PROTOCOLO PARA EL ACCESO, USO Y APROVECHAMIENTO DEL SISTEMA MULTI-FUENTE SUITE

Índice

Capítulo I

Disposiciones Generales

1) Presentación

El Sistema Multi-Fuente es una herramienta de información multi institucional concebida por el Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (CNI-SESNSP), para apoyar el Modelo Nacional de Policía y Justicia Cívica (MNPyJC) que el Gobierno Federal construye para regresar la paz y seguridad de los ciudadanos de México; a través de la "Propuesta para el uso y explotación de la información de la inteligencia policial local" (Sistema Multi-Fuente) aprobada mediante Acuerdo Octavo de la Comisión Permanente de Información, de la Primera Sesión Ordinaria 2020.

El Sistema Multi-Fuente promueve y fortalece el uso de la información en materia de incidencia delictiva por parte de las instituciones de la Seguridad Pública y Procuración de Justicia de los tres niveles de gobierno a partir de dos premisas: **La primera** enfatiza que los Complejos de Seguridad y los Centros de Atención de Llamadas de Emergencia, generen información de incidencia delictiva lo más exhaustiva y apegada posible a la realidad. **La segunda** se centra en el uso que las instituciones de Seguridad Pública y Procuración de Justicia, hagan aprovechamiento de dicha información para la toma de decisiones estratégicas, tácticas, operativas y basadas en evidencia encaminadas a la prevención de actividades antisociales o delictivas.

En este sentido, el Sistema Multi-Fuente plantea tres objetivos fundamentales: (1) contar con una medición de la incidencia delictiva lo

más apegada a la realidad, (2) apoyar la toma de decisiones, basadas en evidencias, para la estrategia policial y (3) Generar un historial de cada delito desde el inicio del incidente hasta la probable integración con una carpeta de investigación.

Bajo este contexto, el Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, el Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, a través del Centro Estatal de Información, así como las Áreas de Tecnologías de la Información y Comunicación de la Secretaría de Seguridad Pública, la Fiscalía General Estatal y las Secretarías y/o Direcciones Generales de Seguridad Pública de los 11 municipios de la entidad, están llevado a cabo la planeación, desarrollo e implementación del Proyecto Multi-Fuente en Quintana Roo,

Como parte de las acciones para la implementación del proyecto en la entidad, el Centro Estatal de Información desarrollo el **Sistema Multi-Fuente Suite** con el objetivo de homologar los procesos de captura, disposición de datos y generación de información de seguridad pública proveniente de diversas fuentes de información, buscando hacer uso y aprovechamiento de estos datos en la investigación, la planeación y operación policial a nivel local.

El **Sistema Multi-Fuente Suite actualmente está integrado** por tres principales plataformas tecnológicas: Solomon, Xacbe y el Geoportal Municipal. Plataformas orientadas a garantizar la gestión, administración y representación de información de las instancias de seguridad pública y procuración de Justicia del gobierno, a nivel federal, estatal y municipal.

Por lo anterior, el presente documento tiene como objetivo brindar a las instancias estatales y municipales de seguridad pública y procuración de justicia, los mecanismos administrativos y técnicos, así como las reglas de

operación para el acceso, uso y aprovechamiento de las plataformas tecnológicas que conforman el proyecto Multi fuente. (Miranda, 2020)

2) Marco Jurídico

El artículo 21, párrafo noveno de la Constitución Política de los Estados Unidos Mexicanos, dispone que la seguridad pública es una función a cargo de la **federación, las entidades federativas y los municipios,** que comprende la prevención de los delitos, la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas en los términos de la ley y en las respectivas competencias que la Constitución señala.

La Ley General del Sistema Nacional de Seguridad Pública, reglamentaria del artículo 21 de la Constitución Política de los Estados Unidos Mexicanos en materia de Seguridad Pública, ordena en sus artículos 117 y 118 que la federación, las entidades federativas y los municipios serán responsables **de integrar y actualizar el Sistema Nacional de Información (SNI),** así como las bases que integran dicho sistema.

