REGLAMENTO DEL FUNCIONAMIENTO DE LA CAPA DE INTERCAMBIO DE DATOS DE GOBIERNO

SECRETARÍA TÉCNICA Y PLANIFICACIÓN DE LA PRESIDENCIA

GOBIERNO DE EL SALVADOR

FEBRERO DE 2019

OBJETIVO

El presente Reglamento establece los requisitos, reglas de uso y procedimientos de gestión para la capa de intercambio de datos que implementa la integración de información y posibilita la automatización de servicios.

Ámbito de Aplicación

Instituciones del Órgano Ejecutivo del Gobierno de El Salvador y aquellas instituciones del Estado que acuerden cumplir con las disposiciones de este reglamento.

Cada institución es responsable de garantizar la calidad y el acceso a sus datos de acuerdo a la Ley de Acceso a la Información Pública y la Política Nacional de Datos Abiertos.

Definiciones: Los términos utilizados en el Reglamento tienen los siguientes significados:

Autoridad Central: Entidad responsable de la implementación y gestión de la capa de intercambio de datos de Gobierno. La dirección de Gobierno Electrónico en la Secretaría Técnica y de Planificación de la presidencia cumple actualmente esta función.

Capa de Intercambio de Datos (CID) de Gobierno: Conjunto de instituciones que participan en una red distribuida para intercambiar datos de forma segura siguiendo reglas y estándares consensuados.

Cliente de servicio: Miembro que participa en la red de intercambio para usar los servicios disponibles.

DGE: La Dirección de Gobierno Electrónico, en la Secretaría de Planificación de Presidencia.

Estampa de Tiempo: Sello electrónico que contiene la fecha y hora nacional según el Centro de Investigaciones Metrológicas de El Salvador. Este sello garantiza un registro fiel del momento en que se dio una transacción y es uno de los servicios disponibles en la Autoridad Certificadora de SETEPLAN.

Mensaje: Conjunto de datos que aplican formatos estándar y que son enviados desde un proveedor de servicio a un cliente a través de la red CID.

Miembro: Cualquier institución o persona que cumplido con los protocolos de registro para unirse a la red de servicios disponibles en la CID.

Proveedor de servicios de datos: Miembro de la CID que proporciona servicios de datos a otros miembros.

Protocolo de Mensaje de CID: Conjunto de reglas que garantizan el intercambio seguro de datos a través de una red de computadoras.

Registro de consultas: Es un servicio integrado al servidor de seguridad de un Miembro de la red CID. El registro contiene los mensajes enviados y recibidos, cada uno sellado con una Estampa de Tiempo.

Servidor de seguridad: Solución de software que permite crear o consumir información usando el Protocolo de Mensaje de la Tenoli.

Servicio: Cualquier servicio proporcionado por un miembro de la red para implementar el intercambio siguiendo reglas acordadas previamente con otros miembros.

Tenoli: Solución informática que implementa la CID y conecta a las entidades usando Firma Electrónica Simple. Tenoli es una solución libre cuya gestión esta distribuida entre los miembros de la red.

Usuario final: Persona física que utiliza el servicio de datos a través del sistema de información de un miembro de Tenoli.

Dentro de este documento los términos CID y Tenoli son equivalentes.

Principios de Gestión

La capa de intercambio de datos implementada a través de la plataforma Tenoli con el apoyo de la DGE se regirá bajo los siguientes principios:

a) **Independencia Tecnológica:** Los miembros podrán integrarse y comunicarse entre ellos sin importar el lenguaje de desarrollo, las aplicaciones involucradas o el uso de soluciones libres o comerciales.
b) **Acceso Pleno:** Cada miembro puede solicitar acceso a todos los servicios de datos que estén disponibles en la capa de intercambio.
c) **Apertura y Estandarización:** La capa de intercambio aplicará estándares y protocolos internacionales y estará disponible para ser mejorada según sea necesario.
d) **Seguridad de la Información:** La integridad, disponibilidad y la confidencialidad de los datos no se verán afectados al usar la red de intercambio.

