsabilidades más estrictas respecto a la custodia y confidencialidad de datos personales.	Obligación de cumplir con los términos establecidos en contratos o convenios con el gobierno.

### **Organizaciones Públicas:**

Las Organizaciones Miembro (OM) públicas son entidades gubernamentales o descentralizadas que buscan integrarse al sistema X-Road para interoperar con otros organismos públicos. Este proceso permite que las entidades intercambien datos de manera segura y eficiente, mejorando la colaboración entre distintos organismos gubernamentales.

### **Etapas del Proceso:**

#### **Solicitud de Adhesión:**

La entidad interesada presenta una solicitud formal al Operador del Sistema X-Road de Córdoba, detallando la siguiente información:

El nombre y descripción de la entidad.

El propósito de la adhesión, por ejemplo: "Provisión de datos de Registro de Propiedad para consultas interinstitucionales".

Una lista inicial de servicios que la entidad planea ofrecer o consumir, como "Validación de Identidad".

### **La documentación requerida para la adhesión incluye:**

Un acta administrativa que autorice la integración.

Un certificado de firma digital emitido por ONTI.

Información técnica, como las direcciones DNS y IP del servidor, y el nombre del responsable técnico.

### **Evaluación Inicial:**

El operador del sistema X-Road realiza una evaluación inicial en la que verifica varios aspectos clave:

Que la entidad sea reconocida como pública según el marco legal vigente.

Que los servicios propuestos cumplan con los estándares de interoperabilidad y privacidad establecidos por el sistema.

Que la infraestructura técnica de la entidad sea compatible con X-Road.

### **Generación de Certificados:**

Una vez aprobada la solicitud, la entidad debe gestionar los certificados de autenticación y firma digital con ONTI. Además, es necesario solicitar los certificados TLS para proteger las conexiones entre los servidores y garantizar que las comunicaciones sean seguras.

### **Implementación Técnica:**

Durante la implementación técnica, se debe configurar un servidor de seguridad con la siguiente información:

La instalación de los certificados digitales necesarios.

El registro del servidor en el servidor central de X-Road.

Después de la configuración, se realizan pruebas iniciales para garantizar la conectividad entre el servidor de seguridad y el servidor central, y para verificar que los servicios de interoperabilidad estén funcionando de manera segura.

### **Capacitación y Puesta en Marcha:**

Una vez completada la implementación, es necesario capacitar al personal técnico en el uso de X-Road para que puedan gestionar adecuadamente los servicios y mantener el sistema operativo. Finalmente, se procede a publicar y habilitar los servicios en el portal de interoperabilidad del sistema, permitiendo su acceso a otras entidades que necesiten interactuar con esos servicios.

### **Ejemplo Práctico:**

Entidad: Registro General de la Propiedad de Córdoba.

Propósito: El Registro General de la Propiedad de Córdoba busca proporcionar servicios de validación de titularidad y registros de propiedad a otras entidades del gobierno provincial, como el Ministerio de Desarrollo Urbano y la Dirección General de Catastro.

Proceso: En este caso, la entidad pública presenta una solicitud al operador del sistema X-Road en Córdoba, detallando su intención de intercambiar datos del registro de propiedades con otras dependencias gubernamentales.

### **Organizaciones Privadas:**

Las Organizaciones Miembro (OM) privadas son empresas u organizaciones sin fines de lucro que desean integrarse al sistema X-Road para consumir o proporcionar servicios digitales específicos. Estas organizaciones pueden ser proveedores de servicios o consumir servicios que mejoren la eficiencia y la seguridad de sus operaciones.

## **Etapas del Proceso:**

### **Solicitud de Adhesión:**

La organización privada presenta una solicitud formal al operador del sistema X-Road, detallando la siguiente información: el nombre y descripción de la empresa, los servicios que planea consumir o proporcionar, como por ejemplo: "Validación de identidad para apertura de cuentas", y la información del servidor, incluyendo DNS, direcciones IP y el nombre del responsable técnico.