El Reglamento del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, en su artículo 12, fracción VII, establece que el Centro Nacional de Información tiene la facultad para determinar las **estrategias tendientes a satisfacer las necesidades de información y procesamiento de datos requeridos por las Instituciones de Seguridad Pública.** (Miranda, 2020)

El Secretariado **Ejecutivo del Sistema Estatal de Seguridad Pública (SESESP)**. De conformidad con el artículo 6 fracciones III, V, XVI, XVII y XIX de la Ley que crea el Organismo Público Descentralizado denominado Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública del Estado

de Quintana Roo, cuenta con las atribuciones de: concertar los esfuerzos de las instancias que participan en materia de Seguridad Pública y la efectiva implementación de políticas, estrategias y programas, a fin de garantizar el cumplimiento de los principios constitucionales y el respeto a los derechos humanos; asesorar y proponer políticas, lineamientos y acciones a aplicar, para el buen desempeño de las Instituciones de Seguridad Pública; Dictar las medidas necesarias para garantizar el adecuado funcionamiento del Sistema Estatal de Seguridad Pública de Quintana Roo; brindar asesoría a las Instituciones de Seguridad Pública para la integración de información, interconexión, acceso, uso, intercambio y establecimiento de medidas de seguridad para las bases de datos y, dar seguimiento al cumplimiento de las obligaciones relacionadas con las bases de datos de las distintas Instituciones de Seguridad Pública al Centro Nacional de Información del Sistema Nacional de Seguridad Pública.

El Centro Estatal de Información de Quintana Roo (CEIQROO), como unidad administrativa que apoya al SESESP en el cumplimiento a los objetivos del Programa Institucional del SESESP, fortalece los procesos de acopio, análisis e intercambio de información de las bases de datos y registros del Sistema Estatal de Información de Seguridad Pública, que contribuya con datos de calidad para la operación de las instituciones de seguridad pública estatal, municipal y de la fiscalía general del Estado.

En este contexto, el 6 de octubre del 2021, se firmó el Convenio para la Implementación del Sistema Multi-Fuente entre el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, la Secretaría de Seguridad Pública Estatal, la fiscalía general del Estado y el Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

3) Objetivos

a) General

Contar con un instrumento que homologue los criterios administrativos y técnicos, así como las reglas de operación para el acceso, uso y aprovechamiento del Sistema **Multi-Fuente Suite** en el estado de Quintana Roo.

b) Específico

- Medir, lo mas apegada a la realidad, la incidencia delictiva y contribuir a la toma de decisiones, basadas en evidencia.
- Establecer los procedimientos que debe seguir el personal de las áreas encargadas de plataforma México en los municipios para el uso del Sistema **Multi-Fuente Suite.**
- Fortalecer la coordinación y colaboración entre las instituciones de seguridad pública y procuración de justicia a nivel federal, estatal y municipal.
- Homologar los indicadores y registros que sean inherentes a la incidencia delictiva entre las instituciones de seguridad pública y procuración de Justicia a nivel estatal y municipal.
- Proporcionar los criterios administrativos y técnicos, así como las reglas de operación para el acceso, uso y aprovechamiento del Sistema **Multi-Fuente Suite.**

4) Glosario

Para los efectos del presente protocolo, se entenderá por:

I. **Activo crítico:** A las bases de datos e infraestructura tecnológica, que permiten la prestación de servicios gubernamentales estratégicos;

II. **CEIQROO**: Al Centro Estatal de Información de Quintana Roo perteneciente al Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, el cual será responsable de la implementación, actualización y administración del **Sistema Multi-Fuente Suite;**

III. **Derecho de acceso:** al permiso para el uso del servicio de datos en el **Sistema Multi-Fuente Suite**;

IV. **e-stamp:** es un conjunto de datos electrónicos de integridad que cumple como sello electrónico;

V. **Instancias:** A las instituciones de seguridad pública y procuración de justicia federal, estatal y municipal.

VI. **Intermediario del servicio de datos:** al miembro que permite que personal autorizado de su organización acceda al servicio de datos a través de su sistema de información;

VII. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

   a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

   b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

   c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

   d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

VIII. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos y

los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos;

IX. **Mensaje:** al conjunto de información que se intercambia entre un proveedor de servicios de datos y un usuario;

X. **Miembro:** instancias que estén interconectadas y hagan uso del **Sistema Multi-Fuente Suite;**

XI. **Protocolo de mensajes:** es una parte del **Protocolo del Sistema Multi-Fuente** Suite que permite a los miembros procesar mensajes;

XII. **Protocolo del Sistema Multi-Fuente Suite:** es un conjunto de reglas que garantiza el funcionamiento del intercambio seguro de datos a través de una red informática;

XIII. **Proveedor de servicios de certificación aprobado**: proveedor de un servicio de confianza aprobado, que proporciona al menos los siguientes servicios de confianza aprobados: servicio de certificado de autenticación del servidor de seguridad, servicio de certificado

de firma de un miembro y servicio de validación de certificados (OCSP).