Registro y Gestión de Membresía

Registro de Miembros

a) El registro de un nuevo miembro, que tendrá acceso a la CID de gobierno, es necesario completar un acuerdo de adhesión. El Acuerdo de Adhesión fija los derechos, obligaciones y responsabilidades de las partes. Este documento debe ser firmado por la máxima autoridad de la entidad y será enviado a la Dirección de Gobierno Electrónico: https://gobiernoelectronico.gob.sv/adhesion-tenoli

b) La membresía otorga el derecho a utilizar la CID para obtener o compartir datos de forma segura de acuerdo al procedimiento previsto en el presente Reglamento y en el Acuerdo de Adhesión.

Denegación de Registro de Miembro

La solicitud de membresía podrá ser rechazada si:

a) El solicitante no tiene un identificador único (código presupuestario de Hacienda) para el cual se pueda emitir un certificado electrónico.
b) El solicitante no esta autorizado para presentar la solicitud.
c) El solicitante o su sistema de información no cumple con los demás requisitos de este Reglamento.

Terminación de Membresía

Los miembros registrados tienen derecho a cancelar su membresía en cualquier momento mediante la presentación de una solicitud por escrito especificando la fecha en que se desea hacer efectiva la solicitud. Por otro lado, la administración de Tenoli tiene el derecho de rescindir la membresía inmediatamente o de limitar los derechos derivados de la membresía si:

i) Un miembro de Tenoli infringe las condiciones establecidas en este Reglamento, el Acuerdo de Adhesión o el procedimiento para la entrega de servicios de datos.
ii) El miembro usó información falsa o incompleta para obtener su membresía.

Para estos casos se cancelará la membresía previa notificación con 30 días calendario de anticipación.

Autoridad Central Responsable

La Autoridad Central que administra la CID es responsable de:

a) Mantener actualizada la información sobre: los miembros registrados, los servicios disponibles y los servidores de seguridad conectados a la red.
b) Diseñar y procesar aplicaciones para el registro de nuevos miembros y sus componentes.
c) Garantizar la disponibilidad de los servicios necesarios para el funcionamiento de la capa de intercambio de datos de gobierno.
d) Monitorear el uso de la plataforma y recopilar estadísticas de uso.
e) Responder a incidentes de seguridad.
f) Limitar los derechos del miembro en los casos previstos en el presente Reglamento.
g) Asesorar a miembros sobre cuestiones relacionadas con el uso de la plataforma.

h) Informar a los miembros de la red sobre cualquier cambio en la administración y/o sobre cualquier incidente o trabajo de mantenimiento mediante el envío de un correo electrónico usando los contactos registrados de cada miembro.
i) Gestionar y organizar la conexión de servicios de entidades externas al Órgano Ejecutivo, según se requiera.
j) Garantizar a los miembros el acceso gratuito a la CID y sus servicios.
k) Preparar e implementar proyectos de desarrollo de infraestructura para mejorar la CID y garantizar la integridad de la plataforma
l) Aplicar el cese de membresía por las causas dispuestas en este Reglamento
m) Monitorear, garantizar el funcionamiento y la continuidad de los servicios de la plataforma.

Plazos y Notificaciones

La DGE esta encargada de aplicar los plazos y notificar en caso de:

a) Cambio en la administración o trabajos de mantenimiento planificados, se notificarán con un mes de anticipación.
b) Cambios en los protocolos de mensajes que impliquen cambios en los servicios de datos administrados por los miembros, se notificará con 12 meses de anticipación.
c) Podrá usarse a un período de notificación más corto en caso de un cambio de emergencia o de un mantenimiento no planificado.