La documentación requerida incluye una copia del contrato o acuerdo que respalde la participación de la organización en el sistema, así como certificados de firma digital y TLS gestionados con un proveedor autorizado.

### **Evaluación Inicial:**

El operador del sistema X-Road realiza una evaluación inicial para verificar varios aspectos clave. En primer lugar, se confirma la validez legal de la organización privada y el propósito de su integración en el sistema. Además, se revisa que los servicios propuestos cumplan con los estándares técnicos requeridos, y se asegura de que la organización no tenga acceso a servicios restringidos para el sector público.

### **Implementación Técnica:**

Una vez aprobada la solicitud, se procede con la configuración del servidor de seguridad. Este servidor, generalmente virtual, se configura para reducir costos, manteniendo la seguridad del sistema. Se debe instalar los certificados digitales necesarios para autenticar la comunicación y, finalmente, registrar los servicios en el servidor central de X-Road.

### **Pruebas y Autorización:**

Se deben realizar pruebas para garantizar que la conectividad, la firma digital y la autenticación funcionen correctamente. Estas pruebas verifican que los servicios que la organización planea consumir o proporcionar estén alineados con los acuerdos establecidos y que se cumplan todos los requisitos técnicos y de seguridad.

### **Integración Continua:**

Después de superar las pruebas, se habilitan los servicios, y se realiza un monitoreo continuo para asegurar que se cumplan los requisitos del sistema y

que la integración siga funcionando correctamente. El monitoreo permite asegurar que la organización cumpla con las políticas y estándares de interoperabilidad establecidos por X-Road.

### **Ejemplo Práctico:**

Entidad: Banco Córdoba.

Propósito: El Banco Córdoba desea integrar su sistema con el Registro Nacional de las Personas (RENAPER) para validar la identidad de los clientes al abrir cuentas bancarias, mejorando la eficiencia y la seguridad de sus procesos.

Proceso: En este caso, el banco envía una solicitud formal al operador del sistema X-Road, detallando su intención de consumir datos del RENAPER para realizar validaciones de identidad en tiempo real al momento de la apertura de cuentas.

## **SERVIDOR DE SEGURIDAD**

El Servidor de Seguridad es uno de los componentes más importantes dentro de la infraestructura de X-Road, ya que su función principal es garantizar que todas las comunicaciones entre las Organizaciones Miembro (OM) y el Servidor Central sean seguras, autenticadas y cifradas. Este servidor es responsable de validar las transacciones, proteger los datos en tránsito y gestionar los certificados digitales utilizados para la firma y autenticación de las transacciones.

El Servidor de Seguridad juega un papel fundamental dentro de la arquitectura de X-Road, ya que asegura que las interacciones entre las OM se realicen de forma segura, permitiendo que los datos sensibles no sean expuestos a posibles vulnerabilidades. A lo largo de su funcionamiento, el servidor valida la identidad de las partes involucradas en el intercambio de información, cifra los datos durante su tránsito y garantiza que las transacciones sean verificables a través de auditorías posteriores.

En términos de funcionalidad, el Servidor de Seguridad se encarga de la autenticación y autorización de las entidades participantes, asegurándose de que solo los usuarios y organizaciones autorizados puedan acceder a los servicios de X-Road. Asimismo, maneja el cifrado de la comunicación, utilizando protocolos de seguridad como TLS para proteger la confidencialidad de los datos intercambiados entre las OM y el Servidor Central.

Además de la gestión de certificados, que son esenciales para la autenticación y firma digital de las transacciones, el Servidor de Seguridad también desempeña un rol crucial en el registro de auditoría. Todos los eventos y transacciones realizadas en el sistema se registran, lo que permite la trazabilidad de cada acción y facilita la detección de posibles incidencias de seguridad.

Dentro de la infraestructura de X-Road, el Servidor de Seguridad puede ser implementado como una instancia EC2 en AWS o en un entorno on-premise, dependiendo de los requerimientos del proyecto. En ambos casos, su configuración debe seguir buenas prácticas de seguridad para evitar accesos no autorizados. Por ejemplo, se recomienda restringir el acceso SSH solo a direcciones IP específicas y asegurarse de que todas las comunicaciones estén cifradas adecuadamente.