XIV. **Proveedor de servicios de datos:** al miembro que proporciona servicios de datos a otros miembros;

XV. **Registro de consultas:** a la parte del servidor de seguridad basado en el **Protocolo del Sistema Multi-Fuente Suite**, donde se almacenan los mensajes intercambiados confirmados por e-stamp.

XVI. **Responsable:** el personal que actúan en el tratamiento de los datos, aprovechamiento y responden como operadores y/o administradores del **Sistema Multi-Fuente Suite;**

XVII. **Servicio de datos (WS):** al servicio para los miembros a través del cual se realiza el intercambio de datos basado en Internet;

XVIII. **Servidor de seguridad:** a la puerta de entrada la solución de software de comunicación de la plataforma Xacbe;

XIX. **Sistema:** a la parte tecnológica y organizativa definida por el sistema de información de un miembro para la provisión o uso de servicios de datos;

XX. **Sistema de información**: un sistema que incluye el procesamiento de información tecnológica y organizativa de un miembro. El sistema de información utiliza y/o proporciona servicios.

XXI. **Sistema Multi-Fuente:** A la herramienta de información multiinstitucional, para apoyar el Modelo Nacional de Policía y Justicia Cívica (MNPyJC) a través de la “Propuesta para el uso y explotación de la información de la inteligencia policial local”.

XXII. **Sistema Multi-Fuente Suite:** A las plataformas tecnológicas que lo integran:

- **a. Xacbe:** Plataforma tecnológica que permite el intercambio de datos de forma segura;

b. Solomon: Plataforma tecnológica para la captura, acopio y aprovechamiento de los datos de seguridad pública.

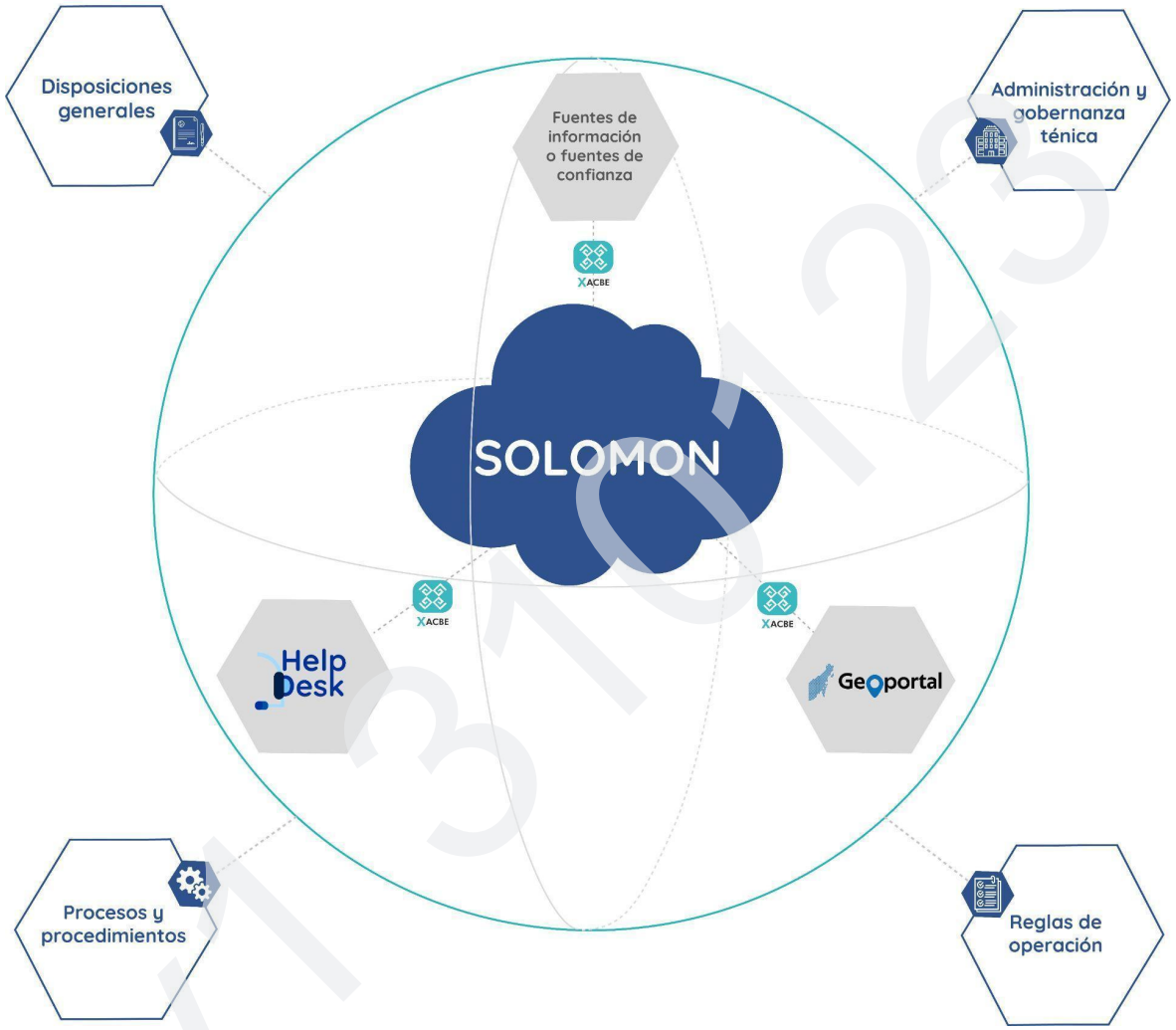
c. Geoportal de Seguridad Pública Municipal (Geoportal): Plataforma tecnológica para la visualización, consulta y generación de reportes cartográficos y estadísticos de incidencia delictiva municipal.