Responsabilidad de los Miembros

Los miembros debidamente registrados y autorizados para usar la CID de gobierno son responsables de:

a) Garantizar el desarrollo y funcionamiento, la continuidad y seguridad de sus servicios de consulta electrónica de datos de gobierno.
b) Aplicar las recomendaciones de seguridad y estándares sugeridos en los Estándares de Interoperabilidad de la DGE (https://egobsv.github.io/EstandaresInteroperabilidad/).
c) Implementar medidas para garantizar la integridad de los datos, la confidencialidad y la disponibilidad para mitigar los riesgos de seguridad, y recibir una auditoría independiente de la Corte de Cuentas de la República.
d) Aplicar los lineamientos remitidos por la Autoridad Central.
e) Mantener actualizados su registro ante la Autoridad Central.
f) Notificar a la Autoridad Central inmediatamente cualquier problema relacionado con el uso de la red de intercambio y cualquier circunstancia que pueda afectar el desempeño de los deberes de la Autoridad Central o de los demás miembros de la red.
g) Informar inmediatamente a la Autoridad Central sobre incidentes de seguridad.
h) Enviar solicitudes y la información mencionada en el literal f) a la Autoridad Central a través de Correspondencia Oficial y correo electrónico.

i) Proporcionar, a solicitud de la Autoridad Central, la información, las reglas de seguridad y las medidas tomadas para evaluar la seguridad del servidor de seguridad.

Seguridad de la Información

Para garantizar la seguridad en la transmisión de los datos, es necesario:

a) Establecer un canal de comunicación de datos seguro.
b) Asegurar el intercambio de datos usando un sello electrónico
c) Definir y configurar adecuadamente el servicio de datos
d) Cumplir la normativa relevante sobre protección de datos y usar datos armonizados
e) Autorizar al cliente del servicio de datos mediante un acuerdo/convenio que define los derechos de acceso.

A) Establecer un canal seguro de intercambio de datos.

1. Para crear un canal de intercambio de datos seguro, cada miembro instalará un servidor de seguridad usando un certificado electrónico emitido por la Autoridad Central, que cumplirá con los requisitos publicados en el sitio web de la Autoridad Certificadora de SETEPLAN.
2. Solo las comunicaciones protegidas por este certificado electrónico podrán integrarse en la CID.
3. Cada miembro debe usar un servidor de seguridad, provisto por Tenoli, el cual:
   3.1. Mantiene un registro sellado electrónicamente de todas las consultas o mensajes enviados o recibidos.
   3.2. Asegura el resguardo de este registro de mensajes y evita que pueda ser modificado o falsificado.
4. Cada miembro de la red de intercambio debe usar una conexión cifrada y autenticación mutua para conectar su servidor de seguridad y servicios con el de otros miembros. El servidor de seguridad de Tenoli realiza este trabajo para cada institución.

B) Asegurar el intercambio de datos usando un sello electrónico

1. Tenoli agrega automáticamente un sello o Estampa de Tiempo a todos los mensajes.
2. Tenoli ignora mensajes que no cuenten con este sello electrónico.

C) Definir y registrar servicios

1. Solo los servicios registrados ante la Autoridad Central pueden ser utilizados y proporcionados a través de la CID.
2. Para definir sus servicios, cada miembro debe enviar a la DGE:
   2.1. Los datos contacto del Administrador responsable del servidor de seguridad.
   2.2. Un listado que incluya:

Nombre del Servicio	Descripción	URL de Documentación	Persona Encargada	Correo	Teléfono (móvil y fijo)

