MIO

Marco de Interoperabilidad

Integrando los servicios del Estado

G-200044179

CNTI

CENTRO NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias

BICENTENARIO

MIO

Marco de Interoperabilidad

Integrando los servicios del Estado

Marco de Interoperabilidad para el Estado Venezolano V 1.0

Directorio:
Ricardo Menéndez Prieto
Ministro del Poder Popular para Ciencia, Tecnología e Industrias Intermedias.
(Decreto N° 7.198 publicado en Gaceta Oficial N° 39.355)

Manuel Fernández Meléndez
Viceministro de Tecnologías de Información y Comunicación
(Decreto N° 7.190 publicado en Gaceta Oficial N° 5.957 Extraordinaria)

Carlos Eloy Figueira
Presidente del Centro Nacional de Tecnologías de Información
Resolución N° 059 publicado en Gaceta Oficial N° 39.197)

Colaboradores:
- Eduardo Poggi
- Vicepresidencia de la República (VP).
- Ministerio del Poder Popular para la Planificación y Finanzas (MPF).
- Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (Cenditel).
- Comisión de Administración de Divisas (Cadivi).
- Compañía Anónima Nacional Teléfonos de Venezuela (Cantv).
- Instituto Venezolano de los Seguros Sociales (IVSS).
- Oficina Nacional de Contabilidad Pública (Oncop).
- Servicio Administrativo de Identificación, Migración y Extranjería (Saime).
- Servicio Nacional Integrado de Administración Aduanera y Tributaria (Seniat).
- Servicio Nacional de Contrataciones (SNC).
- Superintendencia de Servicios de Certificación Electrónica (Suscerte).
- Dirección General de Acceso y Uso de Tecnologías de Información adscrita al Despacho del Viceministro de Tecnologías de Información y Comunicación.

Corrección:
Adriana Carmona

Diseño y diagramación:
George Child

Imprenta:
Publicsol 50 C.A.,

Deposito Legal: If2902011620910
ISBN: 978-980-7411-00-4

MIO
Marco de Interoperabilidad

MIO

Marco de Interoperabilidad para el Estado venezolano Versión 1.0

Índice

Recurso 3: Matriz Multi-Criterio

Recurso 4: Caracterización de procesos

Recurso 5: Acuerdo Inter-Institucional

Recurso 6: Descripción de servicios

Recurso 7: Descripción de Entidades de Datos

Recurso 8: Descripción general de calidad de datos

Recurso 9: Especificaciones técnicas

Recurso 10: Recomendaciones para la implementación de Servicios Web.

Índice de gráficos

Prólogo

La Interoperabilidad es la capacidad de dos o más organizaciones de intercambiar o proveerse información. En el caso de instituciones del Estado, esta capacidad de colaboración permite agilizar la realización de trámites administrativos, disminuyendo costos y evitando que el mismo dato le sea solicitado a un ciudadano si éste ya lo brindó en alguna oportunidad a una institución. De esta forma, se reconoce a las instituciones del Estado como brazos articulados que sirven efectivamente a los ciudadanos.

Este documento pretende servir de guía en la creación, desarrollo e implantación de la Interoperabilidad en el Estado venezolano. El ejemplar contiene basamentos legales, especificaciones técnicas, estándares, políticas y múltiples recomendaciones para su ejecución y gobernanza en el tiempo. Abarca desde las generalidades que deben conocer los líderes de una institución de la Administración Pública para marcar pautas en el avance de la implementación de la Interoperabilidad, hasta especificidades para los programadores que la ejecutarán en cada organismo.

Este Marco de Interoperabilidad se realizó como respuesta a la imperante necesidad del Estado venezolano en aumentar la eficacia en la realización de trámites de y para los ciudadanos, así como el aprovechamiento de los recursos tecnológicos actuales para tal fin. Fue realizado por un grupo transdiciplinario que garantiza la consideración de múltiples aristas en las áreas técnica, informacional y organizacional, así como sus respectivos lineamientos.

El resultado de la aplicación de la Interoperabilidad genera beneficios directos a los ciudadanos, simplifica trámites anteriormente burocráticos y permite a los organismos dedicar tiempo al cumplimiento de los lineamientos del Estado, afianzando el desarrollo social, político y económico de la nación.

Si bien es cierto que hasta el presente día no existe un modelo ideal para la implementación de la Interoperabilidad, el Ministerio del Poder Popular para Ciencia, Tecnología e Industrias Intermedias (MCTI), a través del Centro Nacional de Tecnologías de Información (CNTI),

tiene el compromiso que el Marco de Interoperabilidad presentado en este documento sea un instrumento adecuado a las necesidades del Estado venezolano, que traerá a nuestra población los frutos de la Interoperabilidad.

Carlos Figueira
Presidente del CNTI
Marzo, 2011.

Resumen

La Interoperabilidad es la capacidad que tiene el Estado para que sus instituciones y demás entes intercambien datos entre sí; a través del uso de tecnologías de información. Alcanzar la Interoperabilidad es posible siempre y cuando se tome en consideración la transdiciplinariedad inherente a ella; contemplando las temáticas de carácter técnico, informacional, organizacional y político-legal-social.

En el Marco del Interoperabilidad convergen los esfuerzos realizados para la elaboración de una guía representativa de situaciones que se pueden presentar al momento de desarrollar la Interoperabilidad en nuestro país. Es un documento lo suficientemente amplio para servir de base funcional para el inicio de la implementación; complementario por sus amplios recursos y no coercitivo al suministrar recomendaciones para que cada ente lo adecue a sus necesidades y posibilidades de financiamiento.

Introducción

El presente documento materializa el cumplimiento de una de las metas establecidas por el Ministerio del Poder Popular para Ciencia, Tecnología e Industrias Intermedias (MCTI) a través del Centro Nacional de Tecnologías de Información (CNTI) para el año 2010 - bajo la coordinación de la Dirección General de Acceso y Uso de Tecnologías de Información adscrita al Despacho del Viceministro de Tecnologías de Información y Comunicación -, alineada al Plan Nacional de Desarrollo Económico y Social 2007-2013, apoyando la transformación del Estado como vía para alcanzar la democracia protagónica y participativa. Desde el punto de vista estratégico institucional, el Marco de Interoperabilidad para el Estado venezolano busca proporcionar sustentabilidad a los componentes de plataformas y servicios de Gobierno Electrónico, bajo el empleo de Tecnologías de Información Libres en las instituciones de la Administración Pública (AP).

El presente Marco de Interoperabilidad, es el resultado de un trabajo colaborativo realizado con las siguientes instituciones del Estado:

- Vicepresidencia de la República (VP).
- Ministerio del Poder Popular para la Planificación y Finanzas (MPF).
- Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (Cenditel).
- Comisión de Administración de Divisas (Cadivi).
- Compañía Anónima Nacional Teléfonos de Venezuela (Cantv).
- Instituto Venezolano de los Seguros Sociales (IVSS).
- Oficina Nacional de Contabilidad Pública (Oncop).
- Servicio Administrativo de Identificación, Migración y Extranjería (Saime).
- Servicio Nacional Integrado de Administración Aduanera y Tributaria (Seniat).

- Servicio Nacional de Contrataciones (SNC).
- Superintendencia de Servicios de Certificación Electrónica (Suscerte).

Esta publicación y sus futuras versiones tendrán como finalidad crear y mantener las condiciones necesarias para garantizar un adecuado nivel de Interoperabilidad técnica, informacional y organizacional de los sistemas informáticos de la AP.

Objetivo

Servir como un documento de referencia que comprende un conjunto de políticas, lineamientos y estándares base para gestionar el intercambio electrónico de datos, mediante la publicación de servicios, entre los órganos y entes de la Administración Pública.

Alcance

El Marco de Interoperabilidad (MIO) es un instrumento destinado a todos los órganos, entes y dependencias del gobierno central, los gobiernos locales, el sector público en sentido amplio incluyendo empresas estatales y mixtas, organismos públicos no gubernamentales y todos los poderes del Estado.

El cumplimiento de los lineamientos establecidos no puede imponerse a ciudadanos y empresas de cualquier origen ni a gobiernos extranjeros, pero el Estado venezolano establece que el presente marco define su método preferencial de intercambio electrónico de datos.

Recomendación 1:
Todos los organismos de la Administración Pública (AP) deberán apropiarse del MIO y participar en su mantenimiento y mejora.

Este marco no especifica, ni limita el uso de las tecnologías de información. Tampoco incluye la estandarización en la manera de presentar los servicios de Gobierno Electrónico, por el contrario, se centra en la definición de lineamientos y condiciones relevantes para garantizar la interconexión entre sistemas de información, el intercambio electrónico de datos entre organismos y la elaboración de Procesos Inter-Institucionales.

El MIO está dividido y estructurado en cinco capítulos, donde se encontrarán recomendaciones específicas aplicadas a cada área:

- Capítulo 1: Basamento legal.
- Capítulo 2: Sobre la Interoperabilidad.
- Capítulo 3: Políticas para la implementación de la Interoperabilidad.
- Capítulo 4: Estándares.
- Capítulo 5: Recomendaciones generales para la implementación de la Interoperabilidad en Procesos Inter-Institucionales.

El marco esta compuesto por un conjunto de recursos que permiten impulsar y afianzar la Interoperabilidad en la AP, estos se encuentran citados a lo largo del documento, a fin de destacar su uso en cada una de las recomendaciones realizadas.

Capítulo 1

Basamento legal

Basamento legal

Se describe a continuación toda la documentación relacionada en el ámbito legal que ampara y promueve la implementación de la Interoperabilidad y el desarrollo de este marco para el Estado venezolano.

Constitución de la República Bolivariana de Venezuela CRBV). Gaceta Oficial Nº 36.860 de fecha 30 de diciembre de 1999. Artículo 110. Establece que: "El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país".

Ley de Reforma de la Ley Orgánica de Ciencia, Tecnología e Innovación. Gaceta Oficial Nº 39.575 de fecha 16 de diciembre de 2010. Artículo 10. Expresa: "La autoridad nacional con competencia en materia de ciencia, tecnología, innovación y sus aplicaciones actuará como coordinador e integrador de los sujetos de esta Ley, en las acciones de su competencia, en articulación con los órganos y entes de la Administración Pública". Artículo 18. Expresa: "La autoridad nacional con competencia en materia de ciencia, tecnología, innovación y sus aplicaciones, ejercerá la dirección en el área de tecnologías de información".

Ley de Simplificación de Trámites. Gaceta Oficial Nº 5.393 de fecha 22 de octubre de 1999 y Decreto Nº 6.265 del 22 de julio de 2008. Artículo 11. Expresa: "Los órganos y entes de la Administración Pública Nacional, en virtud del principio de cooperación que debe imperar en sus relaciones interorgánicas y con las demás ramas del Poder Público, deberán implementar bases de datos automatizadas de fácil acceso y no podrán exigir la presentación de copias certificadas o fotocopias de documentos que la Administración Pública Nacional tenga en su poder, o de los que tenga la posibilidad legal de acceder".

Ley Orgánica de la Administración Pública. Gaceta Oficial Nº 37.305 de fecha 17 de octubre de 2001, establece los principios y bases que rigen la organización y el funcionamiento de la Administración Pública; los principios y lineamientos de la organización y funcionamiento de la Administración Pública Nacional. También regula los compromisos de gestión, los mecanismos para promover la participación y el control sobre las políticas y resultados públicos; y establece las normas básicas sobre los archivos y registros públicos.

Ley Especial contra los Delitos Informáticos. Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2010. Tiene como objeto: "la protección integral de

los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley".

Decreto con fuerza de ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas. Gaceta Oficial Nº 37.148 de fecha 28 de febrero de 2001. Artículo 1º. Establece: "otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos".

Decreto Nº 2.479 del 27 de junio de 2003. Decreta la creación de la Comisión Presidencial para la conformación de la red del Estado, con la finalidad de facilitar la comunicación e interacción de los órganos y entes de la Administración Pública.

Decreto Nº 3.390. Gaceta Oficial Nº 38.095 de fecha 28 de diciembre de 2004. Artículo 1º. Establece:"La Administración Pública Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos, en sus sistemas, proyectos y servicios informáticos. A tales fines, todos los órganos y entes de la Administración Pública Nacional iniciarán los procesos de migración gradual y progresiva de éstos hacia el Software Libre desarrollado con Estándares Abiertos".

Capítulo 2

Sobre la Interoperabilidad

Sobre la Interoperabilidad

En este capítulo se presenta la definición de la Interoperabilidad (IO) para el Estado venezolano y se describen sus dimensiones y componentes.

Definición de Interoperabilidad

La IO es la capacidad de organizaciones dispares y diversas de interactuar con objetivos consensuados. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de Procesos Inter-Institucionales (PII), mediante el intercambio electrónico de datos entre sus respectivos sistemas de tecnología de información.

La IO busca proveer sistemáticamente servicios a la sociedad cumpliendo los principios de Simplificación Registral y Ventanilla Única, entendiendo que:

- El ***Principio de Simplificación de Registral*** exige que los organismos de la Administración Pública (AP) no pueden volver a solicitar un dato o documento a ciudadanos o empresas que ya se encuentre en poder de algún organismo del Estado.
- El ***Principio de Ventanilla Única*** exige que la AP debe presentarse ante la sociedad como una única entidad, independientemente de su estructura interna y sus divisiones políticas, territoriales o estatutarias.

Alineados a la citada Ley de Simplificación de Trámites Administrativos, el cumplimiento de estos principios exige a todos los organismos de la AP facilitar el acceso a los datos públicos que administran, reformular y simplificar los trámites donde participan otras instituciones. Así se evita que los ciudadanos presenten en reiteradas ocasiones los mismos datos y documentos, o se trasladen de una ventanilla a otra para completar sus solicitudes. Los datos deben transferirse digitalmente entre los organismos del Estado.

Esta definición de IO se focaliza en la implementación de PII basados en el intercambio electrónico de datos. La IO es, en este sentido, una capacidad del Estado y un medio para alcanzar los siguientes fines:

1. Bajar los costos y la carga administrativa que el Estado demanda

a los ciudadanos y empresas.

2. Mejorar la atención de los ciudadanos, facilitando el acceso a información actualizada, oportuna y confiable.

3. Fomentar la transparencia, la eficiencia y la simplicidad de los procedimientos administrativos.

4. Propiciar la cooperación y la interrelación entre los organismos de la AP.[1]

5. Impulsar la optimización de los procesos de la AP que proveen servicios a la sociedad, a manera de no solicitar información que ya el Estado posee.

6. Mejorar la calidad de los datos públicos.

7. Disminuir los costos de operación de la AP.

8. Cumplir con lo establecido en la Ley Orgánica de la Administración Pública, informado a la población de las actividades, servicios, procedimientos y organización de la AP.

Recomendación 2:
A las instituciones de la AP se les sugiere impulsar la reutilización de datos como un carácter complementario a la implementación de PII y no como un aspecto central de la IO.

Recomendación 3:
Se aconseja a todas las instituciones de la AP y a todas las organizaciones privadas que interactúen con éstos que, utilizando el Marco de Interoperabilidad (MIO), impulsen el intercambio electrónico de datos para brindar mejores servicios a la sociedad.

Recomendación 4:
Se recomienda a todos los organismos de la AP que revisen sus procesos e impulsen, cuando sea conveniente, su rediseño a fin de poder intercambiar datos electrónicamente con otros organismos, dando así cumplimiento a la Ley de Simplificación de Trámites Administrativos.

Dimensiones de la Interoperabilidad

La implementación de la IO es un problema complejo que atraviesa todos los planos del quehacer de una organización: cultural, legal, organizacional, informacional y técnico. La diversidad temática y las interrelaciones requieren de un nivel importante de gobernanza, que permita articular con éxito los factores dentro de cada contexto. Para tratar esta diversidad se ha establecido un marco conceptual que reconoce la existencia de las siguientes cuatro dimensiones transversales entre sí:

- Dimensión temática.
- Dimensión de implantación.
- Dimensión de servicio.
- Dimensión de madurez.

Dimensión temática

Agrupa las áreas del conocimiento necesarias para elaborar y apropiar la efectiva implementación de la IO. Se divide en:

Interoperabilidad técnica
Establece las pautas, normas y estándares técnicos necesarios para la interconexión de sistemas -hardware y software- y servicios, garantizando accesibilidad y seguridad de la información.

[1] En función de esa cooperación, los Servicios de Información no deben disminuirse, degradarse, ni causar perjuicio a los órganos y entes de la AP; evitando imponer gastos en plataforma tecnológica.

Interoperabilidad informacional

Establece las pautas para asegurar el significado preciso de los datos intercambiados y su entendimiento por todos los sistemas que participan en el intercambio electrónico de datos. Se divide en:

Interoperabilidad sintáctica, se refiere a los aspectos de comunicación, transporte, almacenamiento y representación de datos.

Interoperabilidad semántica, se refiere a los aspectos necesarios para que los sistemas informáticos combinen y procesen correctamente datos provenientes de otras fuentes y puedan entender las capacidades e intenciones de aquellos con los que se comunican.

Interoperabilidad organizacional

Se encarga de asegurar que los mensajes intercambiados e interpretados por todos los actores involucrados sean usados adecuadamente en los PII que brindan servicios a la sociedad. A su vez establece las pautas para implementar los acuerdos de cooperación necesarios para el intercambio de información entre dos o más instituciones de la AP, a fin de superar los retos organizacionales que buscan mejorar los servicios prestados a la sociedad.

Este plano de la IO tiene como objetivo lograr que las organizaciones puedan aprovechar la información provista por otros para desarrollar sus procesos, transformándola en beneficio para los ciudadanos. El trabajo coordinado se logra al definir metas y al modelar procesos entre organizaciones dispuestas a intercambiar información, a pesar que sus estructuras y sistemas informáticos sean diferentes.

Interoperabilidad político-legal-social

Busca establecer las condiciones que definan el ámbito político, legal y social con el cual se desarrollará la IO. Asegura que los PII sean realmente apropiados, aprovechados y alineados a las políticas públicas.

Dimensión de implantación

Agrupa las diferentes acciones que se realizan en pro de la implementación de la IO. Contempla las actividades y recursos para el desarrollo de:

Marco de Interoperabilidad

Es un conjunto de documentos de referencia que comprende lineamientos, políticas, estándares y herramientas para gestionar el intercambio electrónico de datos mediante la publicación de Servicios de Información entre los organismos de la AP, que aseguren un adecuado nivel de IO organizacional, informacional, técnica y político– legal-social.

Contexto

Son todos los aspectos que deben ser reconocidos y tomados en consideración dada su injerencia en la IO, tales como: leyes, normativas, marcos de referencia, infraestructura informática, capacidades institucionales, recursos informáticos, etc. Los proyectos o iniciativas que se desarrollen en el ámbito de la IO deben respetar los lineamientos establecidos o en su defecto deben ser adecuados, si no lo son, entonces se debe reconocer las restricciones que presentan.

Proyectos

Son todas las acciones realizadas o previstas que incluyen aspectos de la IO, pueden ser ejecutadas por

comunidades o instituciones sin importar si estas difieran en parte de lo determinado en este marco, o en las acciones diseñadas directamente para avanzar con la implementación sistemática de la IO.

Recomendación 5:
Se invita a todos las instituciones de la AP a elaborar sus planes de Gobierno Electrónico y simplificación de trámites administrativos.

Recurso 1:
Se recomienda a las instituciones del Estado alinear sus planes de IO a las sugerencias establecidas en el anexo: "Plan para la implementación de la Interoperabilidad en Venezuela".

Gobernanza
Agrupa la coordinación, la planificación y el control de todas las acciones realizadas en pro de la implementación de la IO, procurando un desarrollo social e institucional duradero. Tiene como objetivo alcanzar la coherencia y facilitar el conjunto de acciones realizadas en la materia, así como impulsar el cumplimiento de los objetivos de mediano y largo plazo establecidos.

Dimensión de servicio

Agrupa aquellos documentos y actividades necesarios para que la IO se logre con la calidad y seguridad apropiada. Se divide en: seguridad, calidad y nivel de servicio. Esta dimensión exige a las instituciones involucradas generar una serie de capacidades de servicio que van desde lo técnico hasta lo organizacional.

Seguridad
La seguridad informática consiste en asegurar que los recursos de un sistema de información -recursos físicos, lógicos y datos- sean utilizados de la manera como se decidió, que el acceso y la modificación de los datos administrados sólo le sea permitido a las personas autorizadas para ello. En esta concepción de seguridad se incluyen las cuatro características fundamentales: disponibilidad, integridad, confidencialidad y no repudio.

Calidad
La calidad de datos implica que los datos gestionados -capturados, procesados, almacenados y publicados- son válidos y son un fiel reflejo de la realidad que se desea tratar. Esto supone que los datos no contengan errores significativos, sean lo más veraces posibles y estén actualizados en función de los requisitos establecidos por el conjunto de actores involucrados en su gestión. Desde esta perspectiva, la calidad de datos implica la capacidad de satisfacer los deseos y necesidades de los solicitantes de información.

Nivel de servicio
Permite establecer de forma clara las características operativas de un servicio que, plasmadas en un acuerdo, establecen los requerimientos de un solicitante de información y el compromiso de un proveedor. Un acuerdo de nivel de servicio es un instrumento que permite otorgar confianza y establecer garantías para que el solicitante pueda basar sus procesos en el servicio.

Dimensión de madurez

Transversalmente a las dimensiones presentadas, se define una cuarta dimensión que corresponde con los diferentes niveles de madurez que se pueden alcanzar en cada uno de los aspectos de la IO.

Un modelo de madurez para la IO, es un instrumento conceptual que permite

diferenciar niveles de complejidad y refinación, que puede ser asumido por un conjunto de instituciones para conocer su situación actual y poder verificar cuáles son los desafíos inmediatos y mediatos que debe afrontar. De esta forma, la comparación entre la situación real y la deseada, establece un marco concreto para la planificación de actividades de corto y mediano plazo.

A continuación se describen los niveles consecutivos de la IO:

Nivel 1 – inicial

Las instituciones se caracterizan por no disponer de un ambiente estable para la IO. El éxito de los proyectos de desarrollo de PII se basa en el esfuerzo personal de los actores involucrados. A menudo se producen fracasos, y casi siempre retrasos y costos extras, por lo que el resultado de los proyectos es impredecible. No hay memoria aprovechable entre experiencias.

Las instituciones realizan intercambios electrónicos de información y reconocen que existen aspectos de la IO que son precisos abordar. Sin embargo, no hay procesos estandarizados, sino más bien enfoques que se aplican caso por caso. El enfoque general de la gestión es desorganizado o inexistente. Los intercambios son bilaterales entre sistemas, normalmente sin formalización e independientes uno de otro.

Nivel 2 – administrado

En este nivel las instituciones disponen de prácticas de gestión de proyectos para el desarrollo de PII. Existen métricas básicas y un razonable seguimiento de la calidad de los mismos. La relación con los demás miembros es gestionada sistemáticamente.

Existen intercambios bilaterales realizados de manera más o menos homogénea. Se cumple con características básicas de seguridad y confiabilidad a nivel de cada una de las partes. Se sustentan los intercambios mediante acuerdos bilaterales y niveles de servicio rudimentarios. Los procesos están en una etapa de desarrollo en que diferentes personas siguen procedimientos similares para encarar la misma tarea. No hay capacitación o comunicación formal de los procedimientos utilizados y la responsabilidad queda librada a cada persona. Hay un alto grado de dependencia del conocimiento de determinadas personas, por lo cual es probable que apliquen formas de solución diferentes.

Nivel 3 – definido

Además de una buena gestión de proyectos, los organismos disponen de procedimientos correctos de coordinación entre ellos, formación del personal, técnicas de ingeniería más detalladas y un nivel avanzado de métricas para procesos.

Los procedimientos son estandarizados, documentados y difundidos a través de actividades de capacitación. Sin embargo, la adhesión a los procesos queda librada a cada persona y, si existen desviaciones, es poco probable que sean detectadas. Los procedimientos no son sofisticados pero son la formalización de las prácticas existentes. La utilización de intercambios de información es práctica habitual y existen procedimientos apropiados para su uso. Los intercambios son confiables y seguros. Los servicios disponibles pueden ser ubicados digitalmente. Los intercambios están protegidos legalmente.