## INSTALACION DEL SERVIDOR DE SEGURIDAD

La instalación del Servidor de Seguridad es un paso crucial para garantizar el correcto funcionamiento de X-Road. A continuación se detallan los pasos para instalar y configurar el Servidor de Seguridad dentro de la infraestructura de X-Road en AWS, específicamente para la Provincia de Córdoba.

Para comenzar, es necesario cumplir con ciertos requisitos previos. Se necesita tener acceso a la Consola de AWS para crear una instancia EC2 en la VPC de X-Road. Se recomienda usar Ubuntu 24.04 LTS como sistema operativo base para la instancia EC2, debido a su compatibilidad con X-Road y su estabilidad. Además, la instancia EC2 debe ser de tipo t3.medium o superior, con un mínimo de 4 GB de RAM y 60 GB de almacenamiento en disco EBS. La instancia debe estar configurada en una subred privada para mantener la seguridad de la comunicación.

Una vez creada la instancia, se debe proceder con la instalación del servidor. Primero, es necesario actualizar el sistema y asegurarse de que todas las dependencias necesarias estén instaladas. Para ello, se pueden ejecutar los siguientes comandos:

```
sudo apt update
sudo apt upgrade -y
sudo apt install -y openjdk-11-jre-headless curl unzip
```

Luego, se debe proceder con la descarga de la última versión de X-Road Security Server desde el repositorio oficial, descomprimir el archivo y acceder a la carpeta de instalación:

```
wget https://github.com/ria-ee/X-Road/releases/download/v6.0.0/xroad-security-server-6.0.0.zip
```

```
unzip xroad-security-server-6.0.0.zip
```

```
cd xroad-security-server-6.0.0
```

Una vez descargado el software, es necesario configurar los certificados de seguridad para garantizar que las comunicaciones estén cifradas. Si no se cuenta con certificados emitidos por una autoridad de certificación, se pueden generar certificados autofirmados utilizando los siguientes comandos:

```
sudo openssl req -new -newkey rsa:2048 -days 365 -nodes -keyout /etc/xroad/keys/server.key -out /etc/xroad/keys/server.csr
```

```
sudo openssl x509 -req -days 365 -in /etc/xroad/keys/server.csr -signkey /etc/xroad/keys/server.key -out /etc/xroad/keys/server.crt
```

Con los certificados generados, es necesario configurar el Servidor de Seguridad para que se registre correctamente en el Servidor Central de X-Road. Esto se realiza utilizando el Member Class y Member Code proporcionados por el operador del sistema. La configuración de los nodos de seguridad también es esencial si se requiere manejar múltiples instancias. Asegúrese de que todos los nodos estén autenticados correctamente.

Una vez completada la instalación y la configuración, se deben realizar pruebas para verificar que la comunicación entre el Servidor de Seguridad y el Servidor Central sea exitosa. Se puede hacer una prueba simple utilizando el comando curl para verificar el estado del sistema:

```
curl -X GET https://[Servidor Central URL]/healthcheck
```



Por último, es fundamental realizar un mantenimiento continuo del Servidor de Seguridad, que incluya la renovación de certificados y la gestión de accesos a medida que se agregan nuevas Organizaciones Miembro o se realizan cambios en la infraestructura. Además, se debe monitorear el servidor utilizando herramientas como AWS CloudWatch para asegurarse de que el servidor funcione de manera estable.

## Requisitos Previos

Antes de proceder con la instalación del servidor de seguridad, es necesario cumplir con los siguientes requisitos:

El servidor de seguridad debe ser instalado en una instancia EC2 dentro de la VPC de X-Road en AWS. Se recomienda utilizar Ubuntu 24.04 LTS como sistema operativo base para la instancia EC2, ya que es compatible con X-Road y ofrece un entorno seguro y estable. La instancia EC2 debe ser del tipo t3.medium o superior, con un mínimo de 4 GB de RAM y 60 GB de almacenamiento en disco EBS. Además, el servidor debe tener acceso a Internet para descargar las dependencias y actualizaciones necesarias.