3. Para registrar y habilitar un servicio, un miembro de Tenoli debe enviar la solicitud respectiva a la Autoridad Central a través su servidor de seguridad.
4. Para que un servicio pueda ser registrado:
   4.1. Debe estar incluido en el listado enviado a la DGE (ver punto 2).
   4.2. Deben estar disponibles y actualizados los datos de contacto del administrador responsable del servicio y del administrador del servidor de seguridad.
   4.3. Debe aplicar los Estándares de Interoperabilidad definidos por la Red de Gobierno Electrónico (https://egobsv.github.io/EstandaresInteroperabilidad/)
5. Tras el registro de un servicio la institución responsable debe:
   5.1. Designar las instituciones autorizadas para usar el servicio y configurar las reglas de acceso respectivas usando su servidor de seguridad.
   5.2. Garantizar el funcionamiento seguro y sin interrupciones del servicio y el cumplimiento de los acuerdos de acceso que se realicen con otros miembros de la CID.
6. La Autoridad Central podrá rechazar una solicitud de registro de un servicio o de eliminar un servicio del registro si no se cumple alguno de los requisitos establecidos en los numerales 3 y 4.

D) Normativa y armonización de datos

El servicio de datos deberá:

1. Cumplir con el protocolo de mensajes establecido por la Autoridad Central para que pueda ser procesado por el servidor de seguridad.
2. Aplicar los catálogos de referencia y demás estándares de datos definidos en la Política Nacional de Datos Abiertos (http://gobiernoelectronico.gob.sv/datos).
3. Estar registrado en la Autoridad Central, ofrecer información sobre los datos disponibles, y documentar su uso.
4. Estar disponible en el entorno de prueba de Tenoli.

E) Autorización y derechos de acceso a los servicios.

1. El servicio estará disponible en base a los acuerdos que se hagan con otros miembros de la red. Cada acuerdo de uso del servicio determinará:
   1.1. Qué servicios de datos, y las medidas de seguridad necesarias incluyendo medidas organizativas, físicas y técnicas, dependiendo de la naturaleza de los datos.
   1.2. La autorización para compartir el servicio de datos con terceros, si aplica.

1.3. Condiciones y garantías del nivel de servicio.

2. Se requiere que el proveedor de un servicio de datos:
   2.1. Registre ante la Autoridad Central el servicio de datos junto con la descripción técnica del servicio y mantenga esta información actualizada.
   2.2. Antes de firmar un acuerdo con la institución cliente del servicio de datos, asegúrese de que el cliente del servicio de datos aplique las medidas adecuadas de integridad, seguridad y confidencialidad.
   2.3. Asegurarse que los derechos de acceso configurados en el servidor de seguridad sean coherentes con el acuerdo/convenio de uso del servicio.

3. El uso de un servicio de entrega datos es posible a través de un servicio de consulta de datos. El segundo, debe ser configurado en el servidor de seguridad de los miembros autorizados que gestionaron convenios de acceso para el uso ese servicio específico.
4. Se requiere que tanto el usuario como el proveedor de un servicio de datos:
   4.1. Cumpla con el acuerdo/convenio sobre el uso del servicio de datos.
   4.2. Selle electrónicamente los mensajes recibidos en su servidor de seguridad.
5. Es responsabilidad de cada miembro de la red garantizar la autenticación y autorización del usuario final que hace uso del servicio.

Acceso a Terceros

a) Un miembro de Tenoli puede otorgar acceso su servicio a una persona física o jurídica fuera de la organización solo si:
   i) El miembro de la red ha creado y divulgado el procedimiento para ofrecer el servicio de datos a terceros.
   ii) La autorización para compartir el servicio a terceros está incluida en el acuerdo entre el miembro usuario y el que ofrece el servicio dentro la red.

b) El procedimiento para compartir el servicio a terceros incluirá:
   i) La razón para compartir el servicio
   ii) Descripción de los mecanismos para autenticar y autorizar usuarios
   iii) Descripción del registro de consultas, así como los términos y plazos de archivado de estos registros.

c) Al proveer servicios a terceros, el miembro de la red debe:
   i) Cumplir con los procedimientos para compartir servicios que él mismo estableció.
   ii) Notificar a la Autoridad Central y al proveedor del servicio a compartir.
   iii) Asumir los derechos y obligaciones especificadas en los acuerdos y verificar si procede compartir el servicio.
   iv) Divulgar los datos de las partes que comparten el servicio.