Nivel 4 – medido

Los organismos disponen de un conjunto de métricas significativas de cumplimiento, calidad y productividad que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos.

Es posible monitorear y medir el cumplimiento de los procedimientos y tomar acción en aquellos puntos donde los procesos parecen no estar funcionando con eficacia. Los procesos están sometidos a una mejora continua y brindan buenas prácticas. La automatización y las herramientas se utilizan en forma parcial. Los PII se basan en sistemas interoperables. No hay redundancia de información o por lo menos está controlada. Existe un marco general que ampara y garantiza los intercambios, así como reglas generales de seguridad aplicadas automáticamente a los intercambios. Los servicios pueden ser ubicados e interpretados automáticamente.

Nivel 5 – optimizado

Las instituciones están volcadas a la mejora continua de los PII. Se hace uso intensivo de métricas y se gestiona el proceso de control e innovación.

Los procesos se refinan hasta el nivel de las mejores prácticas, sobre la base de los resultados de la mejora continua y los modelos de madurez entre todos los organismos. La tecnología de información se utiliza de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la eficacia, dotando a los organismos de agilidad para la adaptación. Los procesos y los intercambios son implementados eficientemente, monitoreados y mejorados continuamente. No hay redundancia operativa de información ni intercambios por fuera de lo establecido.

Recomendación 6:

Las instituciones deben avanzar en las diferentes dimensiones de la IO de forma incremental, manteniendo un nivel de madurez homogéneo en todos sus aspectos.

Interrelación de las dimensiones de IO

Las dimensiones permiten dividir la gran temática de la IO en unidades más pequeñas y tratables. Al mismo tiempo, refuerza la idea que las distintas dimensiones no están aisladas; sino que están altamente interrelacionadas.

A continuación se muestra un gráfico donde se puede apreciar que el marco de IO -inmerso en la dimensión de implantación- debe contener estándares técnicos, informacionales, organizacionales, políticos, legales y sociales. El contexto y los proyectos relacionados pueden influir tanto en la manera como se está llevando la IO a la práctica como en las diferentes áreas temáticas.

Gráfico 1. Interrelación entre las dimensiones temática e implantación
Fuente. Poggi,Eduardo (2010)

Se podría agregar la tercera dimensión de servicio. El nivel de servicio, la calidad y la seguridad son transversales ya que deben incluirse en todos los aspectos de la concepción y de implementación.

Por ejemplo, la seguridad claramente comprende los aspectos técnicos, informacionales, organizacionales y políticos.

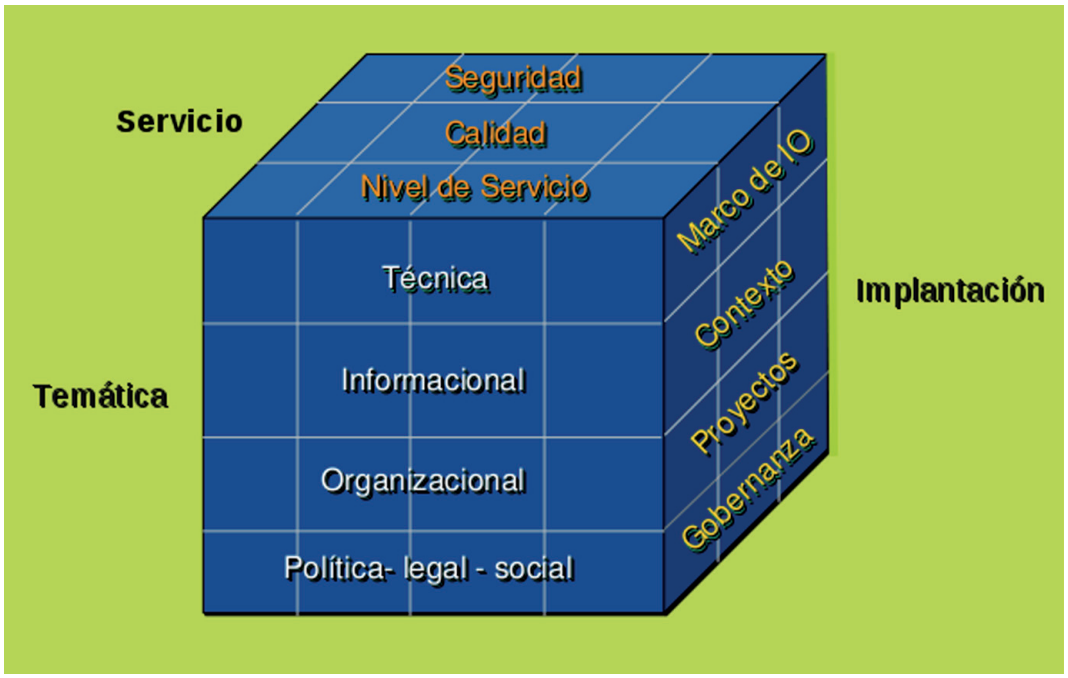


Gráfico 2. Interrelación entre las dimensiones temática, implantación y servicio
Fuente. Poggi,Eduardo (2010)

Continuando con el razonamiento, se puede incluir la cuarta dimensión de madurez, que podríamos representar con una línea de tiempo sobre la que se va moviendo el cubo anterior, que permite visualizar como todos los aspectos de las otras tres dimensiones deben ir madurando en conjunto y paulatinamente.

Principios rectores de la Interoperabilidad

El Gobierno Electrónico establece ciertos principios rectores, como los encontrados en la Carta Iberoamericana de Gobierno Electrónico[2]: igualdad, legalidad, conservación, transparencia, accesibilidad, proporcionalidad, responsabilidad, adecuación y neutralidad tecnológica. Todos ellos son aplicados a la IO, pero existen algunos principios específicos que se relacionan aún más, éstos no deben entenderse en forma aislada, deben mirarse como un conjunto fuertemente interrelacionado.

Foco en la sociedad

Los servicios deben ser ofrecidos a la sociedad en respuesta a sus necesidades y para asegurar sus derechos. Estas necesidades son las que determinan cómo los servicios deben ser definidos y provistos.

La sociedad espera que sus derechos y beneficios no requieran de trámites previos; que el acceso a los servicios sea adecuado a sus capacidades; que la información sea requerida sólo las veces necesarias; que la distribución de la información que les concierne esté garantizada por los límites de la privacidad; que sea la información la que circule entre las administraciones y no los ciudadanos los que deban hacerlo; y que estos estén disponibles a través de servicios confiables con la mayor amplitud posible.

Subsidiaridad

Este principio articula los medios para disminuir los efectos contraproducentes de la asimetría de recursos entre organismos de diferentes capacidades institucionales, especialmente cuando estas diferencias producen disparidades en los ciudadanos a los que deben servir, asegurando así, que las decisiones de la distribución de responsabilidad entre las instituciones involucradas se realice de la forma conveniente.

La IO debe reconocer de acuerdo al principio de subsidiaridad, la autonomía y el conocimiento local de las instituciones y de los actores del sector privado involucrados. Las instancias coordinadoras del Componente de Gobernanza no deben interferir en el funcionamiento interno de las instituciones, dejando a cargo de éstas tomar las medidas necesarias para asegurar la IO. Sin embargo, el Ente Coordinador debe asumir una función subsidiaria y ayudar a las instituciones cuando éstos no cuenten con la capacidad para cumplir con los requerimientos establecidos, especialmente en asegurar los derechos de los ciudadanos.

Asincronía y asimetría

Complementariamente a la subsidiaridad, las diferentes capacidades institucionales y los diferentes ritmos de las políticas públicas deben ser respetados y considerados a la hora de ejecutar las acciones necesarias para implementar la IO. Por lo tanto, los tiempos, las necesidades y las oportunidades de las diferentes actividades deben ser consideradas en todo momento.

[2] http://www.clad.org/documentos/declaraciones/cartagobelec.pdf

Vulgaridad

La elaboración de los estándares y de los recursos deben responder a las capacidades de apropiación del conjunto de actores involucrados y ser susceptibles de ser apropiados por todos para evitar la exclusión de algunos. Todo recurso elaborado en el ámbito de aplicación de este MIO debe poder ser apropiado por cualquier organismo de la AP.

Si por alguna circunstancia no fuera posible encontrar un conjunto de instrumentos apropiables por todos los involucrados, se deberán tomar las medidas necesarias para generar las capacidades en los potencialmente excluidos para lograrlo. Complementariamente, para respetar las capacidades de los organismos más débiles y las necesidades de los más avanzados, será preciso establecer variantes de especificaciones que satisfagan las necesidades de todas las partes sin dejar excluidos.

Preservación

La disponibilidad en el tiempo de los datos administrados por el Estado es un requisito básico que no debe ser olvidado. Se deberá considerar la vida útil potencial, desde el punto de vista de cada dato en sí, y no del uso institucional del Organismo Proveedor. Tradicionalmente cada organismo decidía en función de sus necesidades y posibilidades el tiempo de resguardo de la información bajo su potestad. La caducidad de los datos no debe ser anticipada a priori, ya que usos impensados pueden surgir inesperadamente.

Además de la vida útil de los datos, se debe anticipar la obsolescencia de la infraestructura y la tecnología con vistas a garantizar la recuperación futura de la información.

Capítulo 3

Políticas para la implementación de la Interoperabilidad

Políticas para la implementación de la Interoperabilidad

De cara a la implementación de la Interoperabilidad (IO) se debe resguardar: la seguridad y privacidad de los datos de las personas, la gradualidad de acuerdo al desarrollo, la transparencia al hacer del conocimiento público el procedimiento a implementar, el soporte técnico para asegurar su permanencia, la escalabilidad, la simplificación administrativa y la adopción de estándares abiertos.

Se definen a continuación una serie de políticas que establecen líneas de pensamiento para llevar adelante las prácticas asociadas a la implementación de la IO.

Seguridad

En todas las actividades realizadas para la implementación de la IO se deben tener en cuenta las medidas de seguridad adecuadas para proteger la privacidad de las personas y las instituciones cumpliendo con todas las leyes específicas de protección de información vigentes.

Todo intercambio electrónico de datos debe cumplir con las normativas básicas establecidas en materia de protección de datos y de los requisitos mínimos de seguridad de los sistemas de información: disponibilidad, confidencialidad, integridad y no repudio.

Gradualidad

Los avances en la implementación de la IO se irán realizando por refinamientos sucesivos, siguiendo el modelo de madurez y en función de los resultados obtenido en las etapas anteriores. Se procurará mantener un nivel de madurez parejo en todas las dimensiones de la IO.

Adopción de estándares abiertos

Siempre que sea posible, serán adoptados estándares abiertos para todas las especificaciones necesarias. Estándares propietarios podrán ser aceptados temporalmente, manteniéndose las perspectivas de reemplazo cuando haya condiciones de migración disponibles. Sin perjudicar esas metas, serán respetadas las situaciones en que

haya necesidad de consider requisitos de seguridad e integridad de información.

Transparencia

En el proceso de construcción, gestión, divulgación y actualización de la IO, se deberá contar con la participación activa de los ciudadanos. Los organismos de la Administración Pública (AP) deberán incentivar la opinión, comentarios, aportes y contribuciones de los ciudadanos que puedan mejorar la prestación de los Servicios de Información. Los documentos relacionados a la IO estarán a disposición de la sociedad, por medio de Internet, previendo mecanismos de divulgación, recepción y evaluación de sugerencias. En este sentido, serán definidos y divulgados para amplio conocimiento los plazos y compromisos para la aceptación o rechazo de las sugerencias realizadas.

Soporte

Todas las especificaciones utilizadas para la implementación de la IO deben contemplar soluciones apoyadas en comunidades que proporcionen sustento a los estándares y recursos establecidos. La meta a ser alcanzada es la reducción de los costos y de los riesgos en la concepción y producción de servicios y sistemas de información.

Escalabilidad

Las especificaciones utilizadas para la implementación de la IO deben tener la capacidad de atender alteraciones de demanda en el sistema, como cambios en volúmenes de datos, cantidad de transacciones o cantidad de usuarios. Los estándares establecidos no podrán ser un factor restrictivo, debiendo ser capaces de cimentar el desarrollo de servicios que atiendan necesidades más específicas, involucrando pequeños volúmenes de transacciones y de usuarios, hasta demandas de cobertura nacional, con tratamiento de gran cantidad de información y de usuarios.

Las soluciones multilaterales escalables deben tener prioridad sobre la generalización de la multiplicidad de soluciones bilaterales. Sin embargo, es necesario evaluar que en un inicio, una solución multilateral puede ser muy costosa y no sustentable, por lo que se deberá evaluar si es conveniente realizar implementaciones bilaterales más sencillas, sin perder el horizonte de avanzar a soluciones más complejas.

Simplificación administrativa

La implementación de la IO contribuye a que las interacciones entre los organismos de la AP —y, entre éstos y la sociedad—, sean realizadas de forma simple y directa, sin daños a la legislación vigente. Los procesos y la gestión de datos deben pensarse desde la visión de la AP y no desde la visión institucional, impulsando la coordinación de objetivos inter-institucionales en pro del beneficio de la sociedad.

Recomendación 7:

Todas las instituciones de la AP y todas las organizaciones privadas que interactúen con éstas, deberán apropiarse de los principios y políticas de la IO para guiar e impulsar la prestación de servicios a la sociedad.

Capítulo 4

Estándares

Estándares

Los estándares son lineamientos a establecer para regularizar el proceso de implementación de la Interoperabilidad (IO), pueden ser de carácter organizacional, técnico e informacional.

Las recomendaciones para el uso de especificaciones dentro de esta versión inicial del Marco de Interoperabilidad (MIO), incluyen un conjunto de recursos básicos para que las instituciones puedan realizar actividades relacionadas a la publicación y consumo de servicios, la gestión de datos asociados y la descripción de Procesos Inter-Institucionales (PII). A partir de la experiencia derivada de la aplicación de los recursos, se irán corrigiendo y haciendo cada vez más sofisticados y complejos en cumplimiento de la política de gradualidad.

Estándares para la Interoperabilidad organizacional

Los estándares para la IO organizacional del presente MIO se establecen para las siguientes actividades:

- Gestión de Procesos Inter-Institucionales.
- Elaborar acuerdos inter-institucionales.
- Definir roles institucionales.

Gestión de Procesos Inter-Institucionales

Identificar y describir los procesos que lleva adelante la Administración Pública (AP) es el primer paso para mejorarlos por simple reingeniería o por aprovechamiento de los beneficios de la IO, aumentando así su valor hacia la sociedad.

Recurso 2:
En el anexo: “Modelo Organizativo para la implementación de la Interoperabilidad en Venezuela”, se establecen algunas pautas para la construcción del sistema de información que contendrá el inventario y la descripción de procesos de toda la AP.

Inventario de procesos
Se recomienda inventariar, catalogar y describir de manera uniforme los procesos vigentes con el fin de analizar su problemática e impacto y proponer su reingeniería utilizando los beneficios de la IO. El primer paso consiste en identificar e inventariar los procesos de manera que posteriormente puedan ser descritos y evaluados a detalle.

Recomendación 8:

Las instituciones deberán construir el inventario de los procesos a su cargo con una simple descripción que permita conocer su temática y alcance.

Descripción de procesos

La descripción detallada de los procesos permite evaluar las posibilidades de mejora y guiar los esfuerzos de reingeniería de una forma efectiva y viable. Dado que el esfuerzo necesario para describir todos los procesos en detalle puede ser muy grande, se recomienda hacerlo de forma selectiva aprovechando el conocimiento que tienen las instituciones sobre su funcionamiento y sobre como la IO puede enriquecer los procesos ya establecidos. Es necesario aplicar este método sucesivamente y de forma exponencial en el resto de los procesos identificados.

Recomendación 9:

Las instituciones de la AP seleccionarán y describirán en detalle los procesos que sean potencialmente candidatos a mejoras sustantivas a través de la aplicación de la IO.

Evaluación de procesos

Luego de describir en detalle los procesos, estos se deben evaluar y priorizar. Para ello, se deben definir los criterios que van a contribuir con la selección del proceso; una referencia de los criterios a considerar puede ser: su nivel de importancia con respecto a la demanda, costo de operación para la AP y para la sociedad, tiempo y nivel de satisfacción de los usuarios, etc. Los criterios para la jerarquización quedan a potestad de cada institución.
En la selección también deben considerarse criterios que determinen la factibilidad de aplicar la IO, por ejemplo el nivel de optimización, el nivel de automatización y madurez de la plataforma tecnológica. Este último paso, requiere de un levantamiento de información que aporte al análisis de brechas entre lo que actualmente se dispone tecnológicamente y lo que se necesita para implementar la IO.

Recomendación 10:

Las instituciones definirán los criterios de priorización y los aplicarán a sus procesos.

Estas actividades se insertan en lo establecido en el Artículo 6 de la Ley de Simplificación de Trámites Administrativos, que incluye recomendaciones de simplificación y mejoras de trámites administrativos. Una alternativa para la selección del proceso, es la aplicación de la matriz multi-criterio, herramienta para la resolución de problemas, utilizada para facilitar la toma de decisiones con base en factores cualitativos o factores no homogéneos que intervienen en un suceso.

Recurso 3:

Utilizar el método descrito en el anexo: “Matriz Multi-Criterio” como herramienta para la selección y priorización de procesos.

Caracterización de los procesos asociados a la Interoperabilidad

Con el levantamiento de información del proceso seleccionado y de su representación gráfica en diagramas de flujo, se debe rediseñar los procedimientos para representar y documentar los intercambios de información identificados.

Para ello se deben realizar las siguientes actividades:

- Identificación del proceso.
- Caracterización del proceso.
- Representación gráfica del proceso mediante la cadena de valor.

- Establecer la matriz de roles, funciones y actividades, en concordancia con el diseño y adecuación de los procesos y de la plataforma.

Recurso 4:
Utilizar el método descrito en el anexo: "Caracterización de Procesos" para representar el modelo de procesos.

Gestión de Servicios de Información
Se recomienda definir los procesos que van a permitir el mantenimiento de los servicios entre las instituciones involucradas. Los procesos se derivan del compromiso entre las partes, establecidos en el acuerdo inter-institucional. Se puede seguir la misma metodología que se seleccione para representar los procedimientos. Es importante que, de ser éste el caso, se definan los mecanismos de control y seguimiento para atender cualquier eventualidad que se presente.

Recomendación 11:
Las instituciones deberán asignar los recursos necesarios para gestionar sus procesos y, a través de la IO, agregarles valor para la sociedad.

Elaborar acuerdos inter-instituciones

Para brindar confianza y sustento legal a la construcción de PII mediante la utilización de Servicios de Información provistos por otros organismos, es necesario formalizar la publicación y consumo. Para ello, los organismos deben establecer las condiciones de los Servicios de Información que intercambien y formalizarlas en un acuerdo. Un acuerdo puede cubrir más de un servicio y su actualización puede realizarse por adendas al acuerdo original.

Los acuerdos deben componerse de dos cuerpos:

- Uno genérico, con las cláusulas válidas para todo servicio.
- Uno más específico, por cada servicio o conjunto de servicios con cláusulas propias.

El cuerpo principal o genérico del acuerdo debe contener como mínimo:

- Responsabilidades de las partes en la operación, administración y mantenimiento de los Servicios de Información.
- Responsabilidades de la partes sobre la calidad y actualización de los datos incluidos en los Servicios de Información.
- Responsabilidades de las partes sobre la seguridad de los datos.
- Disponibilidad de los Servicios de Información.
- Disponibilidad de recursos para asegurar las prestaciones de los Servicios de Información.
- Compromiso de cumplimiento del MIO y normativas relacionadas.
- Obligaciones específicas del Organismo Proveedor de información.
- Obligaciones específicas del Organismo Solicitante de información.
- Duración del acuerdo.

Los cuerpos específicos de los acuerdos deben contener por cada conjunto de servicios las especificaciones que se enumeran a continuación según los estándares de cada caso:

- Descripción funcional del servicio y de los métodos que contenga.
- Términos del acuerdo de nivel de servicio, con especificación de indicadores y método de monitoreo.

- Especificaciones de los niveles de seguridad, calidad y actualización de los datos involucrados.

Los acuerdos serán implementados en cualquier formato válido para el Estado venezolano, pudiendo implementarse total o parcialmente por medios electrónicos con las condiciones legales que ambas partes acuerden.

Recomendación 12:
Las instituciones soportarán legalmente los intercambios electrónicos de datos, así como los acuerdos de nivel de servicio que se establezcan.

Recurso 5:
En el anexo: "Acuerdo Inter-Institucional" se puede encontrar una recomendación del contenido de un acuerdo para el intercambio electrónico de datos a través de Servicios de Información.

Definir roles institucionales

El ejercicio de la IO requiere la participación de múltiples actores institucionales y la apropiación de prácticas transversales que son nuevas para muchas organizaciones. Se considera necesario que los organismos establezcan roles institucionales con competencias en la materia y asignen personal con las respectivas previsiones presupuestarias.

Las instituciones deberán asignar el personal necesario de acuerdo a sus posibilidades y mantenerlos actualizados en la medida que aumente su nivel de madurez.

Recomendación 13:
Las instituciones definirán roles para la atención de las actividades relacionadas a la IO y asignarán personal capacitado para cumplirlos. Ver anexo: "Modelo Organizativo para la implementación de la Interoperabilidad en Venezuela", sección roles institucionales, donde se encuentran algunas recomendaciones de los roles institucionales a definir.

Estándares para la Interoperabilidad informacional

Los estándares para la IO informacional establecen recomendaciones para las siguientes actividades:

- Descripción de servicios.
- Descripción de Entidades de Datos.
- Descripción de calidad y actualización de datos.

Descripción de servicios

Los Servicios de Información son la forma de intercambiar electrónicamente datos entre diferentes instituciones. Su descripción incluye características propias del servicio en sí, como sus funcionalidades y la descripción de los datos que intercambia.

La información que debe contener una descripción de servicio debe ser suficiente para que un desarrollador pueda invocar y utilizar las funcionalidades de éste, como una extensión de un sistema, así como incluir los detalles de implementación que conciernen al organismo que lo publica.

Recomendación 14:
Las instituciones describirán detalladamente la información -externa- de los Servicios de Información que publican para que otras instituciones los conozcan.

Recurso 6:
En el anexo: "Descripción de servicio" se encontrará una plantilla modelo para la especificación de los Servicios de Información.

Descripción de Entidades de Datos

Manejar eficientemente grandes cantidades de datos entre diferentes organismos de la AP requiere el desarrollo de sistemas interoperables basados en una gestión de metadatos sustentable, que garantice el entendimiento de la información intercambiada, la correcta aplicación de reglas de seguridad específicas y la preservación de los datos a través del tiempo.

Los metadatos documentan el contenido, contexto y estructura de los recursos de información para poder soportar su uso continuo y correcto. La descripción de Entidades de Datos se logra gracias a la aplicación de esquemas de metadatos que posibilitan la IO de objetos digitales en espacios de preservación de la información de los entes.

Además de identificar un esquema de metadatos, es necesario incluir lineamientos generales de entidades y elementos de datos, -referente a su estructuración, definición e identificación de terminologías comunes-. Los atributos básicos o elementales a considerar en el modelo conceptual en el ámbito informacional -o semántico- deben cumplir las siguientes características:

- ***Expresividad***, deben tener suficientes conceptos para expresar perfectamente la realidad.
- ***Simplicidad***, deben ser simples para que los esquemas sean fáciles de entender.
- ***Minimalidad***, cada concepto debe tener un significado distinto.
- ***Formalidad***, todos los conceptos deben tener una interpretación única, precisa y bien definida.

Recomendación 15:

Las instituciones describirán detalladamente las Entidades de Datos accesibles por Servicios de Información.

Recurso 7:

En el anexo: “Descripción de Entidades de Datos” se encuentran las pautas necesarias para la especificación detallada de las Entidades de Datos y metadatos.

Descripción de calidad y actualización de datos

Conocer la calidad y el nivel de actualización de los datos es fundamental para que los Organismos Solicitantes puedan utilizarlos con confianza o para que tomen las medidas pertinentes para mitigar los riesgos de utilizar datos erróneos. Es preciso describir claramente y acordar entre las partes las características de calidad y la actualización de los datos publicados.