## Creación de la Instancia EC2

Para crear la instancia EC2, primero inicia sesión en la Consola de Administración de AWS, navega a la sección de EC2 y selecciona "Launch Instance" para crear una nueva instancia. A continuación, selecciona la imagen base Ubuntu 24.04 LTS o la imagen más reciente disponible para instancias EC2.

Elige el tipo de instancia t3.medium o superior, dependiendo de las necesidades de carga de trabajo. Configura la instancia en una subred privada dentro de la VPC de X-Road para asegurar que el servidor de seguridad no esté expuesto a Internet directamente. Asigna 60 GB de almacenamiento mínimo en disco EBS.

En cuanto a la configuración de seguridad, crea un Grupo de Seguridad que permita únicamente el acceso desde direcciones IP específicas (como las del administrador o los servidores centrales). Abre los puertos 443 (HTTPS) y 80 (HTTP) para permitir la comunicación con el servidor central y otras OM.

Una vez creada la instancia, conéctate a ella mediante SSH utilizando las credenciales adecuadas y comienza el proceso de instalación.

## Instalación del Software del Servidor de Seguridad

Primero, asegúrate de actualizar el sistema ejecutando los siguientes comandos en la instancia EC2:

```
sudo apt update  
sudo apt upgrade -y
```

A continuación, instala las dependencias necesarias para X-Road ejecutando el siguiente comando:

```
sudo apt install -y openjdk-11-jre-headless curl unzip
```

A continuación, instala las dependencias necesarias para X-Road ejecutando el siguiente comando:

```
sudo apt install -y openjdk-11-jre-headless curl unzip
```

Descarga la versión más reciente de X-Road Security Server desde el repositorio oficial con el siguiente comando:

```
wget https://github.com/ria-ee/X-Road/releases/download/v6.0.0/xroad-security-server-6.0.0.zip
```

Una vez descargado, descomprime el archivo y navega a la carpeta de instalación:

```
unzip xroad-security-server-6.0.0.zip  
cd xroad-security-server-6.0.0
```

## Configurar las Variables del Servidor de Seguridad

A continuación, se deben configurar las variables del servidor de seguridad. Define un nombre único para el servidor de seguridad que será utilizado dentro de X-Road. Configura las direcciones IP y los puertos según los requisitos de la infraestructura. Además, se deben generar certificados digitales para autenticar el servidor.

Si no se dispone de certificados emitidos por una autoridad confiable, puedes generar certificados autofirmados con los siguientes comandos:

```
sudo openssl req -new -newkey rsa:2048 -days 365 -nodes -keyout  
/etc/xroad/keys/server.key -out /etc/xroad/keys/server.csr
```

```
sudo openssl x509 -req -days 365 -in /etc/xroad/keys/server.csr -signkey  
/etc/xroad/keys/server.key -out /etc/xroad/keys/server.crt
```

## Configurar X-Road en el Servidor de Seguridad:

Una vez que se haya instalado el servidor de seguridad, se debe registrar el servidor en el servidor central de X-Road. Para hacerlo, se debe configurar el servidor para que se registre correctamente en el sistema, utilizando el Member Class y Member Code proporcionados por el operador del sistema.

Es necesario configurar los nodos de seguridad para gestionar múltiples instancias si es necesario. Para ello, edita el archivo de configuración y especifica el número de nodos que se utilizarán y asegúrate de que todos los nodos estén debidamente autenticados.

## Pruebas y Validación:

Una vez que el servidor de seguridad esté configurado, realiza pruebas para asegurarte de que la instalación ha sido exitosa. Para verificar la conexión entre el servidor de seguridad y el servidor central, puedes ejecutar el siguiente comando:

```
curl -X GET https://[Servidor_Central_URL]/healthcheck
```

Además, realiza pruebas de seguridad para asegurarte de que las comunicaciones estén protegidas por TLS y que los certificados estén

funcionando correctamente. Puedes utilizar herramientas como Postman o curl para estas pruebas.