XXIII. Usuario de servicio de datos: al miembro que usa el servicio de datos;

XXIV. Usuario final del servicio de datos: a la persona física que utiliza el servicio de datos a través del sistema de información del miembro;

5) Arquitectura del Sistema Multi-fuente Suite

ARQUITECTURA DE MULTIFUENTE SUITE PARA USO Y APROVECHAMIENTO



Esquema 1. *Arquitectura del Sistema Multi-Fuente Suite para uso y aprovechamiento de información.*

Fuente: Aportación propia.

Capítulo II

Administración y gobernanza técnica

1) Principios Generales

Los principios de la administración del **Sistema Multi-Fuente Suite** son los siguientes:

I. **Independencia de la plataforma y la arquitectura:** permite que un miembro se comunique con el proveedor de servicios de datos a través del sistema de información sin importar lo heterogéneo que pueda resultar el mismo;
II. **Multilateral**: brinda la posibilidad de que un miembro solicite acceso a todos los servicios de datos proporcionados por otros miembros;
III. **Apertura y Estandarización:** se utilizan estándares y protocolos en la gestión y desarrollo;
IV. **Seguridad:** al intercambiar datos, la integridad, disponibilidad y confidencialidad de los datos se mantienen.

Esquema 2. *Administración y gobernanza técnica.*

Fuente: Aportación propia.

2) Funciones de la Administración (CEIQROO)

Para la administración del **Sistema Multi-Fuente Suite**, el CEIQROO tendrá las siguientes funciones:

I. Gestionar la información en el entorno de producción y prueba de los miembros, los servidores de seguridad registrados y los sistemas conectados.
II. Garantizar la disponibilidad de la información necesaria para el establecimiento del canal de intercambio seguro de datos y los servicios de datos en el servidor de seguridad del miembro;
III. Organizar y atender las solicitudes para ingresar al sistema y al servidor de seguridad;
IV. Asegurar el acceso y la disponibilidad al Sistema Multi-Fuente Suite;
V. Supervisar el uso del Sistema Multi-Fuente Suite y recopilar estadísticas de uso;
VI. Supervisar y coadyuvar en la solución de los incidentes de seguridad relacionados con las plataformas del Sistema Multi-Fuente Suite;
VII. Configuración de los niveles de acceso a los miembros;
VIII. Asesorar a los miembros para asuntos relacionados con Sistema Multi-Fuente Suite;
IX. Notificar a los miembros, a través de un correo electrónico, y/o medio electrónico acordado, sobre los cambios en la administración o uso del Sistema Multi-Fuente Suite y de todas las circunstancias conocidas o trabajos de mantenimiento que impidan su uso;
X. Gestionar y organizar la conexión del entorno del Sistema Multi-Fuente Suite con otros entornos de intercambio de datos;
XI. Brindar a los miembros software oficial y/o actualizaciones.
XII. Garantizar el cumplimiento del servicio, la disponibilidad de datos y mensajes para los miembros;
XIII. Coadyuvar en la implementación de proyectos para el desarrollo y mejora del Sistema Multi-Fuente Suite y asegurar su integridad arquitectónica, así como su seguridad;
XIV. En el caso de incumplimiento especificado en la regla octava fracción III, suspender del servidor de seguridad del miembro los accesos al Sistema Multi-Fuente Suite, y la disponibilidad de información necesaria para el uso del servicio de datos;