Reomendación 16:

Los Organismos Proveedores de información deben describir claramente la calidad y el nivel de actualización de los datos y darlos a conocer de forma fehaciente a los Organismos Solicitantes.

Recurso 8:

En el anexo: “Descripción general de calidad de datos” se encuentra una guía con la explicación de los niveles de calidad de los datos.

Estándares para la Interoperabilidad técnica

El objetivo de la IO técnica es proponer un mínimo de estándares tecnológicos requeridos en el intercambio electrónico de datos entre las instituciones. Se recomiendan una serie de especificaciones para que sean adoptadas en los aspectos de seguridad, transporte, mensajería, ciclo

de vida de los servicios, etc. Se describen algunos escenarios básicos y se indican las especificaciones necesarias para su posterior implementación.

En este plano del MIO se ofrece una referencia de arquitectura funcional que permite la clasificación por capas de un conjunto de estándares tecnológicos. En el siguiente gráfico se presentan cada una de las capas propuestas para la arquitectura funcional:

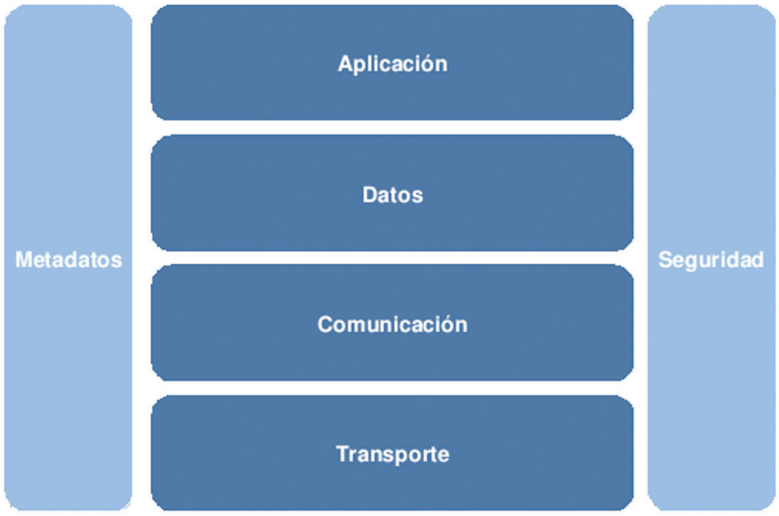


Gráfico 3. Capas de la arquitectura funcional
Fuente. Centro Nacional de Tecnologías de Información (CNTI), 2010

- ***Capa de aplicación:*** Proporciona un medio para acceder a la información sobre el intercambio de los datos a través de aplicaciones como el directorio activo de servicios, entre otros.
- ***Capa de datos:*** Describe las especificaciones de la estructura y codificación de los datos.
- ***Capa de comunicación:*** Establece los protocolos, lenguajes y reglas que son utilizados para normar el intercambio de información entre los participantes.
- ***Capa de transporte:*** Es el canal que habilita los protocolos necesarios para el envío y recepción de archivos, hipertexto, mensajería y paquetes de datos.
- ***Capa de metadatos:*** Esta capa es transversal en la implementación de la IO. Enriquece la representación estándar de datos como elementos o nodos de información requeridos para habilitar funcionalidades adicionales en los servicios. Es importante destacar que el término metadato empleado en esta capa es referencial sólo para la arquitectura funcional de IO técnica, y no debe asociarse con la definición de metadato descrita en la IO informacional.
- ***Capa de seguridad:*** Esta capa es también transversal en la implementación de la IO, en ella se describen los diversos estándares tecnológicos para garantizar el cumplimiento de políticas como cifrado de datos, no repudio, autorización, autenticación, integridad, entre otros.

Especificaciones técnicas

Las especificaciones técnicas sugeridas para el intercambio básico de mensajes entre sistemas heterogéneos son ampliamente recomendadas en el contexto internacional.

Recomendación 17:
Las instituciones utilizarán los estándares técnicos identificados en el MIO para la implementación de la IO.

Recurso 9:
En el anexo: "Especificaciones técnicas" se puede encontrar la lista de los estándares recomendados.

Estándares según esquemas

El objetivo de esta sección es definir un conjunto de esquemas de intercambio de datos entre organismos con diferentes características y establecer los estándares necesarios para cada caso. Es necesario contemplar las siguientes acciones:

- Delimitar el esquema.
- Identificar el tipo de intercambio.
- Identificar las características del esquema independientes de la arquitectura.
- Realizar las recomendaciones sobre las cuales se debe seleccionar el esquema.

En las siguientes secciones se presentan los esquemas correspondientes para la implementación del intercambio de datos entre organismos de la AP. En las subsiguientes versiones del MIO se irá ampliando el conjunto de esquemas para cubrir otros más complejos.

Es importante destacar que para todos los esquemas identificados, se establece el formato XML como el estándar para el intercambio electrónico de datos entre los sistemas de información de la AP.

Recomendación 18:
Utilizar las especificaciones establecidas para implementar intercambios según el escenario especificado.

Esquema 1: Intercambio de información bilateral

Esquema 1.1 Arquitectura de Servicios Web

Este tipo de esquema opera para intercambios bilaterales entre instituciones de la AP a través del uso de arquitecturas de Servicios Web, Web Semántica y la combinación de ellas. En la siguiente sección se muestra cada uno por separado. [*Ver gráfico 4*]

En esta arquitectura el protocolo de comunicación recomendado es SOAP, soportado por contratos de servicios (WSDL) que especifiquen su funcionalidad y las políticas establecidas para la comunicación.

Puede operar en ambientes síncronos o asíncronos en función de los acuerdos de nivel de servicio suscritos entre las instituciones involucradas, los cuales responden a los requerimientos de información identificados en los PII. Aplica también para intercambios en línea y fuera de línea.

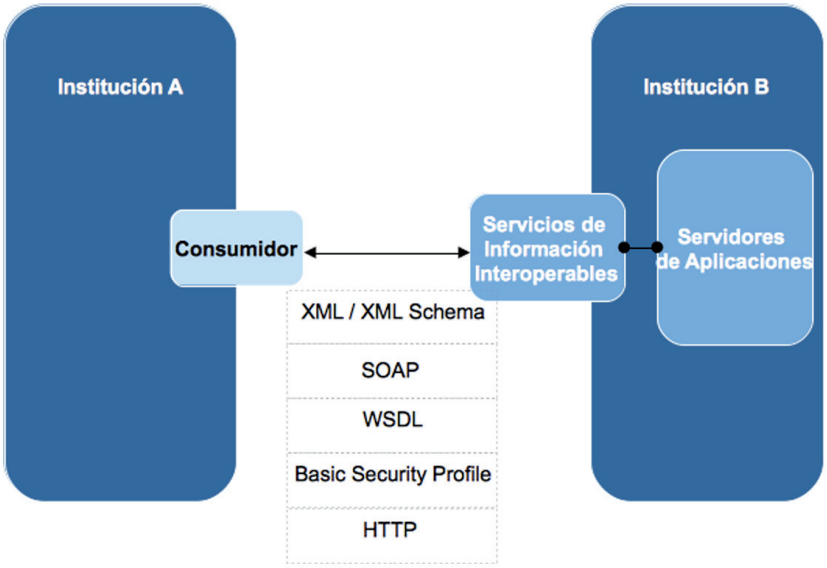


Gráfico 4. Intercambio de información con base a una arquitectura de Servicios Web de forma bilateral
Fuente. Centro Nacional de Tecnologías de Información (CNTI), 2010

Los estándares de seguridad que pueden aplicarse en este tipo de arquitectura son: conexiones seguras tipo VPN, SSL, TLS, etc, dado que las conexiones son puntuales entre instituciones, como se muestra a continuación:

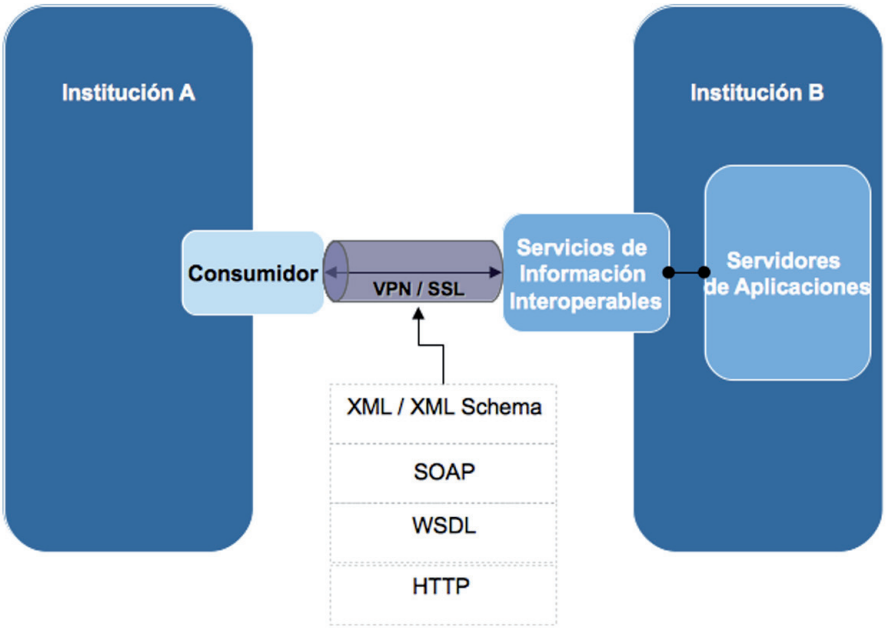


Gráfico 5. Intercambio de información con base a una arquitectura de Servicios Web de forma bilateral implementado VPN/SSL como capa de seguridad
Fuente. Centro Nacional de Tecnologías de Información (CNTI), 2010

Recomendación 19:
Las Instituciones utilizarán los estándares técnicos identificados en el Esquema 1.1 cuando deban realizar intercambios bilaterales autónomos.

Recomendación 20:
Utilizar los estándares de seguridad para Servicios Web, en particular el Basic Profile Security (WS-I).

Recurso 10:
En el anexo: "Recomendaciones para la implementación de Servicios Web" se incluyen una serie de consideraciones para el intercambio de información mediante la publicación y consumo de servicios.

Esquema 1.2 Arquitectura basada en Web Semántica o Web 2.0

Este esquema aplica para el descubrimiento y representación de datos de la AP, de manera uniforme y estandarizada en formatos universales a través de Internet. Esta arquitectura se recomienda para la consulta de datos públicos disponibles por las instituciones de la AP.

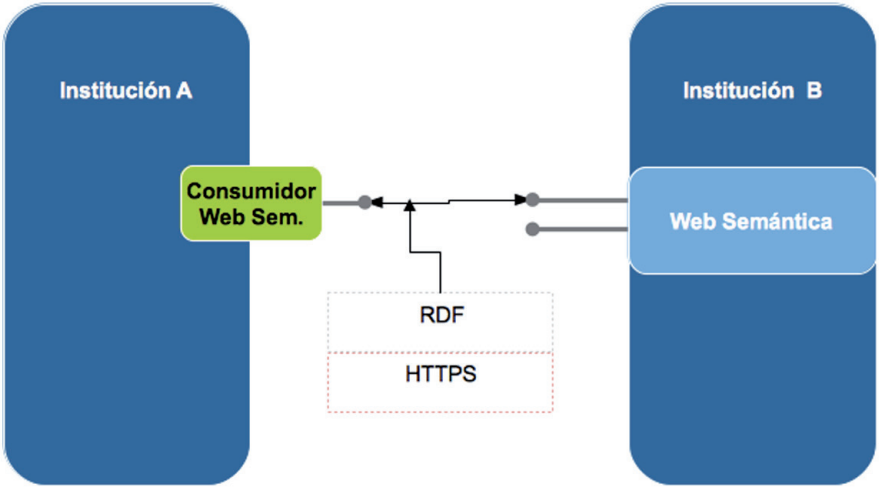


Gráfico 6. Intercambio de información con base a una arquitectura de Web Semántica de forma bilateral
Fuente. Centro Nacional de Tecnologías de Información (CNTI), 2010

Los formatos estándares de representación de conocimiento válidos son: RDF -capa de comunicación-, JSON y XML dependiendo del consumidor final y la necesidad de presentación de dichos datos.

Esta arquitectura opera sólo en ambientes síncronos en función de los acuerdos de nivel de servicio suscritos entre las instituciones involucradas.

Recomendación 21:
Usar certificados electrónicos para validar la fuente de los datos.

Esquema 1.3 Arquitectura híbrida basada en Servicios Web con Web Semántica

Esta arquitectura es el resultado de la combinación de las arquitecturas planteadas en los gráficos 5 y 6, cuenta con la implementación de Servicios Web para el intercambio de información, soportado por la definición de datos y metadatos en Web Semántica. Esta combinación es ideal para ambientes heterogéneos, donde se contemple la consulta de datos públicos y la intervención de operaciones que lleven a cabo una acción específica en una determinada aplicación. Las especificaciones de implementación de este escenario, así como los lenguajes de representación y comunicación son los utilizados en los esquemas mencionados con anterioridad.

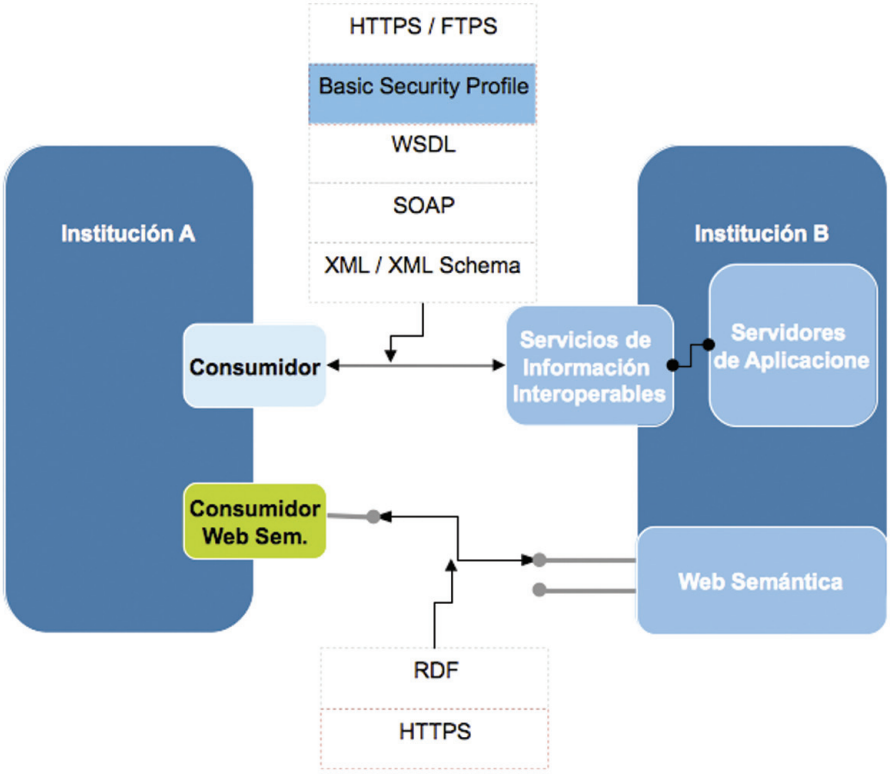


Gráfico 7. Intercambio de información con base a una arquitectura de Servicios Web y Web Semántica de forma bilateral
Fuente. Centro Nacional de Tecnologías de Información (CNTI), 2010

Esquema 2. Intercambio de información multilateral con capa de integración

Este tipo de esquema utiliza como base las arquitecturas planteadas para los escenarios bilaterales, por lo que las recomendaciones realizadas anteriormente aplican también en este contexto. La diferencia se encuentra en la incorporación de una capa de integración común mediante la implementación de un bus de servicios que permite el intercambio masivo de información entre dos (2) o más instituciones.

El escenario planteado a continuación puede operar en ambientes síncronos o asíncronos en función de los acuerdos de nivel de servicio suscritos y aplica para intercambios en línea y fuera de línea. En el siguiente gráfico se ilustra el intercambio entre varias instituciones.

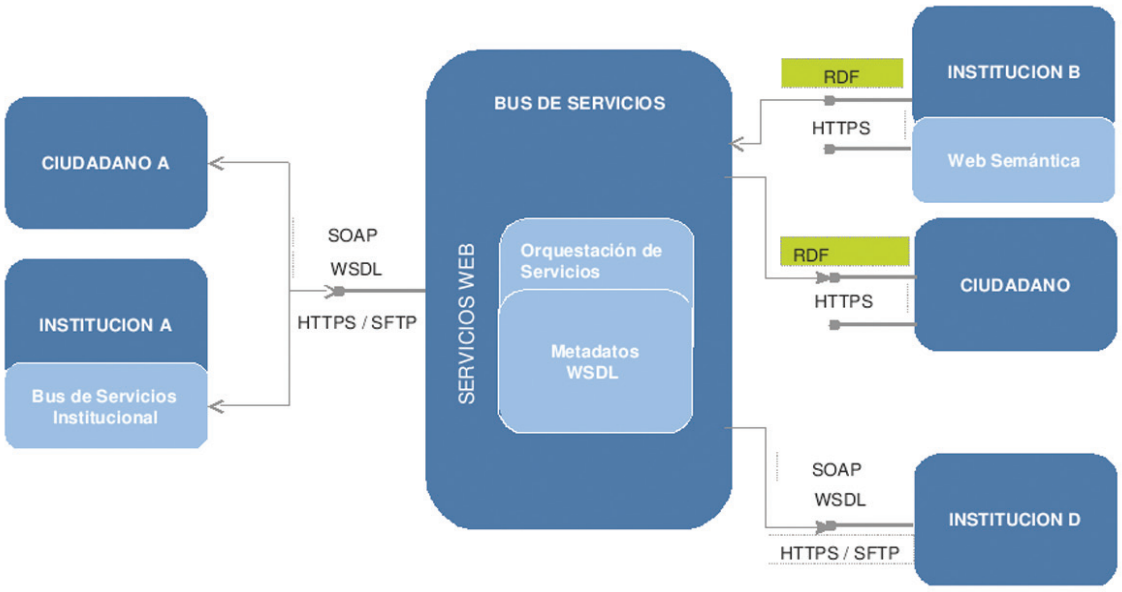


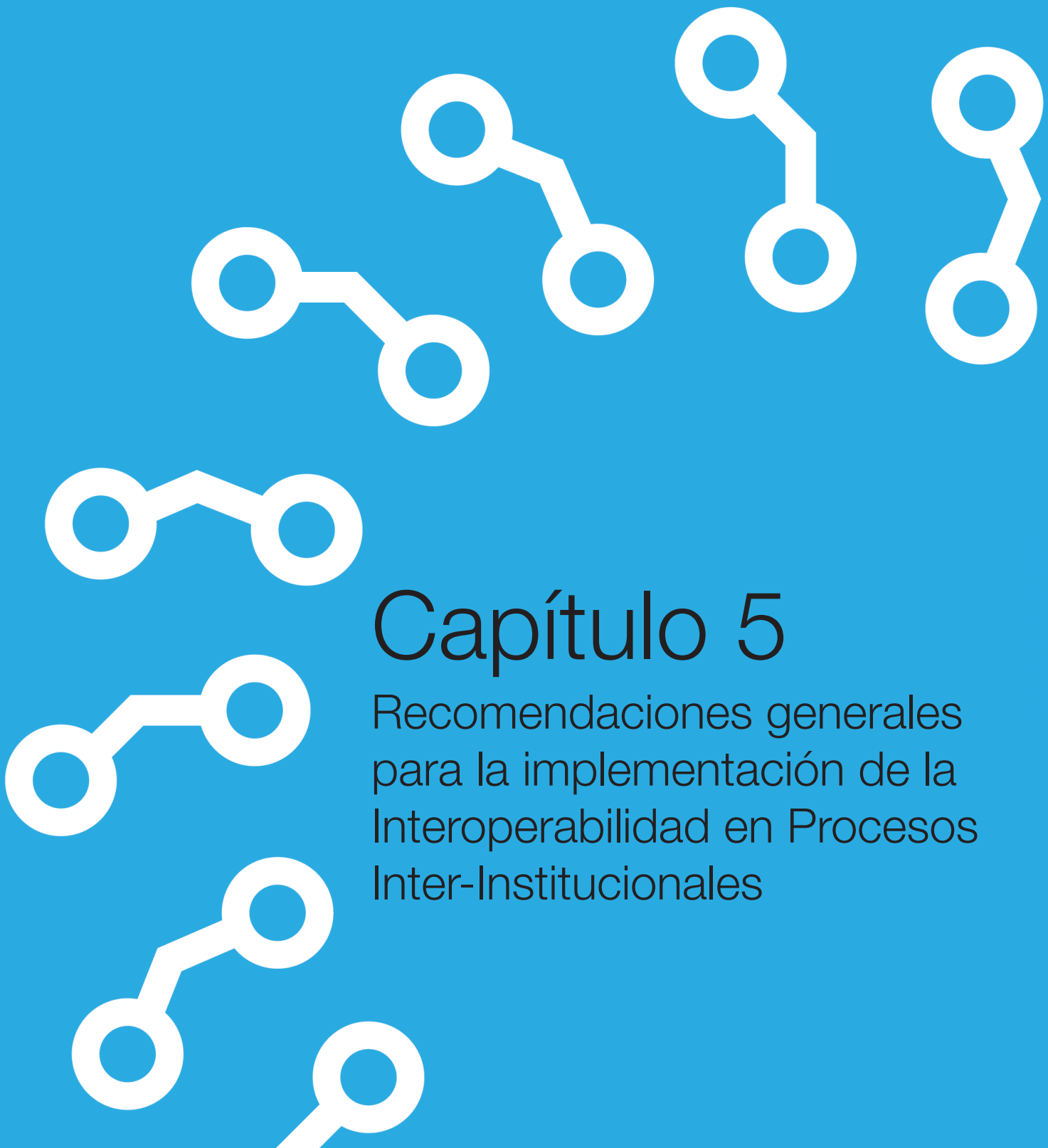
Gráfico 8. Intercambio de información con base a una arquitectura de Servicios Web y Web Semántica con capa de integración
Fuente. Centro Nacional de Tecnologías de Información (CNTI), 2010

Recomendación 22:

Utilizar los estándares técnicos identificados en el Esquema 2 cuando se deban publicar servicios por medio de un bus.

Recomendación 23:

Incorporar un repositorio de Servicios Web para la definición y publicación de los diferentes servicios desplegados en el bus.



Capítulo 5

Recomendaciones generales para la implementación de la Interoperabilidad en Procesos Inter-Institucionales

Recomendaciones generales
para la implementación de la Interoperabilidad en Procesos Inter-Institucionales

Complementariamente a lo establecido a lo largo del presente Marco de Interoperabilidad (MIO), se recomienda a las instituciones de la Administración Pública (AP):

1. Adoptar los estándares, principios, políticas y demás contenidos de este marco y de sus futuras versiones, en forma progresiva y de acuerdo a sus capacidades.

2. Destinar los recursos necesarios para cumplir con las recomendaciones impuestas en el presente marco.

3. Rediseñar sus procesos focalizando el servicio en la sociedad, identificando tanto los datos que puede utilizar provistos por otros organismos como los datos que se puede proveer a otros.

4. Establecer los instrumentos legales que faciliten la publicación y el consumo de Servicios de Información.

5. Establecer todos los recursos y las buenas prácticas necesarias con el fin de asegurar el cumplimiento del principio de seguridad, particularmente en lo referente al manejo de información confidencial y personal.

6. Canalizar las necesidades de adecuaciones a los recursos relacionados a la Interoperabilidad mediante las vías establecidas.

7. Incorporar en los nuevos sistemas las capacidades de publicación y consumo de servicios provistos por otros organismos, aplicando las recomendaciones del MIO.

8. Desarrollar las competencias y habilidades necesarias para el consumo, implementación y prestación de Servicios de Información en cumplimiento general del MIO y demás documentos asociados.