Por último, para monitorear el estado de la instancia EC2, utiliza AWS CloudWatch y asegúrate de que el servidor de seguridad esté funcionando correctamente y sin fallos.

## **Mantenimiento y Actualización**

Es importante realizar mantenimientos regulares para asegurar la estabilidad del servidor de seguridad. Esto incluye la actualización de los certificados y la gestión de accesos para nuevos miembros. Las actualizaciones del software de X-Road también deben gestionarse periódicamente para garantizar que el sistema se mantenga seguro y eficiente.

### **Componentes del servidor de seguridad**

Los componentes del servidor se dividen en: componentes de configuración y componentes de gestión.

## ***Componentes de configuración del servidor de seguridad***

### **Componentes de Configuración del Servidor de Seguridad**

Dentro de la configuración del Servidor de Seguridad en X-Road, existen varias solapas o secciones que permiten gestionar aspectos clave del servidor, como los certificados y claves, el diagnóstico del sistema y la configuración general. Es importante destacar que estas configuraciones son críticas para el correcto funcionamiento del servidor y deben ser tratadas con precaución.

### **Solapa de Keys and Certificates (Claves y Certificados)**

La solapa Keys and Certificates es donde se gestionan los certificados digitales y las claves privadas utilizadas para autenticar y cifrar las comunicaciones del Servidor de Seguridad. Esta sección es crucial para la gestión de la seguridad dentro de X-Road, ya que asegura que las transacciones entre las Organizaciones Miembro (OM) y el Servidor Central sean validadas correctamente.

Durante la instalación inicial del servidor de seguridad, el responsable técnico debe configurar los certificados en esta sección. Los certificados deben ser generados o proporcionados por una Autoridad Certificadora (CA) confiable, o en su defecto, generados internamente si el sistema lo permite.

Una vez que el servidor está instalado y funcionando correctamente, no se recomienda realizar modificaciones en esta sección a menos que sea solicitado por el operador del sistema de interoperabilidad. Cualquier cambio en los certificados o claves puede afectar la seguridad y la operatividad del sistema, lo que puede resultar en la invalidación de las transacciones o en problemas de comunicación entre las partes involucradas.

### **Solapa de Diagnostics (Diagnóstico)**

La solapa Diagnostics proporciona herramientas y opciones para verificar el estado y monitorear el funcionamiento del Servidor de Seguridad. Aquí se pueden obtener registros detallados sobre el estado de los servicios, la integridad de los certificados, la conexión con otros servidores y las transacciones realizadas.

Es recomendable utilizar esta sección principalmente en las fases de configuración inicial y pruebas del servidor. Una vez que el servidor de seguridad esté en funcionamiento, el uso continuo de esta solapa no es necesario, excepto en situaciones de diagnóstico o para realizar auditorías de seguridad.

Como con la solapa de Keys and Certificates, no es recomendable realizar cambios en la configuración de diagnóstico una vez que el servidor ha sido configurado correctamente, a menos que se reciba una instrucción explícita del operador del sistema de interoperabilidad o de los responsables técnicos del sistema. Esto es para garantizar que los registros y diagnósticos no se alteren de forma inadvertida, lo que podría dificultar la resolución de problemas en el futuro.

### **Solapa de Settings (Configuración)**

La solapa Settings permite realizar configuraciones adicionales en el Servidor de Seguridad, como ajustar parámetros de red, personalizar el comportamiento del servidor y gestionar las conexiones a otras entidades o servidores.

Esta solapa debe ser utilizada principalmente durante la instalación inicial y configuración de los parámetros básicos del servidor, como las direcciones IP, los puertos y las configuraciones de red. Al igual que las secciones anteriores, se recomienda no realizar modificaciones una vez que el servidor ha sido configurado y está en producción, a menos que se reciba una solicitud del

operador del sistema de interoperabilidad o haya cambios en la infraestructura que lo requieran.

Cualquier cambio no autorizado en esta sección puede afectar la conectividad del Servidor de Seguridad con las Organizaciones Miembro y el Servidor Central, lo que podría interrumpir los servicios de interoperabilidad y comprometer la seguridad del sistema.