XV. Gestionar y desarrollar las soluciones necesarias para el registro de miembros, el servicio de confianza y para el funcionamiento, así como la supervisión de servicios, a fin de garantizar el funcionamiento del Sistema Multi-Fuente Suite.

XVI. Al cumplir con la obligación de notificación descrita en la fracción IX de la presente, el CEIQROO cumplirá con los siguientes períodos de notificación:

A. Para un cambio en la administración o uso del Sistema Multi-Fuente Suite o mantenimiento planificado se notifica con 15 días hábiles de anticipación;

B. Para la notificación de un cambio extraordinario en la gestión y el uso del Sistema Multi-Fuente Suite y el trabajo de mantenimiento no planificado, el CEIQROO tiene derecho a notificar con 5 días hábiles de anticipación;

C. Para un cambio en el protocolo base o el protocolo de mensaje del Sistema Multi-Fuente Suite que causa cambios en el sistema o servicio de datos del miembro se notificará con un mes de anticipación.

Capítulo III

Procesos y procedimientos

1) Registro de miembros para uso y aprovechamiento de servicios

I. Para registrarse, un miembro, se deberá presentar una solicitud vía correo electrónico con la siguiente información:

A. Demostrar que está suscrito al Convenio para Implementación del Sistema Multi-Fuente Suite;

B. Oficio dirigido al titular del CEIQROO, asignado a una persona para fungir como responsable del funcionamiento del sistema, como contacto y como administrador del Sistema Multi-Fuente Suite;

C. Brindar un escrito de las donde se describa el estatus de las medidas que cuenta el miembro para garantizar la integridad, trazabilidad, la confidencialidad y la disponibilidad de datos, con el fin de mitigar los riesgos relacionados con la seguridad, y se permita la realización de una auditoría, independientemente de las medidas que deberán ser aplicadas.

II. Después del registro, se requiere que el miembro registrado, envíe mediante oficio dirigido al titular del CIEQROO los siguientes datos:

A. Definición de usuarios que tendrán derecho a usar el Sistema Multi-Fuente Suite y, por lo tanto, los servicios de datos a utilizar, para permitir el acceso solo a personas autorizadas;
B. Escrito donde exista el compromiso de garantizar el funcionamiento seguro e ininterrumpido del Sistema Multi-Fuente Suite y al cumplimiento del acuerdo sobre el uso del servicio de datos entre los miembros.

2) Objeto de negación de servicios

El CEIQROO podrá rechazar una solicitud para unirse al Sistema Multi-Fuente Suite bajo los siguientes supuestos, si:

I. El solicitante no ha presentado la documentación necesaria que acredite su derecho de representación o el solicitante no tiene el derecho de representación para la presentación de la solicitud de acceso a la plataforma;
II. La información presentada al momento de la solicitud no está registrada o la información no está actualizada;
III. El solicitante o su sistema de información no cumple con otros requisitos establecidos en el presente Protocolo o los principios de funcionamiento del Sistema Multi-Fuente Suite.

El CEIQROO se reservará el derecho de admisión de una solicitud de registro cuando se haga incumplimiento de alguno de los términos anteriores que pongan en riesgo o que comprometan la integridad, disponibilidad y confidencialidad de la información y de la operatividad del sistema Multi-Fuente suite.

3) Requerimientos mínimos por parte del Miembro

Para garantizar el intercambio, acopio seguro y estandarizado de datos en el **Sistema Multi-Fuente Suite**, cada miembro deben cumplir las siguientes condiciones:

I. Haber implementado un canal seguro para intercambio de datos;
II. Garantizar la integridad del intercambio de datos con un sello electrónico "**e-stamp**";
III. Contar con al menos una conexión estable a internet;
IV. Cumplir con los requisitos para la prestación de servicios de datos;
V. Tener identificados a sus usuarios del servicio de datos, así como contar con un acuerdo sobre el uso del servicio de datos y la concesión del derecho de acceso con los mismos.
VI. Haber definido un enlace como responsable de recibir y responder las notificaciones que el CEIQROO realice mediante los canales oficiales.