9. Las Instituciones deben fomentar la colaboración y participación entre sí para facilitar la gestión de conocimiento.

10. Todos los órganos alcanzados por el presente marco deben poner a disposición de los demás, los Servicios de Información que sean de utilidad, a través del registro de Servicios de Información que sea establecido para tales fines, así como mantener actualizada la información publicada por esa institución.

Adicionalmente se invita a los organismos de la AP a:

- Participar en la actualización permanente del MIO.
- Participar en la implementación del Plan de implementación de la Interoperabilidad en Venezuela, con los respectivos planes de Interoperabilidad institucionales.
- Participar en el establecimiento de los mecanismos requeridos para la discusión pública del MIO.
- Divulgar y promocionar los avances de la Interoperabilidad.
- Establecer mecanismos de control para garantizar de forma efectiva la aplicación de las disposiciones establecidas en este marco.

Las unidades y organismos incluidas en el Componente de Gobernanza junto con la participación colaborativa de todos los organismos de la AP, están invitadas a:

- Establecer un plan estratégico para el desarrollo de la Interoperabilidad que deberá ser adoptado, de forma progresiva, por organismos de la AP.
- Mantener actualizado en forma permanente el MIO.
- Establecer, implantar y divulgar indicadores de gestión de los resultados obtenidos mediante la implantación del MIO vigente en cada momento.

Definiciones

Definiciones y acrónimos

Definiciones y acrónimos

Acuerdo de nivel de servicio: También conocido como SLA -por sus siglas de Service Level Agreement-, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar los niveles de servicio y calidad acordados para un servicio. Es una herramienta que ayuda a ambas partes a llegar a un consenso en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, solución de conflictos, etc.

Adendas: Apéndice o conjunto de notas añadidas después de terminada una obra escrita para aclarar, completar o rectificar su contenido.

Asíncrono: Se refiere a intervalo de tiempo no constante entre cada evento registrados dentro de algún escenario.

Bus de servicio: Aplicación informática desarrollada para la integración de sistemas que desean compartir información automáticamente. Es una solución de integración distribuida que proporciona una comunicación fiable entre los distintos recursos tecnológicos tales como aplicaciones, plataformas y servicios, que se encuentran de manera desagregada.

Cadena de valor: Sucesión procesos enlazados de forma ordenada e interconectada que en conjunto produce un resultado consumible por un usuario.

Dato: Es una representación de un hecho, concepto o instrucción formalizado y adecuado para la comunicación, interpretación o procesamiento por medios automáticos o humanos.

Emisor: La aplicación del Organismo Solicitante que genera y envía al Proveedor los mensajes con requerimientos.

Entidad de Datos: Conjunto de datos o de otras entidades de datos relacionados entre si por una coherencia lógica, temática o funcional. Es un concepto equivalente a entidad en el modelo entidad/relación en el paradigma orientado a objeto.

Estándar: Toda especificación que ha sido establecida de uso obligatorio -estándar de jure- en algún contexto o adoptada de forma voluntario masivamente -estándar de facto-.

Estándar abierto: Es aquel estándar que: (i) esté publicado y su especificación y documentación completas están disponibles de forma gratuita o al precio de coste de su distribución; (ii) su propiedad

intelectual se ofrece de forma irrevocable libre de regalías, de cualquier otro derecho de explotación de la propiedad intelectual, y no sujeto a patentes o contratos que restrinjan su uso y reutilización directa o indirectamente; (iii) existe al menos una implementación de referencia que desarrolla todas las funcionalidades de la especificación, que está disponible bajo una licencia que permite que sea usada para cualquier propósito, y que puede ser copiada, estudiada, mejorada y distribuida libremente, con o sin cambios.

Gobierno Electrónico: Uso de las tecnologías de información y comunicación por parte de las instituciones de gobierno, para mejorar cualitativamente los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana.

IO: Interoperabilidad

LDAP: Protocolo de Acceso Ligero a Directorio. Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio, ordenado y distribuido para buscar informaciones diversas en un entorno de red.

Metadatos: Son datos que describen otros datos

MIO: Marco de Interoperabilidad

MOIO: Modelo Organizativo para la implementación de la Interoperabilidad en Venezuela.

Organismo Proveedor -de un Servicio de Información-: Organismo que provee -publica, mantiene en producción y resuelve- un Servicio de Información que permite a un Organismo Solicitante consumirlo y, por medio de este, interrelacionar sus sistemas informáticos.

Organismo Solicitante -de un Servicio de Información-: Organismo que utiliza o ejecuta un Servicio de Información publicado por un Organismo Proveedor.

Persistencia: Capacidad de persistir o mantener información de contexto para sostener una sesión a lo largo del tiempo.

PII: Procesos Inter-Institucionales.

PIIO: Plan para la implementación de la Interoperabilidad en Venezuela.

Plataforma tecnológica: Son todos los medios utilizados para procesar, almacenar y transmitir la información. La plataforma tecnológica esta compuesta por la arquitectura y el inventario de activos de información que esta contiene.

Proceso: Es un conjunto de actividades y tareas relacionadas lógicamente llevadas a cabo para lograr un resultado definido. Cada proceso tiene sus entradas, funciones y salidas. Las entradas son requisitos que deben tenerse antes de que una función pueda ser aplicada. Cuando una función es aplicada a las entradas de un método, tendremos ciertas salidas resultantes. Como colección estructurada de actividades relacionadas se espera que produzcan un valor para la organización o sus usuarios. Un Proceso de Negocio puede ser parte de un proceso mayor que lo abarque o bien puede incluir otros procesos de negocio que deban ser incluidos en su función. Los procesos se definen con cierto grado de formalidad, puede ser medidos su funcionamiento y desempeño, tienen resultados específicos, entregan resultados a usuarios y responden a alguna acción o evento específico que los activa. Los procesos de negocio son vistos como un recetario para hacer funcionar un negocio y alcanzar las metas definidas en la estrategia de negocio de la empresa.

Procesos Inter-Institucionales: Es el subconjunto de procesos que realizan las instituciones con la intervención de dos o más organismos.

Proveedor: Aplicación del Organismo Proveedor que recibe y procesa los correspondientes requerimientos emitidos por el emisor.

Publicación de Servicios de Información: Poner en disponibilidad de uso un Servicio de Información a otros organismos. Por extensión se puede aplicar a las Entidades de Datos que un servicio permite acceder.

Recurso: Todo producto terminado necesario para llevar adelante el proceso de Interoperabilidad, ya sea software, hardware, procedimientos, documentación, instrumentos legales, marcos de referencia, etc.

Servicio: Conjunto de actividades que buscan proporcionar valor agregado a los usuarios, al ofrecer un beneficio o satisfacer sus necesidades.

Servicio Web: Sistema de software diseñado para permitir interacción máquina a máquina en una red. En general, los servicios web son sólo APIs Web que pueden ser accedidas en una red, como internet, y ejecutadas en un sistema de hosting remoto.

Síncrono: Intervalo de tiempo constante entre cada evento. Por ejemplo, existen procesos síncronos que dependen de un acontecimiento externo que dispara una acción.

Sistema legacy/heredados: Sistema informático -equipos informáticos o aplicaciones- que ha quedado anticuado pero continúa siendo utilizado por el usuario -típicamente una organización o empresa- y no se quiere o no se puede reemplazar o actualizar de forma sencilla.

SOAP: Protocolo de Acceso a Objeto Simple - por sus siglas en inglés Simple Object Access Protocol-, es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.

Tasa de contención: Límite superior de requerimientos del solicitante a un Proveedor. Se especifican como un conjunto de restricciones escritas en términos de cantidades por unidad de tiempo. Pueden utilizarse combinaciones complejas por ejemplo: no más de km transacciones por minuto y no más de kh transacciones por hora.

Tasa de servicio: Límite inferior de requerimientos que el proveedor garantiza satisfacer al solicitante. Se especifica en los mismos términos que la tasa de contención.

Taxonomías: Ciencia que se ocupa de los principios,métodos y fines de la clasificación.

Ticket: Componente informático que representa una asignación temporal de credenciales electrónicas para verificar la identidad de un cliente ante un servicio particular. El ticket es emitido por un servidor de autenticación para un servicio ante la solicitud de un cliente debidamente autenticado. Está compuesto fundamentalmente por un Token y una Firma.

Trámite administrativo: Conjunto ordenado de tareas, actividades, diligencias, actuaciones o gestiones que deben realizar los ciudadanos ante un organismo de la Administración Pública para adquirir un derecho o cumplir con una obligación.

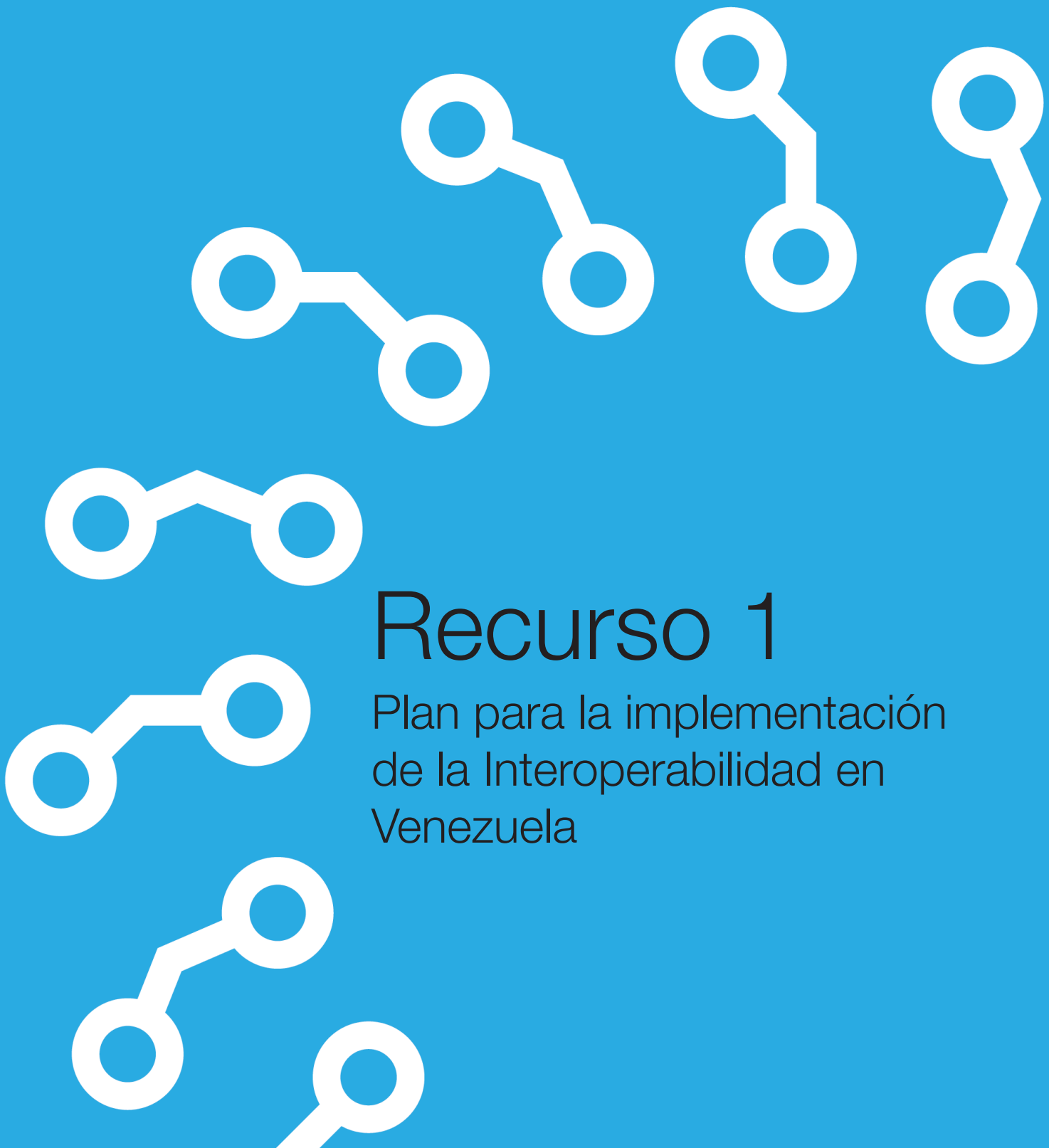
URL: Localizador de Recurso Uniforme -por sus siglas en inglés Uniform Resource Locator-, la dirección global de documentos y de otros recursos en la World Wide Web.

Web semántica / Web 2.0: Es una evolución en el desarrollo de la www donde la parte semántica de la información y servicios de la web se definen, haciendo lo posible para que los usuarios y las

aplicaciones puedan interactuar mejor a la hora de realizar peticiones de contenidos.

WSDL: Lenguaje de Descripción de Servicios Web -por sus siglas en ingles Web Services Description Language- , un formato XML que se utiliza para describir servicios Web.

Anexos



Recurso 1

Plan para la implementación de la Interoperabilidad en Venezuela

Plan para la implementación de la Interoperabilidad en Venezuela

Objetivo

Establecer las bases y los lineamientos para iniciar la implementación de la Interoperabilidad en Venezuela.

Contexto

Para comprender el propósito de este documento, es preciso reconocer que la Interoperabilidad (IO) no puede ser considerada una especialidad madura. A pesar de los años de desarrollo que lleva en el mundo, la producción de marcos, normativas específicas, casos de éxito, productos de alta tecnología, presentaciones magistrales y trabajos académicos; no es posible hoy día, presentar una metodología probada para su implementación. Dada la variedad de experiencias aisladas, aciertos y errores, se puede proponer una serie de recomendaciones útiles a la hora de dar los primeros pasos en la IO y afianzarlos posteriormente.

A lo largo del texto, se describen un grupo de recomendaciones prácticas para iniciar el camino hacia el cumplimiento de uno de los mandatos más fuertes que exige la reforma del Estado bajo los lineamientos del Gobierno Electrónico y recomendaciones de tipo estratégico que deben en algún momento ser encaradas para asegurar la calidad y la viabilidad de la IO. Adicionalmente, se presentan algunos consejos para dar los primeros pasos y establecer las bases para su generalización.

La eficacia de los recursos y prácticas resultantes de las recomendaciones aquí expuestas, requiere de una debida contextualización en el entorno institucional en el que deben incorporarse y operar. La historia, las tradiciones, el contexto socio-económico, el marco político-legal y los proyectos en curso en cada realidad son factores que condicionan los contornos específicos de cualquier modelo genérico.

Sin exclusión a lo anterior, las recomendaciones realizadas se han ajustado en lo posible a la situación venezolana conocida y se han realizado propuestas específicas a las que les faltaría coordinar los recursos a aportar para convertirlas en un documento de proyecto. Suposiciones, que no pueden ser realizadas dentro del alcance del este documento.

Recomendaciones para la implementación de la Interoperabilidad

Se incluye a continuación una serie de recomendaciones, generales y específicas, para llevar adelante planes de implementación de la IO. Basado en estas sugerencias se diseñaron los planes que se presentan en los apartados subsiguientes.

Recomendaciones generales

A continuación se explican algunas recomendaciones generales que deben ser cabalmente entendidas y aplicadas en todos los aspectos de la IO:

1. ***Asumir la complejidad y la variedad de temas involucrados en la Interoperabilidad.*** El Marco de Interoperabilidad (MIO) permite comprender la gran variedad de temas relacionados a la IO. El proceso de apropiación social de la tecnología y los distintos temas deben ir articulándose entre sí para que el conjunto tenga coherencia y sea viable. Se considera sumamente importante que la IO sea entendida de una manera amplia y se tengan en cuenta todos los aspectos en su análisis. Esfuerzos parciales pueden hacer fracasar proyectos en los puntos más débiles.

2. ***Abordar la apropiación de la Interoperabilidad como un proceso gradual.*** Para abordar una situación tan compleja y variada, se recomienda la aplicación de un proceso de construcciones sucesivas, cada vez más elaboradas, que permitan generar experiencia para avanzar sobre bases más sólidas. La aplicación de modelos de madurez en otros contextos evidencia que saltar niveles suele ser poco productivo y que un nivel significativamente mayor en algún aspecto aislado, no suele ser provechoso. Los logros más sustentables se dan cuando se avanza de forma pareja en la diferentes dimensiones pero con niveles de capacidad institucionales similares. Las estrategias incrementales aseguran resultados más previsibles; permiten responder con menor riesgo a la demanda; anticipar con más precisión los impactos, costos, beneficios y ampliar la capacidad para prever el comportamiento de los involucrados. La viabilidad de las decisiones queda asegurada ya que se basa en un itinerario empírico lento y sostenido en el que los errores pueden ser rápidamente absorbidos. Este enfoque requiere de constancia y continuidad para lograr cambios generalizados.

3. ***Aplicar una planificación estratégica situacional.*** Las actividades a realizar son muchas y se prolongan en el tiempo. Por ello, deben ser planificadas, pensando hoy donde se quiere estar mañana. La planificación se refiere a hacer caminos para transitar hacia al futuro, no a predecirlo. Este modo de trabajo nos ayuda a crear con base en las posibilidades futuras que seamos capaces de imaginar y descubrir. Es preciso tener en cada instancia objetivos claros y los indicadores que permiten saber en que medida éstos se han cumplido.

4. ***Rediseñar los procesos.*** Apropiar la capacidad de interoperar crea posibilidades inexistentes en el momento en que fueron definidos los procesos actuales, por ende, éstos deben ser definidos nuevamente. Se debe evitar incluir tecnología en procesos existentes sin antes evaluar su necesidad. El mayor

valor agregado se logra cuando a la apropiación de la tecnología se le suma la reingeniería de los procesos.

5. ***Entender la seguridad, la calidad y el nivel de servicio como procesos transversales.*** El enfoque basado en procesos lleva implícito el control continuo, alineado a la gestión de la calidad que enfatiza: la importancia del cumplimiento de los requisitos o necesidades, la consideración de los procesos en términos que aporten valor, la obtención de resultados de desempeño y eficacia del proceso y la mejora continua de los procesos con base en mediciones objetivas. Como se expone en el MIO, las variables seguridad, calidad y nivel de servicio son transversales a todas las demás y deben estar presentes en todos los aspectos y niveles de la IO.[1]

6. ***Aplicar el principio de Parsimonia.*** Para enfatizar las recomendaciones anteriores se propone como matriz de pensamiento la apropiación de la IO según el principio de Parsimonia en sus versiones más básicas: “en igualdad de condiciones se debe preferir la solución más sencilla” o “no deben utilizarse más componentes que los absolutamente necesarios”. La preocupación por la eficiencia de la gestión pública es relevante en su totalidad. El tratamiento de los instrumentos debe realizarse en plena consideración de los objetivos de la acción estatal y como referencia a las configuraciones de poder que les sirven de sustento. Es preciso darle a cada situación su importancia y su aporte a las políticas públicas a las que sirve. Deben diseñarse soluciones sencillas que cumplan con los requisitos fundamentales. El crecimiento se deberá ir generando con base en experiencias concretas y el análisis real de necesidades.

Recomendaciones para la fase inicial

Se describen a continuación las recomendaciones para iniciar la primera fase de apropiación de la IO. Aunque estas recomendaciones se presenten en forma separada, están fuertemente interrelacionadas entre sí. Por lo tanto, es fundamental realizar el ejercicio de entenderlas como conjunto organizado.

7. ***Establecer un modelo de gobernanza.*** La cantidad de actividades a desarrollar y variedad de actores involucrados en el proceso de apropiación de la IO exige un modelo que asegure el establecimiento de objetivos, guíe las acciones hacia éstos y verifique el camino realizado. El ejercicio de la IO debe ser una tarea de todas las partes involucradas. Algunas actividades como la planificación estratégica, la promoción, el control y la asistencia técnica, resultan beneficiosos al estar centralizados en algún área específica y reconocida con buen manejo de recursos políticos. El modelo de gobernanza requiere de una coordinación de políticas, principios rectores y metas que permitan conocer los objetivos a alcanzar. También requiere de indicadores sistemáticos que permitan saber si se está recorriendo correctamente el camino establecido.

8. ***Elaborar estándares básicos.*** Elaborar y mejorar los estándares será una tarea permanente en la implementación y mantenimiento de la IO. Se recomienda partir de un conjunto muy básico de estándares para evitar distorsiones iniciales difíciles de corregir una vez implementados. Los estándares técnicos básicos son candidatos a ser establecidos junto a los aspectos informacionales y organizacionales. En las implementaciones de casos pilotos se podrán evaluar las decisiones tomadas.

[1] No se harán recomendaciones específicas sobre estos temas. Se asume que tendrán que ser considerados en todo momento.

9. ***Implementar casos pilotos.*** La implementación de los casos pilotos genera múltiples resultados: la experiencia obtenida en la aplicación de los recursos utilizados, la capacitación y la obtención de elementos de difusión y promoción que pueden ser aprovechados para motivar a otros actores. Estos casos deben seguir las buenas prácticas de planificación y ejecución de un proyecto inserto en un programa más amplio. Son los primeros de un conjunto mayor de implementaciones y no pueden ser considerados de manera aislada. El Ente Coordinador tiene un rol central en la ejecución de la implementación de proyectos pilotos como garante de la experiencia, articulador de estándares y demás recursos, mientras que los organismos involucrados llevan adelante el peso de la implementación en sí.

   Es preciso seleccionar cuidadosamente los procesos a implementar como casos pilotos; encontrar un equilibrio entre complejidad, viabilidad, utilidad y atractivo político-social que aseguren su puesta en producción en buenas condiciones. Por ello, se deben definir los criterios sobre los cuales se seleccionarán los casos, en particular los casos pilotos. Algunos de los criterios de selección que pueden ser utilizados:

   - Complejidad accesible. La complejidad –en todos los aspectos– debe ser atendida con los recursos disponibles y con la madurez para abordarlos con éxito. Los estándares y demás recursos deben ser suficientes para resolver los problemas que presente el caso.

   - Interés de los actores involucrados. Los actores involucrados, en particular los responsables de los organismos, deben estar interesados en llevar adelante el proyecto y manifestarlo disponiendo de la mayor parte de los recursos necesarios para su realización.

   - Impacto deseable. El resultado de implementar el caso debe ser atractivo para algún conjunto de destinatarios, particularmente al mostrar los beneficios alcanzados.

   - Alineación a las políticas públicas. Los casos a tratar deberían estar alineados a alguna política pública bien ubicada en la agenda del gobierno, para que sea atractiva para los cuadros políticos y se realicen esfuerzos funcionales a las acciones del gobierno en curso.

   También pueden seleccionarse casos pilotos por otros criterios que no respondan directamente a la provisión de Procesos Inter-Institucionales (PII). Por ejemplo:

   - Publicar registros básicos. Al poner a disponibilidad de los organismos datos de una entidad sin que necesariamente estén atados a un servicio específico, se puede incentivar el consumo para fines no específicos.

   - Generar la base de un modelo. No todos los procesos pueden resolverse con un único modelo. Propiciar el desarrollo de los recursos necesarios para llevarlo adelante puede ser una buena estrategia para que luego sea replicado por otros.

   - Forzar la innovación. A partir de forzar la resolución de un caso que requiere de recursos no desarrollados aún, se pueden lograr soluciones novedosas que podrán ser reutilizadas por otros sin la necesidad de invertir nuevamente en su desarrollo.

   - Producir un efecto demostración. Algunas reformulaciones son fáciles y baratas de implementar. Aunque

no sean sumamente interesantes pueden impulsarse para producir efectos de demostración y avanzar rápidamente en la reformulación de procesos.

- Estandarizar los PII en funcionamiento. La reformulación de PII pre-existentes fuera de los estándares puede ser una buena estrategia para ir eliminando las situaciones de excepción. Esto deberá sopesarse para invertir en temas ya resueltos con bajo riesgo.

- Avanzar en una temática específica. Con acuerdo de la comunidad en particular se puede avanzar en algún programa de gran alcance como puede ser salud, educación, servicios empresarios, energía, etc. Suelen ser proyectos ambiciosos que requieren un fuerte compromiso. No suelen ser proyectos indicados para iniciar la implementación de la IO sino para etapas con mayor madurez.

10. ***Documentar la experiencia.*** La experiencia de implementar los casos pilotos debe dejar su rastro en personal más capacitado. Estas experiencias deben guiar una parte de la actualización de los recursos y estándares necesarios para la implementación de la IO definidos en el MIO.

Recomendaciones para afianzar la Interoperabilidad

Esta sección incluye una serie de recomendaciones aplicables, cuando resultados semejantes a los producidos en el proceso descrito en la sección anterior sean realidad. Es posible que algunas sugerencias se realicen en paralelo al desarrollo de las acciones resultantes de las estrategias precedentes. Esto dependerá, fundamentalmente, de los recursos disponibles.

11. ***Gestionar un portafolio.*** La existencia de portafolios, conocidos también como inventarios, es fundamental para asegurar el buen desarrollo de los planes. Es importante hacer esfuerzos y lograr interesar a los involucrados para mantener la información actualizada, lo cual puede ser una buena práctica de IO. En todos los casos deberán desarrollarse herramientas informáticas cada vez más sofisticadas para gestionar estos portafolios. Los principales portafolios a crear y mantener son:

    - Inventario de procesos. El inventario de todos los procesos del Estado es una fuente formidable de información para la gestión pública. Su recopilación inicial y mantenimiento pueden ser muy costosos y no necesariamente útil en un principio. Se recomienda dejarlo como un programa a largo plazo y atacar su construcción como un proceso continuo y creciente a la par de otras acciones de implementación. Este portafolio debe servir como base para la selección de los PII a implementar y para llevar un control de lo realizado y lo pendiente.

    - PII. La identificación y descripción detalladas de los PII y de los servicios involucrados es precisamente una de las fuentes fundamentales para la gestión de la IO. Tanto si fueron desarrollados bajo el MIO o no.

    - Servicios. Los Servicios de Información publicados y en desarrollo que sean parte -o no- de PII también deben estar inventariados y publicados de forma que puedan ser fácilmente descubiertos. La publicación de servicios con vistas a que sean consumidos lo más posible, es una de las actividades centrales de la implementación de la IO. Es fundamental darlos a conocer y contabilizarlos, éstos pasan a formar

parte del activo tecnológico del Estado. Los datos involucrados en cada Servicio de Información deben ser documentados y catalogados.

- Entidades de Datos. Las Entidades de Datos bien descritas y catalogadas deben ser inventariadas y publicadas de forma que puedan ser fácilmente explotadas.

- Recursos y experiencias. El inventario de recursos desarrollados para dar soporte a los PII y a los Servicios de Información pueden ser una fuente interesante para evitar el despilfarro de recursos rehaciendo lo ya existente.

- Relaciones y capacidades. Al estilo de una red social profesional, permite la interrelación de los funcionarios involucrados en los procesos y la conformación de una Comunidad Práctica, parte esencial del ejercicio de la IO, con beneficios que van más allá de la simple implementación de PII.

Estos inventarios no son independientes entre sí, están fuertemente relacionados y sería útil que existiera un sistema de información que permitiera la relación y explotación integral de esta información, conformando la gestión de la IO y de los datos públicos. Éste sigue siendo uno de los temas más complejos de la IO, donde todavía no se cuenta con soluciones integrales de costo razonable. Se sugiere comenzar con una descripción básica pero estandarizada de los datos y del conjunto de servicios puestos en producción. Esta recomendación también corresponde a una fase inicial que será complementada en niveles más avanzados.

12. ***Formar al talento humano.*** La capacitación en IO es esencial, ya que ésta no forma parte de ninguna formación específica. Es una mezcla de muchas profesiones o disciplinas diferentes. La adopción de prácticas plurales requiere tanto de componentes de cambio personal, como de la adopción de nuevos instrumentos y del establecimiento de vínculos interpersonales. Es importante ir formando funcionarios de diferentes especialidades pero relacionados a los procesos de los organismos. Dada la importancia de la modificación actitudinal que requieren los cambios organizacionales y reconociendo la importancia que la formación del personal involucrado en estos procesos tiene sobre el logro de los objetivos, es fundamental fortalecer las capacidades de los organismos por medio de la capacitación de sus funcionarios. Además de la formación básica es relevante establecer lazos profesionales entre las partes. Esto se puede alcanzar impulsando la inclusión de ejercicios motivacionales y de integración grupal en las actividades de capacitación presencial y fomentando la interrelación con herramientas de cooperación virtuales.

La capacitación en IO tiene como objetivo avanzar en tres líneas complementarias:

- Promocionar y difundir los beneficios y la necesidad del trabajo inter-institucional, haciendo comprender que éste potencia el valor de los organismos en lugar de debilitarlos.

- Hacer conocer herramientas ya probadas en otros ámbitos o por organismos más avanzados.

- Establecer vínculos interpersonales que se reconocen indispensables para la aplicación viable de los instrumentos organizacionales.

Los principales objetivos de estos procesos de capacitación podrían sintetizarse de la siguiente manera:

- Adquirir los conceptos y elementos fundamentales del desarrollo de procesos bajo los lineamientos del Gobierno Electrónico (Gob-e).
- Comprender los beneficios del trabajo inter-institucional para los organismos participantes y para la sociedad.
- Comprender los beneficios y la problemática de la IO como herramienta fundamental para mejorar la gestión de los organismos y la provisión de servicios a la sociedad.
- Conocer experiencias locales exitosas de aplicación de los lineamientos del Gob-e y establecer contactos con los referentes de cada caso.
- Conocer las principales prácticas producciones internacionales sobre IO y las fuentes de información relacionadas.
- Conocer las iniciativas nacionales sobre IO, las fuentes de información relacionadas y establecer contactos con los actores involucrados.
- Conocer las principales leyes o disposiciones legales acerca del intercambio y publicación de datos, con el fin de no incurrir en malas prácticas.
- Adquirir un vocabulario y una práctica de trabajo común con los actores involucrados de la comunidad para la elaboración de procesos.
- Adquirir criterios para la selección de procesos a reformar según los lineamientos establecidos.
- Establecer relaciones con actores involucrados de otros organismos de la misma comunidad por medio de la participación común en actividades y realización conjunta de planes.

No todos los actores requieren del mismo nivel de conocimiento, por lo tanto se recomienda definir por lo menos tres niveles de capacitación:

- Nivel básico para difusión masiva.
- Nivel intermedio para actores relacionados a los procesos, tanto político como operativo.
- Nivel avanzado para actores involucrados en la elaboración de procesos.

Se recomienda forzar la interrelación de funcionarios con los diferentes perfiles involucrados en la IO, tales como: abogados, expertos en organización, informáticos, etc.

13. ***Adecuar el marco legal.*** Para formalizar los intercambios electrónicos de datos y la provisión de servicios en los casos pilotos, no es necesario contar con un marco legal amplio. Los casos pilotos pueden ser soportados por acuerdos entre partes que establezcan mutuas responsabilidades y protejan los intercambios del contexto legal restrictivo que pueda existir. Esta experiencia debe ser aprovechada para ir generando un marco legal más amplio. Los cambios en la normativa pueden requerir reformas profundas en leyes que requieren tiempos por fuera del alcance de un proyecto de implementación inicial. Por ello, se recomienda utilizar recursos legales de alcance limitado que protejan los intercambios definidos y no requieran intervención de partes externas al proyecto. La elaboración de marcos legales para la IO corresponde a niveles más avanzados de madurez. La eliminación de tensiones entre normas; leyes vigentes; las necesidades del Gob-e -en general- y de la IO en particular, es un tema sumamente

complejo. Los cambios deben ser analizados, pensados y madurados en el contexto antes de realizarse. Se considera necesario trabajar conjuntamente con las áreas legales y las sustantivas para elaborar un marco doctrinario, acompañarlo por jurisprudencia y luego por el soporte legal que asegure el intercambio de datos dentro del Estado, respetando las normativas de protección.

14. ***Elaborar modelos.*** En la medida que se avance con implementaciones sólidas, se sugiere aprovechar estas experiencias y generar un modelo para estructurar una solución integral a partir de los componentes utilizados que pueda ser aprovechada en otras situaciones. Estos modelos deben incluir los recursos metodológicos, procesos, software, etc. Es prudente elaborar, publicar y difundir modelos de soluciones genéricas a partir de las experiencias concretas y promover su utilización en situaciones estructuralmente semejantes.

    Muchos procesos pueden ser eficientemente resueltos con modelos semejantes permitiendo resolver problemas complejos más rápidamente, aprovechando la experiencia. Existen algunos ejemplos de modelos típicos de PII, que una vez implementados para un caso, los recursos utilizados pueden ser fácilmente aprovechables nuevamente en otros:

    - Intercambios bilaterales. Dos organismos desarrollan los recursos necesarios para realizar intercambios entre ellos, basado en vínculos bilaterales.

    - Certificaciones digitales. El modelo de certificaciones digitales puede utilizarse en infinidad de casos. Distintos organismos producen continuamente certificados que garantizan que alguien está habilitado ante otro para hacer algo. Si estos certificados se empiezan a publicar masivamente con respaldo legal entre los organismos, evitando el movimiento y la duplicación de los papeles, el impacto puede ser importante. Estas soluciones para ser exitosas, no deben ser sólo logros del organismo que las provee, sino que deben ser reconocidas por los entes y organismos consumidores.

    - Concentradores de datos. Los datos correspondientes a una función distribuida entre muchos organismos pueden ser consultados, por medio de un concentrador, de forma íntegra por medio de un único servicio. Los casos candidatos a este modelo son todos aquellos provenientes de algún modelo distribuido en los organismos regionales, por ejemplo: licencias de conducir, habilitaciones sanitarias, etc.

    - Repositorio unificado. En cada Comunidad de Información se pueden encontrar casos para implementar este modelo, donde un organismo captura y guarda los datos centrales de cierta temática y los provee al resto de los interesados, evitando así la multiplicación de capturas y la redundancia de repositorios. Los balances contables de las empresas y las historias clínicas, aunque con complejidades funcionales, son dos buenos ejemplos de aplicación de este patrón. De esta manera los distintos organismos podrían trabajar conjuntamente para mejorar la calidad de los datos sobre un único repositorio, en lugar de duplicarlos cada uno para sí. Las novedades o defectos sobre los datos detectados por alguno de los organismos usuarios podría ser informado al administrador para que mejore su calidad, aplicándose un principio colaborativo que debería repercutir

en el bien general.

El objetivo de esta recomendación es abstraerse de los casos concretos, sistematizar, generar modelos de soluciones e impulsar la implementación, dejando a disponibilidad formas de resolver problemas o mejorar situaciones. Estas experiencias tienen la riqueza de haber sido realizadas en el mismo ámbito y por actores conocidos, y no ser soluciones exógenas fuera de contexto. Mantener los modelos es un proceso evolutivo que debe realizarse de manera continua.

15. ***Diseñar y proveer infraestructura.*** Los casos pilotos implementados, las definiciones de estándares y los modelos elaborados deben dejar componentes de infraestructura -software, hardware, acuerdos de nivel de servicios asociados y otros recursos- que pueden ser reutilizados en otras implementaciones. Para una situación inicial no es necesaria la utilización de complejas infraestructuras, en caso de estar disponibles se pueden emplear, pero se pueden realizar muy buenas implementaciones con pocos recursos. El exceso en cantidad o complejidad de tecnología no es garantía de mejores PII. Para avanzar de forma sistemática y ordenada se recomienda la utilización de estas plataformas o de una red de éstas que permita manejar con economía una gran cantidad de servicios y proveer un soporte común que garantice seguridad y disponibilidad.

16. ***Reutilizar el software desarrollado.*** La experiencia obtenida en algunos países durante los últimos años ha demostrado que el componente tecnológico no es un problema en términos generales ni es inaccesible para los organismos de pocos recursos. Entre los estándares y desarrollos que se han ido madurando en estos años, se dispone de un conjunto de recursos suficientes para realizar intercambios seguros, robustos y confiables, pudiendo conformar soluciones adoptables por cualquier organismo sin necesidad de mayores recursos específicos. Muchas de estas soluciones han sido conformadas por el ensamblado de componentes de software libre, por lo menos dentro del propio Estado. En toda solución de este tipo es necesario un trabajo de selección, prueba, configuración y ajuste que requiere de cierto conocimiento y experiencia. Es recomendable que las soluciones ya probadas se estandaricen y documenten como productos para lograr su vulgarización y que queden accesibles a cualquier organismo que las pueda aprovechar, aunque no cuente con los recursos necesarios para su elaboración. Los organismos que ya han implementado estas soluciones pueden aportar su conocimiento, requiriendo de un apoyo adicional para la documentación. Probablemente el sector académico pudiera realizar estas actividades de complemento a lo realizado por las áreas operativas.

17. ***Fortalecer y publicar los registros básicos.*** Más allá de la implementación de PII, se puede iniciar un proceso de publicación sistemática de los registros básicos de información. Publicar con criterio los datos resulta una medida adecuada para ir mejorándolos y evitar su desactualización, es necesario tomar en consideración las reglas de seguridad correspondientes e implementar mecanismos de corrección. Los principales problemas que se encuentran al momento de compartir datos son los niveles de calidad, esta situación puede ser atendida con la construcción de Comunidades de Información o de alguna estructura semejante para sistematizar el tratamiento plural de los datos públicos.

18. ***Estandarizar y mantener el MIO.*** La elección de una especificación como estándar es compleja. Existen ciertos estándares que son incuestionables,

de hecho están aceptados y su formalización es un reconocimiento a lo ya establecido. Pero otros estándares, deben ser cuidadosamente seleccionados y se deberá asumir su continua actualización. Por ello, se debe establecer una clara política de selección de estándares que permita articular y prever los efectos de corto y mediano plazo que puede acarrear su aceptación. Lograr que un colectivo elabore coordinadamente productos que puedan ser reutilizados sistemáticamente por otros, se puede lograr gracias al cumplimiento de estándares pluralmente aceptados. Se debe mantener actualizado el MIO, para que sea adecuado a los organismos más o menos avanzados. Si el MIO no puede ser mantenido al ritmo necesario, tarde o temprano comenzarán a surgir soluciones por fuera de su alcance.

Además de lo planteado referente a estándares, es preciso tener en cuenta su ciclo de vida desde su uso incipiente hasta su aceptación y posterior abandono. Se deben adoptar estándares maduros y bien probados. Esta decisión no siempre es fácil y debe administrarse la tensión entre afrontar la apropiación de novedosas y prometedoras tecnologías contra las conocidas pero ya maduras.

Es útil comprender el contexto donde se desarrolla un proceso de formulación de estándares, comprender el impacto de su adopción o rechazo, así como los beneficios y riesgos asociados, es fundamental para una adecuada elección.

La adopción de especificaciones como estándares es esencial para el desarrollo de la IO pero, consecuentemente, la adopción de éstos puede tener efectos secundarios no deseables. Existe una serie de pautas para la adecuada elección de especificaciones:

- Priorizar la utilización de software libre y estándares abiertos.
- Asegurar que la especificación candidata esté sustentada por un conjunto representativo de comunidades.
- Asegurar que existen diferentes implementaciones y que son compatibles entre sí.
- Asegurar que la especificación y los instrumentos asociados son vulgarizables en el alcance pretendido.
- Prever un tiempo de vida aceptable para el fin pretendido.
- Asegurar que la especificación efectivamente agrega valor.

La utilización de software libre y estándares abiertos es un medio funcional al cumplimiento de varios de los principios de la IO. Tomando como referencia a la Comisión Europea los estándares abiertos cumplen con las siguientes condiciones:

- El estándar es adoptado y será mantenido por una organización sin fines de lucro y su futuro desarrollo se producirá sobre la base de un proceso de decisión abierto a todas las partes interesadas -consenso o decisión mayoritaria, etc.-.
- El estándar ha sido publicado y su documento de especificación se encuentra disponible libremente o con un costo simbólico. Debe estar permitido a todos copiarlo, distribuirlo y usarlo en iguales condiciones.
- La propiedad intelectual, la presencia de posibles patentes en el estándar, o en partes de él se hace disponible irrevocablemente sobre la base de la liberación de derechos.

- No hay limitaciones para la reutilización del estándar.

19. ***Promover y difundir.*** La existencia de PII en funcionamiento, aunque sean aislados pero significativos, deben ser dados a conocer para avanzar en su apropiación. Se propone entonces la difusión y promoción de estos casos de éxito con soluciones de IO y con resultados interesantes desde el punto de vista de la gestión del Estado, tanto interna como en su relación directa con el ciudadano. Dicha difusión se podría instrumentar mediante una serie de sesiones donde cada una estuviera organizada por algún organismo que expusiera sus logros. Es recomendable que las exposiciones estén lideradas por las principales autoridades políticas de los organismos involucrados y sustentadas por la primera línea de la función pública. El discurso debe dirigirse a los mandos políticos, superiores y medios de otros organismos con el objetivo de inducir la práctica de actividades colaborativas y del trabajo en conjunto para brindar servicios a la sociedad. La temática debe estar centrada en la visión y políticas aplicadas para resolver la situación, descripción de los casos resueltos, logros obtenidos y problemas superados. También se podría incluir una descripción de los recursos elaborados para implementar la solución, resaltando su potencial reutilización en otros ámbitos.

Recomendaciones estratégicas

Las recomendaciones a continuación -de tipo estratégico y de largo plazo-, cubren aspectos que deben ser atendidos para que en un futuro pueda asegurarse el uso extendido de la IO y su gobernabilidad. Éstas no son necesarias en una primera instancia, pero dado que requiere desarrollar actividades de largo alcance y enfrentar problemas difíciles, es necesario anticipar su tratamiento. Las recomendaciones no sólo afectan a la IO, sino también al Gob-e en general y a los procesos de mejora y reforma del Estado.

20. ***Elaborar un mapa de la Interoperabilidad.*** La implementación de la IO involucra variadas actividades y personas de diferentes especialidades que desarrollan labores en muchos organismos de diversos tipos. Debemos sumar a esta heterogeneidad el estilo de implementación creciente y el enfoque participativo y plural que impone el modelo. Contar con herramientas de gestión de todas estas entidades e instrumentos de comunicación social en su interrelación es imprescindible para alcanzar niveles moderados o superiores. Se propone establecer un sistema de gestión de recursos - PII, Servicios de Información, datos, servicios de infraestructura, personas, estándares, ámbitos de discusión, eventos de difusión, etc.-, que funcione como un repositorio de memoria colectiva y soporte a la gestión del conocimiento.

21. ***Modelar los datos públicos.*** La gestión de los datos demanda una misión de ordenamiento que sistematice el funcionamiento, conjugue esfuerzos y facilite el consenso entre los actores involucrados en el proceso. Sin el desarrollo coordinado de una estructura de gerencia y actualización continua y transversal se vuelve inútil la promoción del reuso de datos, puesto que se volverán obsoletos al día siguiente de su publicación. La implementación de los esquemas de XML u otros medios de representación de datos requiere de una gestión sólida que coordine las instancias de definición, creación, aprobación, adopción y asistencia técnica especifica, útil para los organismos.

    El modelo de arquitectura de datos en capas se presenta como una manera adecuada de organizar la información. Desde esta perspectiva, las capas son niveles de organización de los elementos de dato. En el interior de una capa se encuentran aquellos elementos de dato que contienen entre sí cierta afinidad respecto al origen, función o uso. Como

ejemplo se presenta un modelo de administración de elementos de dato en capas.

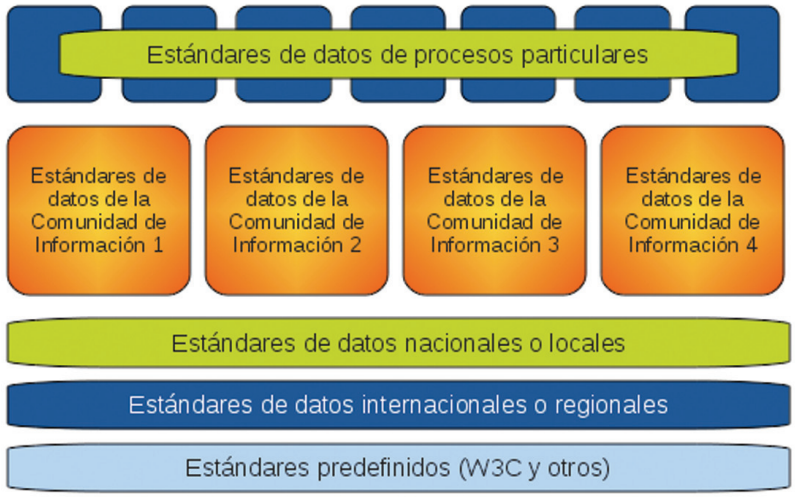
- Estándares predefinidos. Es la base del modelo que contiene los tipos de datos básicos definidos por la W3C[2] y seguramente de algún otro estándar generalizado como Dublin Core[3] por ejemplo.

- Datos internacionales. Corresponde a elementos que están establecidos de forma supranacional. Son considerados necesarios y adecuados para establecer un diálogo con otros países del mundo.

- Datos nacionales o locales. Se caracteriza por contener sólo los elementos de dato que representan conceptos de información característicos y propios del país o ámbito de aplicación del MIO. Son típicos los documentos de identidad de las personas, las identificaciones tributarias, las localidades, etc.

- Datos comunitarios de información. Está delimitada por los sectores que refieren a los elementos que definen intereses en común, afinidades dentro del grupo, e identifican los elementos de dato sobre conceptos de información de uso particular de los macro sectores.

- Datos de PII. Los elementos de dato utilizados provienen en su mayoría de los niveles inferiores en la estructura del modelo de arquitectura, pero únicamente en los casos que los elementos de dato necesarios no existan en los niveles de las capas inferiores.



Arquitectura de datos en capas

[2] www.w3c.org

[3] www.dublincore.org

22. ***Establecer un modelo de seguridad integral.*** La modalidad de Identidad Federada[4], como modernización del *single sign-on*, debe ser definida y aplicada constante y gradualmente. Es prudente que la misma estrategia cubra el acceso a aplicaciones por personas como el acceso a servicios entre componentes informáticos. Estas implementaciones suelen ser costosas en sistemas heredados[5], por lo que se recomienda su aplicación gradual a medida que se realiza la actualización tecnológica.

23. ***Gestionar la evolución.*** La variedad de temas, los múltiples estadios de evolución de cada uno de ellos, más la integración de todo el conjunto, los proyectos sectoriales, la evolución constante de las políticas públicas y la tecnología, conforman un cuadro de difícil administración. Por ende se exhorta a tomar la implementación de la IO como una política pública de largo plazo que permita gestionar los distintos aspectos gradualmente y guiarlos hacia un futuro deseable. El modelo debe ser gestionado y utilizado como guía para la planificación consistente de actividades.

Proyecto a corto plazo

Utilizando las recomendaciones anteriormente descritas, se propone a continuación un proyecto para iniciar la implementación de la IO y las bases para elaborarlo.

Objetivos

Objetivo general

Iniciar la implementación de la Interoperabilidad en Venezuela, a través de la formalización de la versión inicial del Marco de Interoperabilidad y la realización de casos pilotos.

Objetivos específicos

1. Establecer y poner en funcionamiento el Componente de Gobernanza.
2. Publicar el Marco de Interoperabilidad como primer conjunto de estándares para la implementación de la Interoperabilidad en nuestro país.
3. Poner en funcionamiento nuevos Procesos Inter-Institucionales, a través de la Interoperabilidad de dos o más instituciones del Estado.
4. Poner en funcionamiento parcial el Componente de Operación.
5. Realizar la actualización del Marco de Interoperabilidad, con base en la experiencia obtenida en la implementación de los casos pilotos.
6. Difundir la Interoperabilidad mediante estrategias de promoción de los avances obtenidos.