4) Término de la afiliación de un Miembro.

Se procederá a dar por terminada la afiliación, en los siguientes supuestos:

I. Un miembro tiene el derecho a cancelar su afiliación en cualquier momento mediante la presentación de una solicitud escrita dirigida al Titular del CEIQROO.
II. Si la fecha de finalización del convenio no se indica en la solicitud especificada en la fracción I de la presente regla, la membresía finalizará el día hábil siguiente a la recepción de la solicitud antes mencionada.

III. El CEIQROO tiene el derecho de terminar inmediatamente el convenio o restringir los derechos derivados al mismo o establecer un plazo para la eliminación si:
   A. El miembro viola las condiciones establecidas en las presentes reglas, el acuerdo de conexión o el procedimiento de mediación del servicio de datos;
   B. El miembro ha enviado información incorrecta, incompleta o pone en riesgo la secrecía.
   C. Eliminar un sistema registrado, así como revocar permisos, actualizaciones, soporte y altos privilegios si el miembro pone en riesgo o comprometa la integridad, disponibilidad y confidencialidad de la información y de la operatividad del sistema Multi-fuente suite.

IV. El **CEIQROO** tiene el derecho de dar por terminada la membresía notificando al miembro vía correo electrónico, con 5 días calendario de anticipación

Capítulo IV

Reglas de Operación

1) Operación de miembros

Para garantizar la correcta operación y funcionamiento del Sistema Multi-Fuente Suite, los miembros deberán cumplir las siguientes medidas:

I. Cumplir con lo fijado en el Convenio Específico de Coordinación, de Colaboración y las disposiciones legales que le sean aplicables, en virtud del uso de información clasificada como confidencial y/o reservada.
II. Garantizar la continuidad, gestión, desarrollo y operación segura e ininterrumpida de su sistema de información al unirse al Sistema Multi-Fuente Suite;

III. Garantizar el intercambio de datos seguro y estandarizado, previsto en la regla séptima y adaptar su sistema de información para que funcione en el entorno del Sistema Multi-Fuente Suite;
IV. Implementar medidas de seguridad físicas y medidas de seguridad técnicas para garantizar la integridad, trazabilidad, confidencialidad y disponibilidad de datos con el fin de mitigar los riesgos relacionados con la seguridad y permitir la realización de una auditoría independientemente de las medidas implementadas;
V. Cumplir con las recomendaciones o instrucciones emitidas por el CEIQROO;
VI. Mantener actualizados los sistemas de información que de ellos dependa;
VII. Informar de inmediato al CEIQROO sobre cualquier problema relacionado con el uso del Sistema Multi-Fuente Suite o alguna circunstancia que pueda afectar el cumplimiento de las obligaciones del CEIQROO y de un miembro;
VIII. Notificar inmediatamente al CEIQROO sobre algún incidente de seguridad relacionado con el Sistema Multi-Fuente Suite y su peligro inmediato;
IX. Remitir al CEIQROO las solicitudes y la información especificada en la regla sexta, a través o medio convenido;
X. Presentar al CEIQROO la información necesaria para la evaluación de la seguridad del servidor, las reglas de seguridad y una descripción de las medidas implementadas.
XI. Remitir al CEIQROO, a través de los medios establecidos, los datos de los responsables, así como el esquema de privilegios del usuario y las actividades que requiere con motivo de sus funciones;
XII. El mantenimiento a una base de datos de un miembro deberá contemplar medidas y acciones para garantizar la protección de la información y la prestación de servicios ya que se considera como un activo crítico.
XIII. Los equipos destinados para la implementación de Multi-fuente suite deberán ser empleados para lo cual han sido concebidos.