Resultados esperados

Los resultados a producir por el proyecto son:

1. Componente de Gobernanza, funcionando y formalizado, con base en el Modelo Organizativo para la implementación de la Interoperabilidad en

[4] La Identidad Federada -del inglés, Federated Identity Management- es una de las soluciones para abordar la gestión de identidad de usuarios en los sistemas de información entre múltiples organizaciones. Su objetivo es obtener una gestión de usuarios eficiente con sincronización de los datos de identificación y una gestión coordinada de acceso a servicios. Mediante estas soluciones, los individuos pueden emplear la misma identificación personal -típicamente usuario y contraseña- para identificarse en redes de diferentes organizaciones y de este modo acceder a sistemas que comparten información sin compartir tecnologías para autenticación. Para su funcionamiento es necesaria la utilización de estándares que definan mecanismos que permiten a las empresas compartir información entre dominios. El modelo se basa en un círculo de confianza entre los organismos involucrados, por el cual un individuo autenticado en uno de los organismos puede circular por los sistemas y servicios de los otros sin volver a autenticarse.

[5] Un sistema heredado o sistema legacy es un sistema informático -equipos informáticos o aplicaciones- que ha quedado anticuado pero continúa siendo utilizado por el usuario.

Venezuela (MOIO).

2. Marco de Interoperabilidad (MIO) versión 1.0 establecido, formalizado y oficialmente publicado.
3. Casos pilotos seleccionados e implementados, aplicando la metodología definida para tal fin.
4. Componente de Operación, en funcionamiento parcial según el MOIO.
5. MIO actualizado, a partir de la experiencia obtenida en los casos pilotos.
6. Plan de difusión cumplido, a partir de los casos implementados y demás recursos elaborados.

Etapas y actividades

Las actividades han sido agrupadas en etapas. Se definieron dos etapas preparatorias para los resultados uno (1) y dos (2), dos etapas de operación para los resultados tres (3) y cuatro (4), y una etapa de cierre para los resultados cinco (5) y seis (6) respectivamente.

Con respecto a las metas, éstas serían aplicables directamente sólo a los resultados tres (3) y cuatro (4). Dependerá fundamentalmente de los recursos disponibles pero se puede recomendar la selección y la puesta en funcionamiento de cuatro (4) casos pilotos. Estos se podrían seleccionar con diferentes modalidades, por ejemplo:

- Un caso para la elaboración de un nuevo Proceso Inter-Institucionales (PII).
- Un caso de publicación de algún registro básico que se considere altamente reutilizable.
- Un caso que consiste en la estandarización de un PII existente que no cumpla los estándares.
- Un caso de PII que sirva como inicio para avanzar luego en una temática específica.

A continuación se presenta un cuadro con una breve descripción de cada actividad. Es importante relacionarlas con las recomendaciones enunciadas inicialmente.

Descripción de las Etapas y Actividades del Proyecto a Corto Plazo						
Etapa	**Actividad**	**Descripción**	**Recursos Componente de Gobernanza**	**Recursos Componente de Operación**	**Resultados**	**Recomendaciones**
Establecer Componente de Gobernanza	Formalizar modelo organizativo	Establecer formalmente el MOIO.	Si		R1-Componente de Gobernanza funcionando	7
	Definir estructuras organizativas	Elaborar y establecer la normativa necesaria, la asignación de recursos presupuestarios para el funcionamiento de las unidades organizativas y asignaciones parciales requeridos por el MOIO.	Si			
	Seleccionar personal y asignar responsabilidades	Seleccionar al personal necesario para cubrir los roles requeridos por el MOIO en lo referente al Componente de Gobernanza.	Si			
	Disponibilizar recursos	Poner en disponibilidad los recursos humanos y físicos requeridos para el funcionamiento del Componente de Gobernanza.	Si			
Establecer MIO 1.0	Publicar, ajustar y oficializar versión	Establecer formalmente la versión inicial del MIO utilizando el MOIO.	Si		R2-MIO 1.0 establecido	8
Seleccionar casos pilotos	Identificar casos candidatos	Elaborar el primer inventario de casos pilotos a implementar, puede contener: – Procesos candidatos a reformularse. – Servicios de consulta de Entidades de Datos.	Si		R3-Casos pilotos seleccionados	9
	Evaluar casos candidatos	Evaluar los casos incluidos en el inventario según la política acordada.	Si	Si		
	Formalizar casos y elaborar proyectos	Seleccionar los casos, formalizarlos con las partes involucradas y elaborar los proyectos correspondientes.	Si	Si		

Descripción de las Etapas y Actividades del Proyecto a Corto Plazo						
Etapa	**Actividad**	**Descripción**	**Recursos Componente de Gobernanza**	**Recursos Componente de Operación**	**Resultados**	**Recomendaciones**
Implementar casos pilotos	Establecer Componente de Operación (parcial)	Establecer el Componente de Operación que corresponda según los organismos, temáticas y comunidades involucradas en los casos pilotos. Asignar el personal institucional necesario para los proyectos y lo que establezca el MOIO para el Componente de Operación.	Si	Si	R4-Casos pilotos implementa-dos	9, 12
	Asignar recursos	Asignar los recursos humanos y físicos necesarios para el desarrollo de los proyectos.		Si		
	Capacitar al talento humano	Capacitar al talento humano involucrado en el proyecto en los recursos relacionados al MIO.	Si	Si		
	Desarrollar proyectos	Ejecutar los proyectos.		Si		
	Brindar asistencia técnica	Asistir al personal asignado al proyecto para asegurar un correcto desarrollo, según lo propuesto por el MIO.	Si			
	Evaluar proyecto	Evaluar los resultados obtenidos por los proyectos, las lecciones aprendidas y consolidar las modificaciones necesarias a los recursos y al MIO.	Si			
Documentar experiencia	Documentar experiencia	Recopilar en forma sistemática todas las modificaciones necesarias a incluir en el MIO, aprovechar para elaborar instructivos y rescatar recursos reutiliza-bles. Actualizar los inventarios.	Si	Si	R5-MIO actualizado R6-Difusión realizada	10, 14, 15, 16, 17
	Actualizar MIO	Actualizar el MIO y generar una nueva versión.	Si			18
	Elaborar material de difusión	Elaborar el material de difusión sobre los casos y las experiencias.	Si	Si		12, 19

Descripción de las Etapas y Actividades del Proyecto de Corto Plazo

Proyecto a largo plazo

El proyecto a largo plazo tiene como objetivo fundamental, avanzar de forma sistemática en la implementación de la IO, construyendo estándares cada vez más elaborados para cubrir las distintas necesidades y desarrollando todos los elementos necesarios para su real funcionamiento.

La estructura del plan a largo plazo tiene una fase cíclica donde se propone repetir el proceso empleado en la primera fase o plan a corto plazo:

- Selección de casos.
- Implementación de casos.
- Documentación de la experiencia de forma repetitiva anualmente.
- Gestionar los portafolios de procesos,

PII, Servicios de Información, Entidades de Datos, recursos y experiencias, relaciones y capacidades.

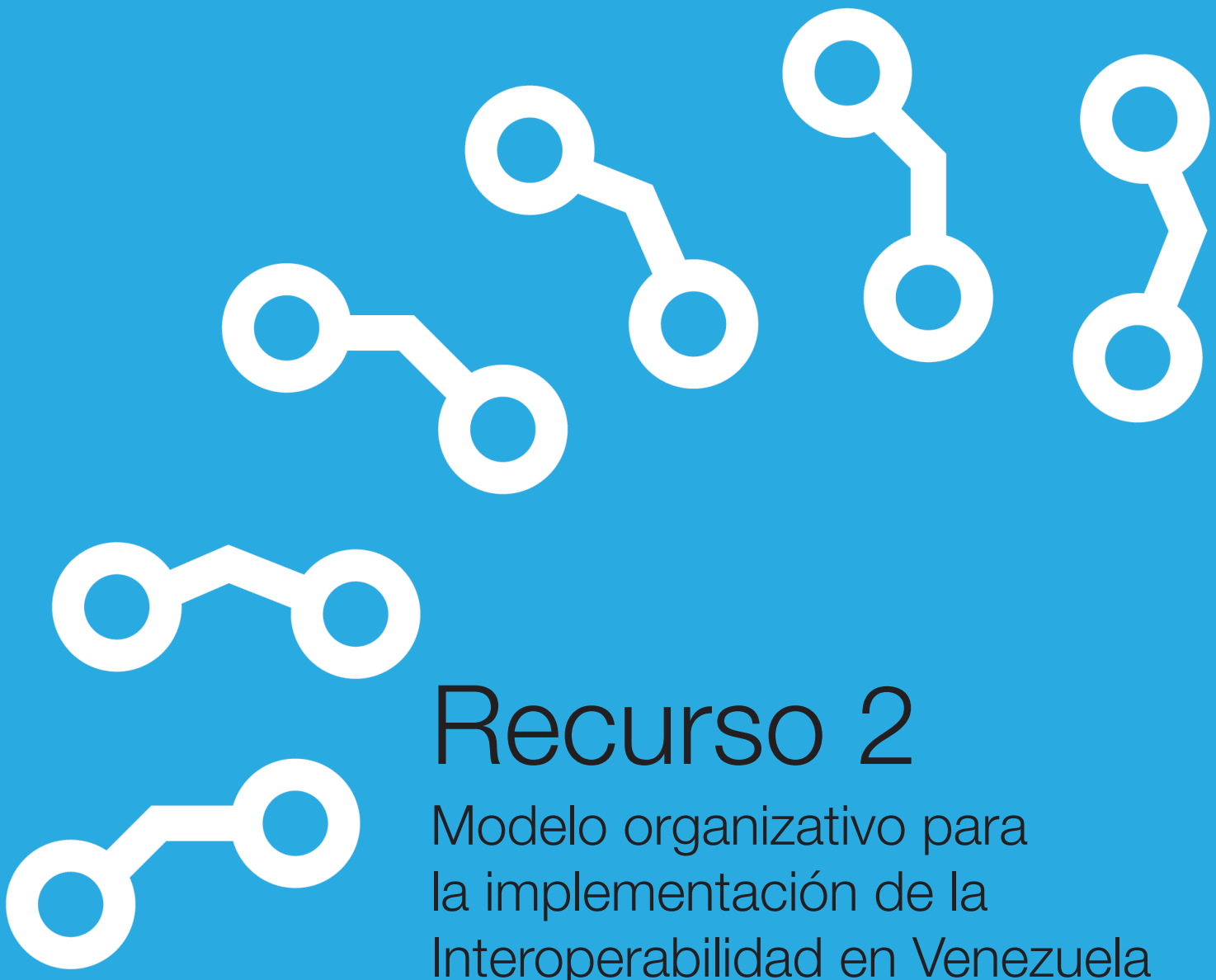
- Formar talento humano.
- Adecuar el marco legal.
- Elaborar modelos.
- Diseñar y proveer infraestructura.
- Reutilizar el software desarrollado.
- Fortalecer y publicar los registros básicos.
- Estandarizar y mantener el MIO.
- Promover y difundir.

Las fases a corto y largo plazo no son independientes, constituyen un círculo de retroalimentación.

Todos estos procesos deben estar acompañados por el fortalecimiento tanto del Componente de Gobernanza como el de Operación, incrementando sus capacidades para desarrollar sus propias funciones, elevando permanentemente el nivel de madurez y su inserción cada vez más profunda en las instituciones.

Los indicadores básicos que pueden guiar el crecimiento de la implementación del plan y fijar las metas para cada período son:

- Cantidad de elementos en los portafolios, para todas las entidades.
- Talento humano formado o inducido, en todos los niveles.
- Modelos construidos y replicados.
- Funcionamiento de la plataforma, cantidad de servicios resueltos, tasa de falla, no repudios, etc.
- Software publicado y reusado.



Recurso 2

Modelo organizativo para la implementación de la Interoperabilidad en Venezuela

Modelo organizativo
para la implementación de la Interoperabilidad en Venezuela

Objetivo

Proponer una base conceptual para establecer un modelo de gestión de la Interoperabilidad en Venezuela, que especifique los principales roles y responsabilidades que permitan poner en marcha un plan sistemático para su implementación.

Componentes principales

El modelo organizativo que se presenta es genérico. No está relacionado explícitamente con ningún área organizativa del Estado. Podrá ser utilizado como instrumento conceptual para establecer el conjunto de responsabilidades a ejercer. La asignación parcial o total de dichas responsabilidades se realizará según las consideraciones de cada organismo.

Se definen dos grandes componentes para la gestión de la Interoperabilidad (IO):

- Componente de Gobernanza.
- Componente de Operación.

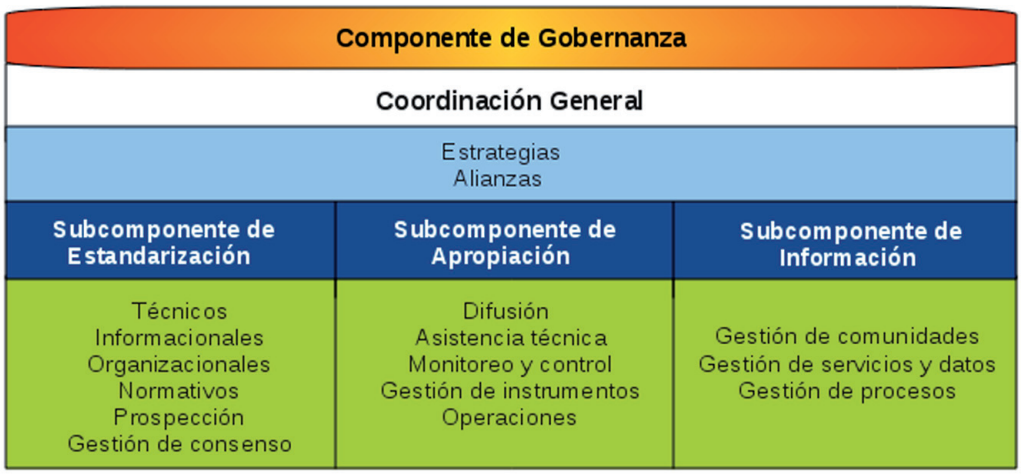
Componente de Gobernanza o Ente Coordinador

Responsable colectivo de la gobernanza[1] e implementación de la IO, incluye las responsabilidades de coordinación general, control y asistencia de los organismos que realicen acciones relacionadas a la IO.

Las funciones y responsabilidades de este componente son variadas y pueden ser asignadas a distintos sectores del Estado. Se propone a continuación una forma de agruparlas para que puedan ser asignadas a áreas de estructura. En caso que algunas de éstas ya estén designadas a algún área existente, se podrán ampliar o ser transferidas a otra nueva.

Los subcomponentes propuestos para el Componente de Gobernanza se muestran en la siguiente imagen:

[1] Se entiende por gobernanza a los acuerdos entre los gobiernos y actores que participan en los procesos de Interoperabilidad y la forma de alcanzarlos. La gobernanza busca que las autoridades cuenten con la institucionalidad necesaria para establecer los estándares de Interoperabilidad, asegurar su adopción y dotar a las instituciones de capacidades organizacionales, informacionales y técnicas necesarias para ponerlos en práctica.



Subcomponentes del Componente de Gobernanza

Coordinación general

El área coordinadora cumplirá con las funciones básicas de toda área de coordinación pública. Será la autoridad intermediaria en los aspectos relacionados con el desarrollo y aplicación del Marco de Interoperabilidad (MIO).

Las principales funciones de la coordinación general son:

- Definir las estrategias para el avance de la IO.
- Coordinar el conjunto de actividades relacionadas a la IO.
- Proveer los recursos tecnológicos, financieros, humanos para el desarrollo de servicios y de infraestructura tecnológica necesarios para la implementación de la IO.
- Coordinar las relaciones políticas necesarias para cumplir con las estrategias establecidas.
- Promover las alianzas con todos los actores involucrados.

La coordinación general esta dividida en varias unidades, según funciones específicas.

Subcomponente de estandarización

Este subcomponente se encarga de la gestión de los estándares que forman parte del MIO. Se subdivide en áreas técnicas específicas según la temática, siendo aconsejables las siguientes:

- Técnicos.
- Informacionales.
- Organizacionales.
- Normativos.
- Prospección.
- Gestión de consenso.

Todos estos grupos deben mantener la coherencia de los estándares en todas las temáticas y a través de las versiones del MIO. Es conveniente que, aunque la producción de los estándares se realice en un contexto acotado, se desarrollen consultas abiertas para su verificación. Para esto se ha incluido un grupo de gestión de consenso, el cual debe coordinar las actividades con la Comunidad Práctica del Componente de Operación.

Análogamente, la gestión del consenso debe considerar los insumos para realizar ajustes y actualizaciones a los estándares de forma amplia, utilizando la misma Comunidad Práctica y otros estamentos posibles.

Sus principales funciones son:

- Mantener, validar, aprobar y actualizar los estándares del MIO.

- Realizar prospección tecnológica para anticipar la actualización del MIO.
- Establecer los estándares para el diseño e implementación de los sistemas de información necesarios para la gestión de Servicios de Información, Entidades de Datos y otros aspectos relevantes, cumpliendo con lo establecido en el MIO.

Subcomponente de apropiación

Desarrolla las actividades necesarias para impulsar, apoyar y mantener la implementación de la IO. Se subdivide en áreas específicas según los tipos de actividades, siendo recomendables las siguientes:

- Difusión.
- Asistencia técnica.
- Monitoreo y control.
- Gestión de instrumentos.
- Operaciones.

Las principales funciones por área son:

Difusión

- Divulgar y promover la reingeniería de los procesos.
- Divulgar y promover la IO en general.
- Divulgar y promover el uso del MIO.
- Divulgar y promover la producción, publicación y consumo de las Entidades de Datos.

Asistencia técnica

- Elaborar y publicar la documentación necesaria para facilitar la efectiva utilización y cumplimiento del MIO.
- Asesorar y asistir a todos los organismos y actores involucrados para el cumplimiento del MIO.
- Implementar los medios necesarios para que los organismos puedan acceder a la asistencia técnica.

Monitoreo y control

- Verificar y asegurar la publicación, actualización y reutilización de las Entidades de Datos.
- Verificar y asegurar el cumplimiento del MIO.
- Verificar el cumplimiento de la reingeniería de procesos.

Gestión de instrumentos

- Gestionar los recursos necesarios para las actividades relacionadas con la administración y ejecución de la IO.
- Diseñar e implementar los sistemas de información necesarios para la implementación de la IO.

Operaciones

- Mantener en producción los recursos informáticos necesarios para llevar adelante las actividades relacionadas a la IO.
- Realizar la planificación de capacidad -Capacity planning[2]- para mantener el nivel de operación en términos adecuados a la demanda.

Subcomponente de información

Este subcomponente resume todas las actividades necesarias para gestionar los datos intercambiados. Se subdivide en áreas específicas según los tipos de actividades, siendo apropiadas las siguientes:

- Gestión de Comunidades de Información.
- Gestión de Servicios de Información y Entidades de Datos.
- Gestión de procesos.

[1] Capacity planning es una actividad estratégica que planifica la incorporación y asignación de recursos para enfrentar necesidades actuales y futuras. Es una de las responsabilidades vitales en la administración de infraestructura de tecnologías de información.

Las principales funciones por área son:

Gestión de Comunidades de Información

- Establecer y mantener los procedimientos para el funcionamiento de las Comunidades de Información.
- Crear y mantener un registro de Comunidades de Información.

Gestión de Servicios de Información y Entidades de Datos

- Establecer y mantener los procedimientos para el tratamiento de las Entidades de Datos.
- Mantener un registro de Servicios de Información y Entidades de Datos.

La gestión de los Servicios de Información se debe administrar a través de un sistema de información, que permitirá realizar las funcionalidades necesarias para:

- Describir Servicios de Información, considerando los aspectos relacionados como: identificación del Organismo Proveedor, tipo de servicio, nivel de servicio mínimo o estándar, Entidades de Datos relacionadas, funcionalidades y métodos que incluye, manuales de uso, facilidades de desarrollo y prueba de aplicaciones que lo consuman, soporte técnico, etc.
- Describir y conocer las restricciones para su suscripción y consumo.
- Descubrir los Servicios de Información disponibles en el Estado.
- Realizar suscripción y des-suscripción a Servicios de Información.
- Acceder a estadísticas de uso.

La administración de las Entidades de Datos debe estar apoyada en un sistema de información que implemente como mínimo:

- La descripción de las Entidades de Datos, considerando todos los aspectos relacionados como: descripción de los datos comprendidos, descripción del ciclo de vida, nivel de calidad y criterios de actualización.
- La explicación de las restricciones para su suscripción y consumo.
- Los acuerdos de nivel de servicio mínimos.
- Otros criterios de validez, seguridad, temporalidad, caducidad y permanencia aplicables.

Gestión de procesos

- Mantener actualizado un mapa detallado de los procesos del Estado, que sirva como base para orientar la definición de proyectos de rediseño de procesos.
- Establecer la política para la selección de los procesos a ser rediseñados.
- Asistir a los organismos en la selección de los procesos a rediseñar.
- Asistir a los organismos en el rediseño de los procesos.

Para la efectiva administración de los procesos del Estado -que proveen servicios a la sociedad- es necesario disponer de un sistema de información -instrumento- que los describa, considerando todos los aspectos relacionados, tales como, identificación del proceso y de las tareas que lo conforman, identificación de los responsables de llevarlo a cabo, especificación de los Servicios de Información utilizados, esquemas de datos, datos y documentos requeridos con manejo de versiones, acceso a estadísticas de demanda, uso y costo.

Componente de Operación

Responsable de la ejecución concreta de las acciones operativas que se realicen para la implementación de la IO. El componente presenta cuatro roles centrales:

- Organismo Proveedor de información.
- Organismo Solicitante de información.
- Comunidades de Información.
- Comunidad Práctica.

Organismo Proveedor de información

El Organismo Proveedor es aquel que proporciona los datos a intercambiar desde sus sistemas de información.

Sus funciones principales son:

- Establecer en la estructura del organismo, los puestos de trabajo con los roles que respondan a las competencias requeridas y asignar el personal idóneo en ellos.
- Poner a disposición los Servicios de Información que produzca y que sean de utilidad para algún otro organismo.
- Publicar en el registro de Servicios de Información y en el registro de Entidades de Datos, las descripciones de servicios, entidades y elementos de datos que se ponga a disposición.
- Exponer y procurar el cumplimiento de los criterios del nivel de validez, seguridad, temporalidad, caducidad y permanencia de los datos puestos a disposición.
- Definir, implementar y publicar los procedimientos a través de los cuales se recuperan y actualizan los datos que se pongan a disposición.
- Publicar el acuerdo de nivel de servicio con el que ponen a disposición los datos administrados.
- Procurar que las Entidades de Datos publicadas sean consistentes con los estándares definidos a nivel general y con las demás Entidades de Datos publicadas.
- Asegurar dentro de su ámbito de competencia el cumplimiento de las medidas de calidad y seguridad establecidas para cada Servicio de Información y Entidad de Datos publicada.
- Atender las observaciones efectuadas por las Comunidades de Información y Organismos Solicitantes sobre la validez, actualización y seguridad de los datos administrados.
- Acordar con los Organismos Solicitantes de información y Comunidades de Información a la que pertenece, las modificaciones previstas relativas a los servicios que proveen.
- Atender, dentro de sus posibilidades de recursos, los requerimientos institucionales de datos que realicen otros organismos.
- Procurar que los componentes informáticos involucrados en la prestación de los servicios se encuentren en condiciones óptimas.
- Asegurar que se cumplan las mejores prácticas en materia de administración de bases de datos, de tal forma que los procedimientos de persistencia, almacenamiento y acceso a los datos hagan uso óptimo de los recursos informáticos que le son asignados.
- Aplicar las políticas y prácticas de seguridad de la información vigentes para el acceso a las Entidades de Datos puestas a disposición.
- Cuando las medidas de seguridad lo requieran, acreditar, identificar, autenticar y autorizar a los Organismos Solicitantes de información para el acceso a los servicios que proveen.

- Difundir y hacer cumplir dentro del organismo el MIO y demás prácticas e instrumentos relacionados.

Organismo Solicitante de información

El Organismo Solicitante de información es aquel que demanda el Servicio de Información al Organismo Proveedor.

Sus funciones principales son:

- Establecer en la estructura del organismo, los puestos de trabajo con los roles que respondan a las competencias requeridas y asignar el personal.
- Asegurar la pertinencia del consumo de los Servicios de Información y de la utilización de los datos asociados.
- Asegurar el cumplimiento de las medidas de seguridad establecidas en los acuerdos de nivel de servicios, Comunidades de Información u otra legislación aplicable.
- Cuando las medidas de seguridad lo requieran, acreditar, identificar, autenticar y autorizar a los usuarios de los sistemas de información que consuman los servicios provistos por otros organismos.
- Establecer contratos de confidencialidad para el tratamiento de datos con los usuarios de los sistemas de información que consuman los servicios provistos por otros organismos.
- Asegurar dentro de su entorno el cumplimiento de las medidas de calidad y seguridad establecidas para el tratamiento de la información obtenida a través de servicios provistos por terceros.
- Documentar e informar las deficiencias de los datos obtenidos de un Organismo Proveedor de información, con el fin de mejorar su calidad.
- Implementar mecanismos de mitigación ante deficiencias de los datos obtenidos de un Organismo Proveedor de información.
- Proponer mejoras a los servicios provistos por los Organismos Proveedores de información.
- Participar en las actividades de las Comunidades de Información en las temáticas relacionadas a sus funciones específicas.
- Difundir y hacer cumplir dentro de la institución el MIO y recursos relacionados.

Comunidades de Información

Las Comunidades de Información están conformadas por un conjunto de organismos que tienen injerencia sobre las mismas Entidades de Datos. Un organismo puede formar parte de más de una Comunidad de Información, pero cada Entidad de Datos será responsabilidad de una sola Comunidad de Información.

Las funciones principales de las Comunidades de Información -o del conjunto de organismos que la conforman- son:

- Conformarse ante el Componente de Gobernanza y vincularse con las demás Comunidades de Información.
- Identificar, describir, registrar y publicar las Entidades de Datos que producirá la Comunidad de Información.
- Determinar el Organismo Proveedor de información para cada Entidad de Datos.
- Cooperar con el Organismo Proveedor de información para mejorar la calidad de los datos que administre y publique.
- Asegurar dentro de la Comunidad de Información la no redundancia de los datos disponibles.
- Establecer los criterios de nivel de

validez de los datos producidos dentro de la Comunidad.

- Establecer los criterios de seguridad de los datos producidos dentro de la comunidad.
- Establecer los criterios de nivel de temporalidad, caducidad y permanencia de los datos producidos dentro de la comunidad.
- Establecer los estándares específicos necesarios para el funcionamiento de la comunidad de acuerdo a los criterios establecidos por el MIO.

Comunidad Práctica

La Comunidad Práctica representa un colectivo de personas interesadas y conocedoras de las temáticas referidas a la aplicación y difusión del MIO, que se ordenan bajo un estatuto de funcionamiento para servir como ámbito de consulta no vinculante al Componente de Gobernanza. Será conformada por técnicos de diferentes áreas y niveles de la Administración Pública (AP), universidades nacionales y la industria, convocados por el Componente de Gobernanza con el objetivo de promover el trabajo horizontal y participativo.

Sus funciones principales son:

- Probar, evaluar y gestionar las solicitudes que le presente el Componente de Gobernanza sobre temas que se estén analizando para ser incorporados al MIO.
- Fomentar a través de la generación de herramientas virtuales el desarrollo de espacios de intercambio de experiencias y colaboración de carácter permanente.
- Organizar procesos de planificación y gestión de conocimientos, en apoyo a los demás actores involucrados en la IO.
- Desarrollar espacios presenciales y virtuales de gestión del conocimiento convocando a actores de la AP, la academia y otros sectores, a efectos de ampliar el acervo técnico del Estado en general.
- Identificar y registrar fuentes de conocimiento, experiencias y personal técnico ligado a éstas, que configuren el capital de conocimiento y la memoria institucional de la AP en materia de IO.

Roles institucionales

Todos Organismo Solicitante o Proveedor de información debe definir y establecer los roles que se describen a continuación y asignar personal capacitado para cumplir con las funciones establecidas.

Coordinador institucional de la Interoperabilidad del Estado

Funciones:

- Coordinar la relación de su institución con el Componente de Gobernanza, las Comunidades de Información y los demás Organismos Solicitantes o Proveedores de Información.
- Promover en su institución la publicación de Servicios de Información y Entidades de Datos.
- Promover en su institución la solicitud de Servicios de Información y Entidades de Datos a los Organismos Proveedores responsables.
- Atender y coordinar la resolución de los requerimientos de Servicios de Información solicitados a su institución.
- Difundir los servicios de información que posea su institución.
- Identificar y dar prioridad a los requerimientos de Servicio de Información solicitados.

- Identificar las necesidades de mejoras de los servicios ofrecidos tanto al ciudadano como a otras instituciones del Estado.
- Velar por el cumplimiento de los acuerdos de nivel de servicio establecidos.

Competencias mínimas:

- Comprender los aspectos legales, normativos, organizacionales, informáticos y tecnológicos de los datos públicos.
- Conocer y comprender el MIO y demás recursos relacionados establecidos para la implementación de la IO.
- Conocer los aspectos legales, normativos, informáticos y tecnológicos relacionados a los procesos en los cuales su organismo interviene.
- Conocer sobre los Servicios de Información publicados y las Entidades de Datos gestionados por el Estado y su organismo.

Analista institucional de la Interoperabilidad del Estado

Funciones:

- Asistir al coordinador institucional en la relación del organismo con el Componente de Gobernanza, las Comunidades de Información y los Organismos Solicitantes o Proveedores de información.
- Asistir al coordinador en lo relativo a la producción y consumo de información en el organismo.
- Analizar y resolver los requerimientos de información solicitados a su organismo.
- Analizar y resolver la adecuación de los procesos para implementar Servicios de Información.
- Asistir en la difusión y publicación de los Servicios de Información producidos por el organismo.
- Gestionar el catálogo de servicios del organismo, lo que produce y lo que consume, así como su constante actualización.

Competencias mínimas:

- Comprender los aspectos normativos, organizacionales, informáticos y tecnológicos de los datos públicos.
- Entender la información administrada por la institución.
- Entender la información administrada por las Comunidades de Información a las que pertenece el organismo.
- Entender la información administrada por el sector público.

Recurso 3

Matriz Multi-Criterio

Matriz Multi-Criterio

La matriz multi-criterio es una herramienta utilizada para la toma de decisiones en base a factores cualitativos o múltiples factores no homogéneos que intervienen en un suceso. Los pasos para su aplicación son:

1. Enumerar el conjunto de factores sobre el que se quiere seleccionar o priorizar.

2. Definir los criterios básicos que se deben evaluar para priorizar cada factor.

3. Ponderar los criterios de evaluación. Asignar un valor a cada criterio en función de su importancia: baja, media o alta. Si el criterio tiene un sentido negativo, el signo de su valor de ponderación será negativo.

4. Construir la matriz de puntuación, tal como se muestra a continuación:

Factores	Criterios										Total
	1 Ponderación P		2 Ponderación P		3 Ponderación P		4 Ponderación P		5 Ponderación P		
	V	V * P	V	V * P	V	V * P	V	V * P	V	V * P	
1											
2											
3											

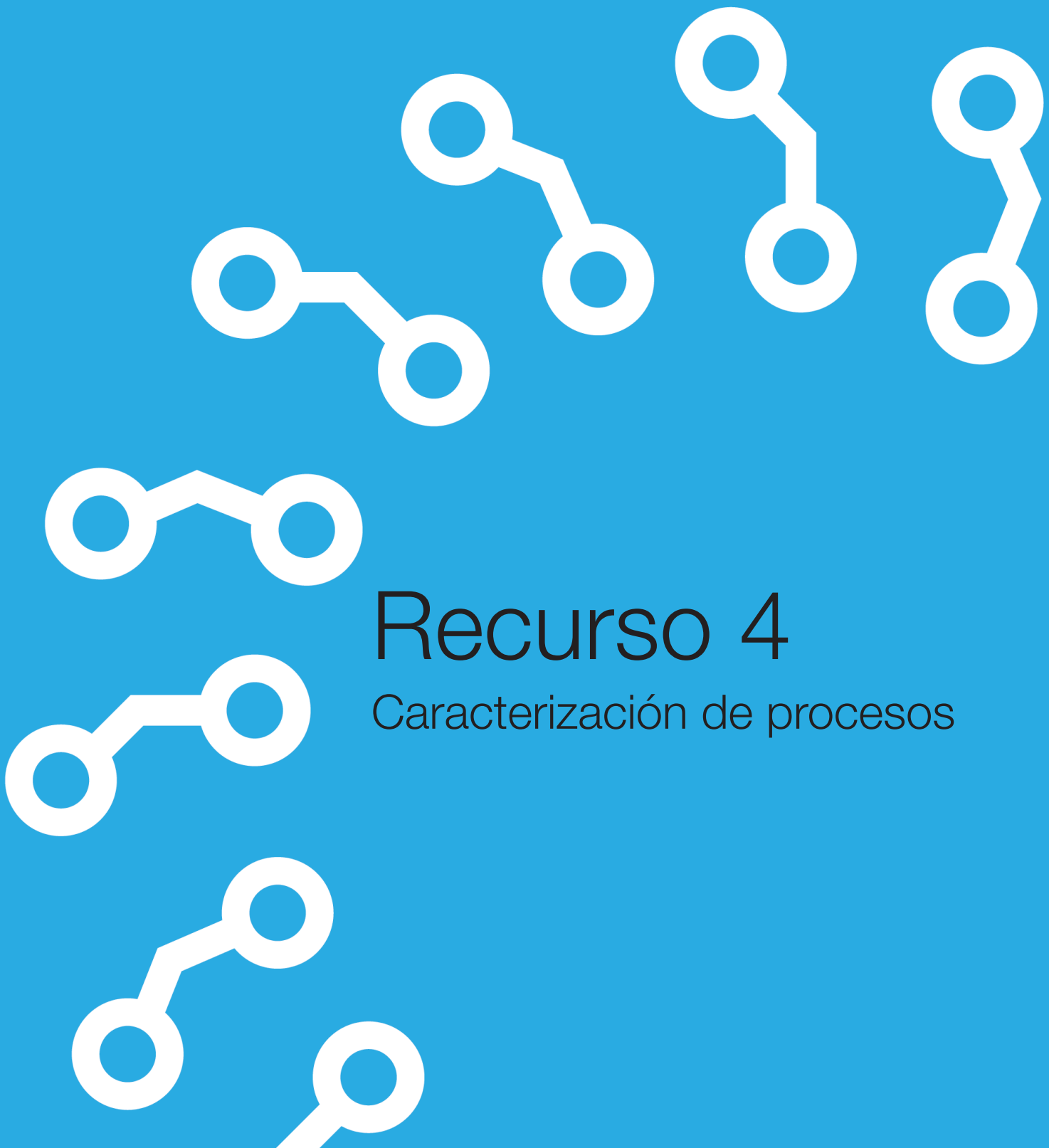
Matriz de puntuación

5. Fijar el criterio de puntuación de cada factor. Se debe definir una escala de valoración para calificar los diferentes factores. La escala debe ser sencilla de 1 a 5, de 1 a 10, entre otros.

A continuación se muestra una tabla ejemplo con datos hipotéticos:

Factores	Automatización P = 2`		Impacto P = 1		Estratégico P = 3		Total
	V	V * P	V	V * P	V	V * P	
1	2	4	3	3	2	6	12
2	3	5	2	2	3	9	17
3	1	2	1	1	1	3	6

Matriz multi-criterio



Recurso 4

Caracterización de procesos

Caracterización de procesos

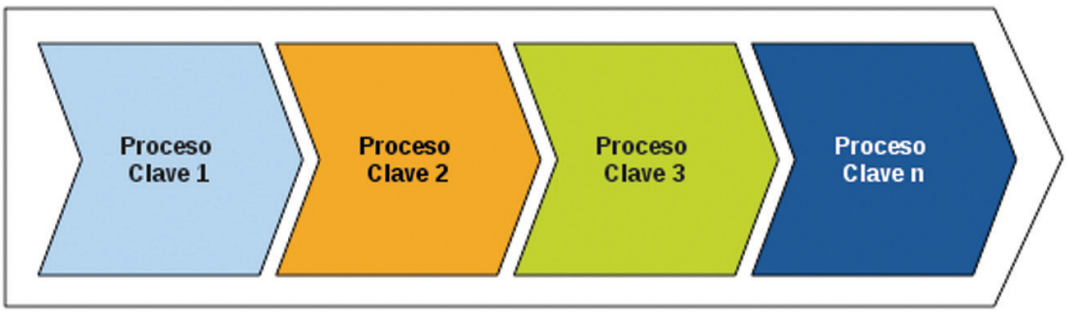
Identificación del proceso

Se debe identificar el proceso interno que responde a las actividades realizadas en el trámite a través de los siguientes pasos:

1. Identifique los procesos claves que constituyen la cadena de valor o tren productivo de la organización a la que usted pertenece.
2. Determine la precedencia de los procesos y colóquelos en orden de consecución.
3. Desarrolle la caracterización de procesos de cada uno de los procesos claves identificados

Procesos claves

La cadena de valor categoriza las actividades que producen valor añadido a la institución en dos tipos: las actividades primarias y las actividades de apoyo o auxiliares. A continuación se puede apreciar una representación gráfica del un proceso utilizando la cadena de valor:



Representación gráfica del proceso mediante la cadena de valor

Caracterización del proceso

El proceso seleccionado es descrito utilizando la plantilla de caracterización de procesos, en donde se describe:

1. Entradas/Insumos
2. Proveedores
3. Actividades
4. Consumidores/Usuarios
5. Salidas/Productos

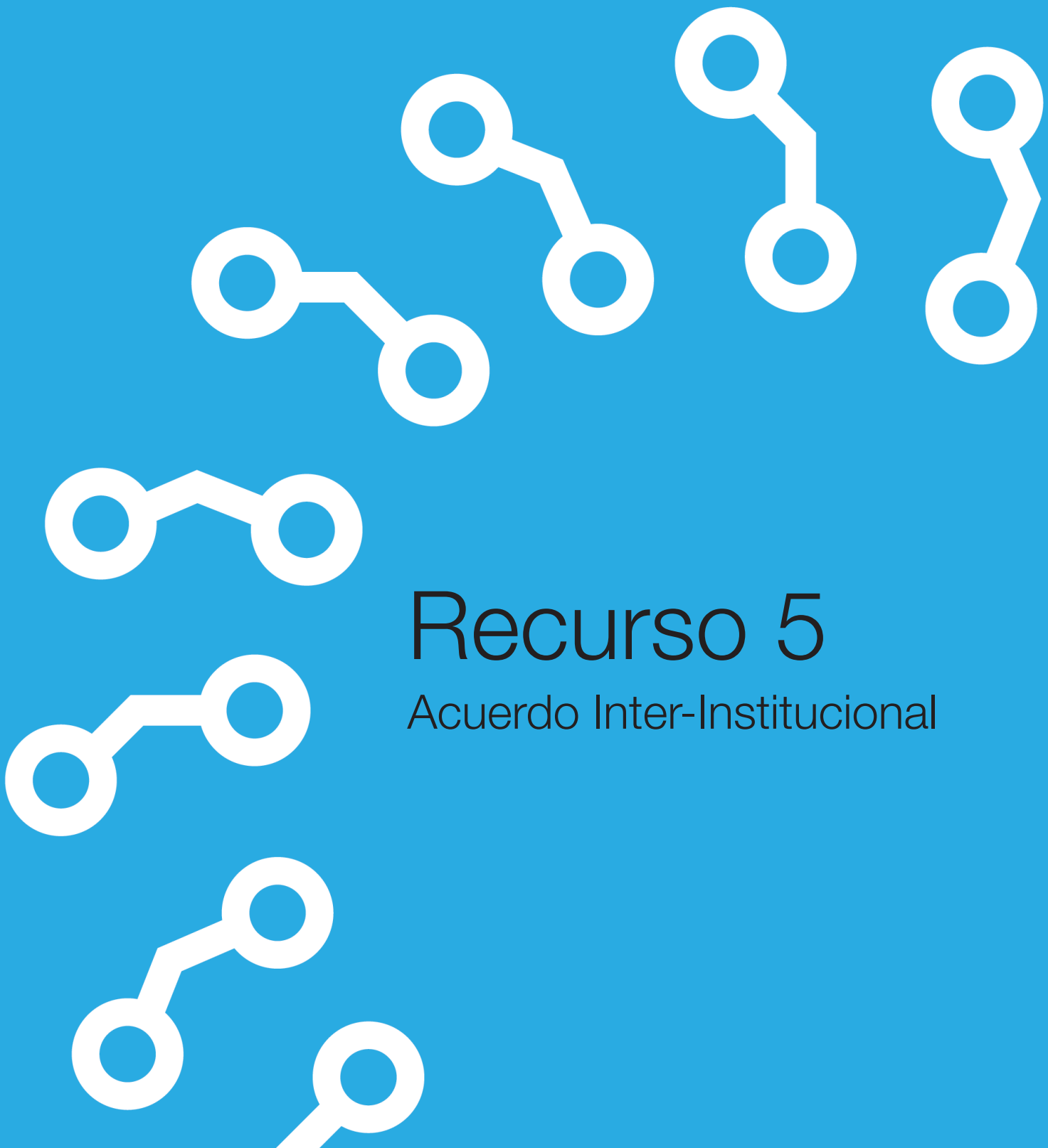
A continuación se muestra una plantilla ejemplo para la caracterización de cada uno de los procesos claves identificados:

Caracterización del procesos:				
Identificación				
Responsable				
Objetivo				
Alcance				
Proveedor(es)	Entrada(s)	Actividades	Salida(s)	Usuario(s)

Plantilla de caracterización de procesos

Recomendaciones generales

- La representación y documentación debe reflejar las entradas, proveedores de información, proceso general, salida y destinatarios.
- Se deben señalar los momentos donde el procedimiento requiere el Servicio de Información y los datos que se esperan intercambiar.
- Para el rediseño, adecuación de los procesos y de la plataforma, se recomienda la formación de mesas de trabajo entre las instituciones involucradas.



Recurso 5

Acuerdo Inter-Institucional

Acuerdo Inter-Institucional

Objetivo

Establecer los términos y condiciones que servirán de base para gestionar el intercambio electrónico de datos mediante la publicación de Servicios de Información entre el Organismo Proveedor y el Organismo Solicitante de la información, a fin de ejecutar de manera eficiente las actividades atribuidas y facilitar el flujo de información al ciudadano.

Descripción de los servicios

Las partes deben acordar como complemento al acuerdo, para cada Servicio de Información incluido, lo siguiente:

- El objeto específico con el cual el servicio es publicado y consumido.
- La descripción detallada de las funcionalidades incluidas.
- Las especificaciones de nivel de servicio.
- La descripción detallada de los datos involucrados, incluyendo: medidas de seguridad requeridas, nivel de actualización y nivel de calidad.

Responsabilidades de las partes

1. Cumplir con lo establecido en el Marco de Interoperabilidad, documentos, políticas, prácticas y demás artefactos relacionados.

2. Realizar el seguimiento y control sobre los aspectos de administración, gestión de riesgo y gestión de incidentes de los Servicios de Información.

3. Garantizar los requisitos de seguridad acordados o particulares de los datos involucrados, con el fin de mantener la disponibilidad, integridad y confidencialidad de los datos intercambiados.

4. Cuando amerite, acordar y proveer los recursos para asegurar el no repudio de las transacciones realizadas.

5. Disponer de mecanismos de contingencia y continuidad según el acuerdo del nivel de servicio establecido, de manera que se obtengan niveles adecuados de calidad de servicio.

6. Llevar un control de los mensajes generados por los Servicios de Información, que pueda ser insumo en la administración y mantenimiento del acuerdo del nivel de servicio establecido.

7. Establecer un procedimiento para gestionar los cambios a los servicios acordados que puedan surgir de su publicación y consumo.

8. Proveer los canales de comunicación adecuados que garanticen los niveles de servicio, calidad y seguridad de los Servicios de Información acordados, adecuados a los fines declarados.

9. Los Servicios Información publicados deben permitir y garantizar el registro confiable de la fecha y hora de ejecución de las transacciones realizadas de acuerdo con la hora oficial venezolana.

10. Permitir obtener reportes, estadísticas e indicadores de gestión del intercambio de datos.

Responsabilidades sobre la calidad de los datos

11. Garantizar que la información intercambiada a través de los Servicios Información sea confiable y que sea utilizada de acuerdo con la legislación vigente.

Responsabilidades sobre la seguridad de los datos

12. Cuando amerite, los servicios publicados deben ser firmados digitalmente con un certificado electrónico, emitido por una entidad legalmente acreditada y debidamente autorizada por la Superintendencia de Certificación Electrónica (Suscerte).

13. Se deben aplicar las medidas de protección adecuadas a las restricciones de seguridad acordadas y requeridas por los datos que se intercambien.

14. De persistir los datos intercambiados en repositorios secundarios o temporales, se les deberá aplicar las medidas de seguridad necesarias para garantizar las mismas restricciones aplicadas a los Servicios de Información.

Disponibilidad de recursos

15. Garantizar la disponibilidad de la tecnología y de los recursos físicos, financieros y humanos necesarios para cumplir con los términos del acuerdo.

Términos de confidencialidad

16. Ambas partes se comprometen a resguardar los datos y la información producto del acuerdo.

Disponibilidad y condiciones generales de los servicios

17. Establecer la disponibilidad de los servicios sujetos a las configuraciones técnicas y de tolerancia a errores establecidas, tales como: tasa del servicio y de contención, horario que se establece para el intercambio de los datos, tipo de intercambio y cualquier otro valor que sea establecido de manera especial entre las instituciones involucradas.

18. Considerar los horarios de monitoreo, así como los canales de comunicación y de información que serán requeridos cuando existan problemas que afecten los servicios, mediante la declarativa de los puntos de contacto y atención ante procesos técnicos y/o administrativos a convenir.

Obligaciones del Organismo Proveedor del servicio

19. Poner a disposición del Organismo Solicitante de la información, los datos contenidos en sus sistemas informáticos y los procedimientos a través de los cuales éstos serán recuperados y o actualizados.

20. Implementar mejoras a los Servicios de Información donde se haya detectado problemas o deficiencias encontradas por el Organismo Solicitante de la información.

21. Contar con mecanismos de respaldo, integridad y seguridad de los datos suministrados.

Obligaciones del Organismo Solicitante de información

22. Comprometerse a no dar a los datos suministrados por el Organismo Proveedor, un destino distinto al originalmente convenido y que es el definido en el “Objeto del acuerdo”.

23. Cumplir con las restricciones de seguridad acordadas con el Organismo Proveedor sobre los datos publicados.

24. Realizar las adecuaciones para incorporar el intercambio de los datos en los trámites administrativos o procedimientos establecidos.

25. Informar los problemas o deficiencias encontradas en los Servicios de Información y datos asociados a los que está accediendo por los Servicios de Información publicados por el Organismo Proveedor.

Duración del acuerdo

26. La duración será establecida entre las partes y de acuerdo al tipo del Servicio de Información provisto.

Recurso 6

Descripción de servicio

Descripción de servicio

Código del servicio	<Identificador del servicio>
Nombre del servicio	<Nombre del servicio>
Versión	<Última versión del servicio>
Funcionalidades del servicio	
1.	<Nombre de la funcionalidad>
2.	<Nombre de la funcionalidad>

Introducción

Este documento detalla la información mínima que debe ser registrada para facilitar a las diferentes instituciones de la Administración Pública (AP) la búsqueda de los diferentes Servicios de Información provistos por el Estado, ya sean implementados a través de Web Semántica o Servicios Web. La descripción realizada se limita a dar una reseña de los requerimientos funcionales y no funcionales. Información suficiente para que cualquiera pueda hacer uso del servicio prestado.

Objetivo

Dar detalles sobre la funcionalidad que presta un servicio específico, incluyendo los requerimientos técnicos relacionados; sus entradas y salidas, flujos y recursos requeridos.

Generalidades del intercambio de información

Se contemplan los aspectos esenciales de un servicio, su objetivo y especificación.