2) Obligaciones de los miembros

Para permitir la implementación y uso de un canal seguro de intercambio de datos el miembro deberá observar lo siguiente:

I. Instalar en su sistema de información el software de Servidor de Seguridad como mecanismo de intercambio de datos y registrar el certificado de autenticación de servidor de seguridad en el CEIQROO.
II. Usar solo el software aprobado por el CEIQROO.
III. Al usar un servidor de seguridad, se requiere que el miembro:
    A. Garantice la existencia de un registro de solicitud de mensajes intercambiados con el sello electrónico;
    B. Determine las personas que, y bajo qué condiciones, tendrán acceso al registro de consultas, así como la administración;
    C. Garantice los mismos requisitos de confidencialidad para el procesamiento de mensajes que se requieren para el uso del servicio de datos;
    D. Alojar los activos críticos en territorio y bajo la jurisdicción de los Estados Unidos Mexicanos.
    E. Un servidor de seguridad puede estar alojado fuera del territorio bajo la jurisdicción de los Estados Unidos Mexicanos sólo con el permiso del CEIQROO y si el miembro asegura el cumplimiento de las obligaciones establecidas en la regla quinta fracción IV;
IV. Al usar un servidor de seguridad aprobado, además de cumplir con las obligaciones especificadas, también deberá:
    A. Usar el software del servidor de seguridad de acuerdo con las instrucciones del CEIQROO;
    B. Actualizar el software del servidor de seguridad a más tardar dos meses después de que el CEIQROO ponga a disposición las actualizaciones de software.
V. Al compartir su servidor de seguridad con otro miembro, utilizará una conexión cifrada y autenticación bidireccional para conectar el servidor de seguridad y el sistema.

3) Integridad de los datos

Se garantizará la integridad del intercambio de datos con sello electrónico si existen los siguientes requisitos:

I. El intercambio de datos y la identificación de la conexión entre un mensaje y un miembro, se realiza mediante la plataforma Xacbe.
II. Servicio de certificación es a través del CEIQROO el cual emite el certificado de sello electrónico;
III. Servicio de confirmación de validez del certificado través del CEIQROO;
IV. Servicio de sello de tiempo través del CEIQROO;
V. Un sello electrónico es válido si la diferencia de tiempo entre la confirmación de validez del certificado utilizado y el sello de tiempo no excede las ocho horas;
VI. Un miembro tiene prohibido procesar datos intercambiados que no pueden confirmarse con el sello electrónico.

4) Prestación de servicios

Los requisitos para la prestación de servicios web son:

I. Cumplir con el protocolo establecido por el CEIQROO;
II. Una descripción del servicio web, que cumpla con los requisitos que emita el CEIQROO, el cual contenga información sobre las medidas de seguridad necesarias para su uso teniendo en cuenta la composición y la naturaleza de este;
III. También se puede usar en el entorno de prueba de ser necesario.
IV. Provisión o uso de servicios de datos a través de su sistema de información.

5) Mediación de servicios entre miembros

El procedimiento para la mediación de los servicios de datos incluirá:

I. La utilización de Xacbe para la mediación de datos;
II. El procedimiento para la autenticación indirecta y la autorización del miembro que utiliza el servicio de datos;
III. El procedimiento para archivar el registro de autenticación y autorización utilizando el servicio de datos y el término para mantener el registro;

IV. El procedimiento para archivar el registro de consultas y acceder al mismo, así como el plazo de almacenamiento.

6) Intermediario de servicios de datos

Como intermediario de servicios de datos, un miembro debe:

I. Seguir el procedimiento de intermediación de servicios de datos establecido;
II. Notificar al CEIQROO y al proveedor del servicio de datos, a cuyo uso el intermediario tiene derecho de acceso, del cambio en el procedimiento de mediación del servicio de datos;
III. Conocer los derechos y obligaciones entre las partes especificadas en los acuerdos especificados en la regla primera y tercera y determinar la admisibilidad de la mediación de los servicios de datos;
IV. Divulgar servicios de información de datos a los participantes por el sistema, si así se solicitara, de acuerdo con el protocolo de mensajes.

7) Sello electrónico

Para garantizar la integridad del intercambio de datos con sello electrónico se requiere cumplir con las siguientes especificaciones:

I. Se requiere un proveedor de servicios de datos para garantizar la integridad del intercambio de datos con un sello electrónico.
II. El usuario de un servicio de datos deberá garantizar la integridad del intercambio de datos con un sello electrónico.

Transitorios

PRIMERO. - El presente entrará en vigor al día siguiente de su firma.

SEGUNDO. - La implementación de las acciones derivadas de la entrada en vigor del presente deberá realizarse con los recursos humanos, materiales y presupuestarios asignados a las dependencias, por lo que no implicará erogaciones adicionales.