Propósito y descripción

<Detalle el propósito y descripción del intercambio de información>

Especificaciones del intercambio de Información

Tipo de Arquitectura				
Servicio Web				
Protocolo de Comunicación		SOAP		
Especificaciones según SOAP				
Nombre y ubicación del archivo Request				
Nombre y ubicación del archivo Response				
Nombre y ubicación del archivo Fault				
Nombre y ubicación del archivo WSDL				
Endpoint del servicio				
URLs Desarrollo				
URLs Testing				
URLs Producción				
Web Semántica/ Web 2.0				
Protocolo de comunicación		XML		JSON
		HTML		RDF
		Servicio Web		
Fuentes de dato		Formato libre		
		OWL		

Tabla 1 - Arquitectura

Tipo de Intercambio		
En línea	Síncrono	
	Asíncrono	
Fuera de línea	En lote	

Tabla 2 - Tipo de Intercambio

Codigos de error	
Código error	Descripción

Tabla 3 - Codigos de Error

Medio de confirmación	
Timeout	
Cantidad de reintentos	
Métodos de contingencia	
Control de unicidad	

Tabla 4 - Medios de Confirmación

Especificación del *ticket*	
Estructura	
Contenido	
Vigencia	
Autenticidad	

Tabla 5 - Especificación del ticket

Integridad del mensaje	
Confirmación	
Digesto	
Autenticidad	

Tabla 6 - Integridad del mensaje

Otras							
Forma de acceso		VPN		Internet		Frame Relay	
		Otros					
Dirigido a:		Ciudadano		Gobierno		Privado	

Tabla 7 - Otros

Requerimientos funcionales

En esta sección se describen las operaciones funcionales del Servicio Web. Estas operaciones son:

<Nombre de la funcionalidad 1>

<Nombre de la funcionalidad 2 >

También se definen las operaciones asociadas al servicio en cuanto a pre-condiciones, terminaciones y post-condiciones resultantes; entradas y salidas, operaciones e interacciones que deben ocurrir para que se cumpla el objetivo, así como la definición del contexto dentro del cual tienen sentido las funcionalidades definidas.

Descripción de la funcionalidad

Las siguientes secciones explican las funcionalidades realizadas por el presente servicio. A continuación se describe a nivel técnico la operación en cuanto a entradas, salidas, pre-condiciones, post-condiciones, además de otros aspectos:

<Nombre de la funcionalidad 1>

En la siguiente tabla se describe a detalle la funcionalidad 1:

Descripción					
Pre-condiciones					
Datos de entrada (mensaje de Requerimiento)					
Atributo	Descripción	Formato	Tipo	Logitud	
Salida (mensaje de Respuesta)					
Atributo	Descripción	Formato	Tipo	Longitud	Fecha de Actualización
Nivel de Calidad			Fuente	Calidad de captura	
			Sistemas	Servicios	
Flujo normal					
Flujo alterno					
Estados resultantes					
Post-condiciones					
Clientes del servicio					
Relación con otros servicios			Si aplica: indique el código del servicio, nombre de la operación involucrada y detalle el por qué requiere de la interacción con ese servicio.		

Tabla 8 - Descripción de la funcionalidad <Nombre de la funcionalidad 1>

<Nombre de la funcionalidad 2>

En la siguiente tabla se describe a detalle la funcionalidad 2:

Descripción				
Pre-condiciones				
Datos de entrada (mensaje de Requerimiento)				
Atributo	**Descripción**	**Formato**	**Tipo**	**Logitud**
Salida (mensaje de Respuesta)				
Atributo	**Descripción**	**Formato**	**Tipo**	**Longitud**	**Fecha de Actualización**

Nivel de Calidad	**Fuente**	**Calidad de captura**
	Sistemas	**Servicios**
Flujo normal		
Flujo alterno		
Estados resultantes		
Post-condiciones		
Clientes del servicio		
Relación con otros servicios	Si aplica: indique el código del servicio, nombre de la operación involucrada y detalle el por qué requiere de la interacción con ese servicio.	

Tabla 9 - Descripción de la funcionalidad <Nombre de la funcionalidad 2>

Requerimientos no funcionales

1. Esta parte del documento incluye: obligaciones (comportamientos requeridos), prohibiciones (comportamientos no permitidos) y restricciones o límites que aplican sobre las funcionalidades definidas en la parte funcional.

Consideraciones de seguridad

	Seguridad
Plano	
Cifrado	
Observaciones: <Alguna aclaratoria que considere importante resaltar>	

Tabla 10. Seguridad

	Otras consideraciones
Nombre	**Descripción**
Observaciones: <Alguna aclaratoria que considere importante resaltar>	

Tabla 11. Otras consideraciones de seguridad

Contexto

<Enumere las características del entorno donde se consideró la implementación del servicio>

Requerimientos de implementación

<Estos requerimientos pueden indicarse de forma general (para todas las funcionalidades) o por cada una de las funcionalidades definidas>

Requerimiento	Descripción
Desempeño	
Disponibilidad	
Transacción	
Otros	

Tabla 12 - Requerimientos de implementación

Recurso 7

Descripción de Entidades de Datos

Descripción de Entidades de Datos

Pautas sobre los atributos

Los elementos básicos de las Entidades de Datos son los atributos. Los atributos siempre son simples y pertenecen a un tipo que restringe los valores que puede contener. La presente especificación está basada en los tipos de datos ISO/IEC 11179-1. Los datos simples son aquellos que no pueden contener ningún otro elemento o atributo, es decir, representa un elemento básico e indivisible. Los tipos posibles de datos simples son:

- **String:** usado para cadenas de caracteres, típicamente alfanuméricas.
- **Decimal:** para datos numéricos con precisión decimal.
- **Integer:** para datos numéricos enteros.
- **Boolean:** para valores de verdad ("true" o "false").
- **Date:** para fechas.
- **Time:** para valores de tiempo.

Los valores que pueden tomar los datos simples pueden ser restringidos:

- Por rango de valores (Ej. Edad entre 1 <= X < 150)
- Por un conjunto de valores (Ej. Sangre: A, B, AB, O+,O-)
- Por restricción en series de valores (Ej. letra=[a-z])
- Por longitud (Ej. Pwd: Min:4..Max:8)

Los elementos de datos compuestos son aquellos que surgen de la combinación de 2 o más elementos simples y puede contener atributos. Por ejemplo:

Nombre de Persona = 1er Nombre, 2do Nombre, 1er Apellido, 2do Apellido.

Pautas sobre las descripciones de Entidades de Datos

Las descripciones deben:

- Identificar o definir un concepto de importancia relevante para el organismo u organización involucrado en los procesos de intercambio de información implementados a través de servicios.

- Establecer el significado esencial del intercambio, de manera precisa, concisa y no ambigua.

- Contener como mínimo un elemento de dato de tipo identificador y de tipo nombre.

- Garantizar la expresividad y comprensión de la Entidad de Datos, en términos de racionalidad, uso funcional y procedimiento de información.

- Utilizar la misma terminología y estructura lógica para las definiciones relacionadas.

Para el manejo de calidad de datos, para una versión inicial, se debe considerar y detallar como mínimo los siguientes aspectos:

- Fuente origen del dato (por declaración jurada o no del interesado, documento original digitalizado, entre otros). *Clasificación Inherente y Dependiente del sistema*[1].

- Proceso a partir del cual se capturaron o registraron los datos (con o sin capacitación, sin control de validación previo, con control de validación posterior, ingreso automático, entre otros). Clasificación Dependiente del sistema.

- Nivel de seguridad (tipo de operación permitida a aplicar: lectura, lectura/escritura). Clasificación Dependiente del sistema.

- Fecha de actualización y/o verificación asociada al dato. Clasificación Inherente.

- Para la extensibilidad de criterios de calidad de datos, se recomienda el estándar ISO/IEC 25012. De igual forma, la definición de la clasificación asignada a cada dimensión a estudiar referente a calidad de datos, se especifica en el anexo “Descripción general de Calidad de Datos”.

- El modelo de datos que contiene las Entidades de Datos debe estar representado en tercera forma normal (3FN) y utilizar tablas de validaciones y/o codificaciones estándar.

- El modelo de datos debe representar un modelo general e integrado que sea capaz de resolver problemas o conflictos de: nombre (sinónimo/homónimo), tipos de datos (diferenciar entre entidad y elemento de dato), dominio de valores y cardinalidad o restricción de asociación entre Entidades de Datos.

- La codificación de caracteres a usar para entidades y elementos de datos debe ser UTF-8[2].

- Tanto las entidades como elementos de datos deben ser nombrados en forma singular, excepto en aquellos casos donde el concepto en sí mismo sea plural.

- El esquema conceptual definido será público, de libre disponibilidad y persistente, respetando cuando aplique los niveles de confidencialidad definidos y garantizando en todo momento:

  Diseño claro, preciso, simple, coherente, inequívoco y que permita la admisión de cambios/extensibilidad de manera sencilla.

[1] **Inherente:** se refiere al grado en el cual las características de calidad del dato tienen el potencial intrínseco para satisfacer las necesidades implicadas cuando el dato es usado bajo condiciones específicas. **Dependiente del sistema:** se refiere al grado en el cual la calidad del dato es enriquecida y preservada dentro de un sistema de cómputo cuando el dato es usado bajo condiciones específicas.

[2] UTF-8 (8-bit Unicode Transformation Format) es un formato de codificación de caracteres Unicode e ISO 10646.

Representación de estructuras de datos relevantes dentro del contexto o áreas de información definidas.

Completitud en la definición del significado de cada entidad y elemento de dato, especificando además su tipo y la delimitación de los posibles valores válidos que puede tener un elemento de dato.

Representar definiciones cuya representación sea global y de interés común, aplicables al Gobierno Electrónico, para que las mismas sean interpretadas de forma única por los entes del Estado involucrados en el intercambio de información.

- Garantizar el formalismo en la definición de los elementos comunes (lenguaje común – lengua franca), con el fin de presentarle a los distintos entes las definiciones de los elementos comunes, con la documentación detallada que se maneja oficialmente. Con respecto al manejo del versionamiento (versiones del modelo – entidad y elemento de datos, y procesos para mantenerlos) debe ser estricto, con la finalidad de garantizar en la medida de lo posible a las organizaciones que consultan/usan la información a intercambiar, un nivel de confiabilidad aceptable.

- Llevar a cabo la promoción y diseminación de las definiciones. Si las definiciones no se dan a conocer no sirven. Es importante que las mismas estén disponibles para toda aquella organización que tenga interés en adoptarlas y en analizarlas. El desarrollo de actividades (talleres, seminarios, cursos) además del uso de medios masivos de publicación (Internet) permitirán una apropiación de las definiciones en las organizaciones. Este gestionamiento de metadata, taxonomías y tesauros debe estar automatizado.

- Garantizar la confiabilidad de las definiciones. Si bien las definiciones pueden variar con el tiempo, éstas deben ser estables. La calidad tanto de los procesos como en las definiciones mismas, genera la confiabilidad que se requiere.

- Considerar de manera inicial dominios o áreas de información básicos donde se mapeen las distintas Entidades de Datos genéricas identificadas. Esta clasificación permitirá en primera instancia aplicar búsquedas por distintos criterios o dominios más lo relacionado a la aplicación de futuras taxonomías. A cada una de las áreas de información se les puede identificar con un número, como se muestra a continuación:

  1. **Temporal:** agrupación o conjunto de elementos de dato que representen conceptos o aspectos que proveen información que tienen que ver con el manejo del tiempo, por ejemplo: duración, fecha, año, hora, tipo período.

  2. **Ubicación:** agrupación o conjunto de elementos de dato que representen conceptos o aspectos que proveen información que tienen que ver con la localización espacial (espacio ocupado) de objetos (personas, documentos, edificios, etc.), por ejemplo: coordenadas, dirección, piso, lugar, zona postal.

  3. **Identificación:** agrupación o conjunto de elementos de dato que representen conceptos o aspectos que proveen información particular, propia y característica de alguien o algo. Dichos elementos de dato permiten la individualización y/o diferenciación de personas,

objetos, documentos u otros elementos de dato que son relevantes para la organización, por ejemplo: número de cédula de identidad, número acto administrativo, código único de identificación de entidad pública.

4. **Organización:** agrupación o conjunto de elementos de dato que representen conceptos o aspectos que proveen información referente a la institucionalidad de entidades u organizaciones, por ejemplo: código tipo persona jurídica, código tipo sociedad.

5. **Personal:** agrupación o conjunto de elementos de dato que representen conceptos o aspectos que proveen información general referente a personas, pero que de por sí no permiten su individualización, por ejemplo: código sexo, código tipo estado conyugal, código pertenencia étnica.

6. **Documental:** agrupación o conjunto de elementos de dato que representen conceptos o aspectos que proveen información respecto de la gestión (creación, distribución y archivo) de documentos, por ejemplo: código tipo documento, texto documento, número de páginas.

7. **General:** agrupación o conjunto de elementos de dato que representen conceptos de información que complementan el uso o la interpretación de otros elementos de dato, y demás que no estén en las otras áreas, por ejemplo: nombre unidad de medida.

En caso de crear una nueva área, se le asignará un número consecutivo a partir de la última establecida. La información contenida allí no debe ser una especialización de una de las áreas creadas anteriormente; ésta deberá corresponder a un área/concepto diferente a las ya definidas.

Se recomienda identificar Entidades de Datos orientadas no solo a su uso genérico y común entre los entes de la Administración Pública involucrados en el intercambio de información, sino que las mismas se definan en función del camino futuro o evolución natural del Marco de Interoperabilidad (MIO).

Pautas sobre la metadata

La metadata utilizada para la descripción de Entidades de Datos debe:

1. Ser fácil de crear y de mantener.
2. Describir la forma, el contenido y la localización de la información.
3. Permitir la construcción de múltiples índices
4. Permitir trabajar con los sistemas de indexación que existen.
5. Permitir su ampliación según las necesidades.
6. Utilizar una semántica que pueda entenderse comúnmente.
7. Poder crearse de forma automática.

Metadatos para la descripción de Entidades de Datos

La propuesta del estándar para metadatos se describe a continuación[3]:

[3] El estándar propuesto está basado en Dublín Core Metadata Standard (ISO 15836:2003). La estructura original fue extendida incorporando metadatos que se consideran estratégicos para la definición del Marco de Interoperabilidad del Estado Venezolano.

Elementos básicos que conforman un metadato	Obligatorios (si y solo si son aplicables)	Recomendados
Nombre		
Fecha		
Asunto		
Creador		
Formato	Accesibilidad	
Valores Permitidos	Audiencia	Lenguaje/Idioma
Identificador	Relación	Contribuidor
Estado	Fuente	Locación
Tipo		
Versión		
Descripciónv		
Alias/Sinónimos		
Validación		

Identificación de metadatos

Cada elemento se describirá utilizando los siguientes atributos:

1. Elemento: nombre del elemento.
2. Definición: descripción del elemento.
3. Nivel de obligación: valor de obligación del elemento (ver tabla anterior).
4. Propósito: uso por el cual el elemento ha sido definido.

Elemento	Definición	Nivel de Obligación	Propósito
Nombre	Nombre asignado (conjunto de caracteres) que debe identificar concreta y coherentemente al elemento de dato.	Obligatorio	Ejecución de búsquedas por medio de un nombre descriptivo, que le permite al usuario su entendimiento, recuerdo y asociación con el concepto que identifica ese elemento de dato.

Elemento	Definición	Nivel de Obligación	Propósito
Fecha	Fecha asociada con un evento en el ciclo de vida del elemento de dato.	Obligatorio	Entregar información de un período exacto, relacionado al contexto dentro de cual se define el elemento de dato. El formato debe respetar el estándar ISO 8601[4], alineado al calendario gregoriano, expresando la hora diaria en 24 horas y usando siempre caracteres numéricos. La fecha y la hora están organizados de más a menos significativos (año, mes, día, hora, minuto, segundo): YYYY-MM-DD (ejemplo 2007-11-03) hh:mm:ss (ejemplo 13:18:05).
Asunto	Se refiere al tópico del contenido o contexto dentro del cual se enmarca el elemento de dato.	Obligatorio	Disponer de la información (narrativa) del tópico
Creador	Ente/Organismo responsable de la creación del elemento de dato. Razón social/Nombre de la(s) organización(es) originaria(s) de la creación o definición del elemento de dato.	Obligatorio	Permitir al usuario conocer la organización y/o persona que elaboró, conceptualizó, definió y/o creó el elemento de dato.

[4] ISO 8601 "Data elements and interchange formats — Information interchange — Representation of dates and times" (en español, "Elementos de datos y formatos intercambiables — Intercambio de información — Representación de fechas y horas") especifica la notación estándar utilizada para representar instantes, intervalos e intervalos recurrentes de tiempo evitando ambigüedades. Esta notación facilita la migración entre distintas plataformas.

Elemento	Definición	Nivel de Obligación	Propósito
Formato	Representación física o digital. Descripción de la forma o restricciones de representación y contenido.	Obligatorio	Mostrar el contenido (representación válida) específico del elemento de dato. A continuación se presenta una tabla base para la definición de formato: ☒ Tipo de dato ☒ Longitud mínima ☒ Longitud máxima ☒ Nro. máximo de decimales ☒ Valor Mínimo permitido ☒ Valor Máximo permitido
Valores Permitidos	Identificación de los valores que puede asumir o tener un elemento de dato, en un dominio y rango respectivo.	Obligatorio	Permitir al usuario conocer los valores permitidos/válidos que puede tomar un elemento de dato, en base al dominio asociado al mismo.
Identificador	Referencia no ambigua (clave unívoca) que tiene validez dentro de un contexto o dominio determinado. Elemento de dato creado con la finalidad de lograr una identificación única, individualizada o diferenciada.	Obligatorio	Permitir al usuario la búsqueda de conceptos o aspectos asociados a información particular, propia y característica de un algo o alguien, mostrando así la individualización del concepto (información específica).

Elemento	Definición	Nivel de Obligación	Propósito
Estado	Representa el estado actual del elemento de dato.	Obligatorio	Permitir al usuario conocer el estado exacto, en un momento determinado, del elemento de dato. Los posibles estados son: ☒ En Definición: el elemento de dato está conceptualizado a partir de una solicitud de servicio. ☒ En Desarrollo Técnico: se está creando o construyendo el elemento de dato (por ejemplo en esquema XML), y realizando las pruebas funcionales y técnicas necesarias. ☒ Publicado: período en el cual el elemento de dato está publicado en un portal para su uso. ☒ No Vigente: cuando el elemento de dato es obsoleto, y por tanto se debe dejar de utilizar. El estado por defecto es : En Definición.
Tipo	Naturaleza o género contenido o asociado al elemento de dato.	Obligatorio	Entregar información relacionada con el tipo utilizado para la clasificación del elemento de dato, estándar ISO/IEC 11179-1

Elemento	Definición	Nivel de Obligación	Propósito
Versión	Representa el número de versión vigente, el cual se denota por dos (2) números separados por un punto (.), mostrando así el desarrollo/evolución del elemento de dato. El valor por defecto es 1.0.	Obligatorio	Mostrar la evolución/ avances realizados sobre el elemento de dato, tanto de manera narrativa (descripción del cambio que originó el versionamiento) como con su respectivo identificador, partiendo que la versión inicial es 1.0. Cada versión que se considere de tipo menor, se identifica con 1.x, donde x es un dígito que inicia en 1. Cada nueva versión que se catalogue como mayor, se identifica como x.0, donde x es un dígito que inicia en 2.
Descripción	Descripción textual de contenido del elemento de dato.	Obligatorio	Entregar información que le permita al usuario entender de manera concreta y exacta el elemento de dato, a través de su explicación detallada y ordenada. Con esta descripción el usuario podrá determinar si necesita o no el elemento de dato, de acuerdo a sus requerimientos.

Elemento	Definición	Nivel de Obligación	Propósito
Alias/ Sinónimos	Nombre(s) alternativo(s) por el(los) cual(es) se conoce también un elemento de dato. Debe identificar concreta y coherentemente al elemento de dato.	Obligatorio	Ejecución de búsquedas por medio de un nombre descriptivo, que le permita al usuario su entendimiento, recuerdo y asociación con el concepto que identifica ese elemento de dato. Es útil para cuando distintos grupos de usuarios tienen nombres diferentes, en su organización, para el mismo elemento de dato. En el caso que efectivamente no se identifique un alias o sinónimo, el valor por defecto es No Disponible (N/D).
Validación	Reglas que deben ser aplicadas en la construcción o definición del elemento de dato.	Obligatorio	Las validaciones que aquí se registran no se encuentran explícitas en la definición de Formato ni valores permitidos (por ejemplo, la fecha de nacimiento debe ser menor a la fecha de defunción). Estas validaciones deben ser implementadas en los servicios que usen este elemento de dato. En el caso que efectivamente no se identifiquen reglas de validación asociadas al elemento de dato, el valor por defecto es No Disponible (N/D).

Elemento	Definición	Nivel de Obligación	Propósito
Accesibilidad	Indica la disponibilidad y usabilidad del elemento de dato a grupos específicos.	Obligatorio si y solo si es aplicable	Entregar información de los niveles de acceso definidos y por tanto posibles, al elemento de dato. Representar la reutilización de los elementos de datos creados, a través de la especificación del uso del mismo – diferenciación semántica.
Audiencia	Categoría/clasificación de los usuarios para los cuales se le provee el elemento de dato.	Obligatorio si y solo si es aplicable	Entregar al usuario información de referencia indicando el público potencial al cual le interese el elemento de dato definido (potenciales usuarios).
Relación	Referencias a elementos de datos relacionados.	Obligatorio si y solo si es aplicable	Entregar información de los elementos de datos que están relacionados con el elemento de dato en específico (relaciones de dependencia – clave foránea, generalización, especialización).
Locación	Ubicación física del elemento de dato (path).	Recomendado	Permitir la ubicación física exacta del elemento de dato. Ruta que referencia un archivo señalando la localización exacta del mismo.
Lenguaje/ Idioma	Lenguaje del contenido interno del elemento de dato.	Recomendado	Permitir a los usuarios limitar sus búsquedas de acuerdo a un lenguaje específico. Se recomienda revisar este metadato, a medida que se avance en el MIO, para concretar tanto las definiciones, alcance y estándares a aplicar en el mismo.

Elemento	Definición	Nivel de Obligación	Propósito
Contribuidor/ Colaborador	Ente/Organismo responsable de hacer contribuciones al contenido del elemento de dato. Razón social/Nombre(s) de la(s) organización(es) que colabora(n) en la definición del elemento de dato.	Recomendado	Permitir al usuario conocer la organización y/o persona que puso a disposición el elemento de dato. De no identificar colaboradores, colocar el valor N/D: No Disponible. Creador (autor) NO puede aparecer como colaborador y viceversa.

Descripción de metadatos

Criterios de selección para versiones, según menor o mayor grado

Tipo de Versión	Descripción del Tipo
Menor	Adición de entidades o atributos opcionales
	Cambio en los atributos, de obligatorio a opcional
	Cambio en la cardinalidad de [0..1] a [0..*]
	Cambio en la cardinalidad de [1..1] a [1..*]
	Adición de un término a una lista enumerada
Mayor	Cambio en las entidades, de opcional a obligatorio
	Cambio en los atributos, de opcional a obligatorio
	Adición de una entidad obligatoria
	Adición de un atributo obligatorio
	Eliminación de una entidad o atributo opcional
	Eliminación de una entidad o atributo obligatorio
	Cambio en la cardinalidad de [0..*] a [0..1]
	Cambio en la cardinalidad de [1..*] a [1..1]
	Eliminación de un término a una lista enumerada

Criterios de selección para versiones

Para determinado elemento de dato, por ejemplo Fecha, los usos identificados se deben documentar de la siguiente manera:

Información General			
Elemento de Dato	Fecha		
Información de Metadatos			
Metadato	**Valor**		
Identificador	fecha		
Descripción	Elemento de dato que representa un día (fecha) en el calendario Gregoriano tal como lo define el estándar internacional ISO 8601.		
Usos	Nombre	Identificador	Descripción
	Fecha Afiliación	FechaAfiliación	Fecha de afiliación o vinculación.
	Fecha Expedición	FechaExpedición	Fecha de emisión o generación de un documento.
	Fecha Vencimiento	FechaVencimiento	Fecha de caducidad de un concepto, documento o acción.
	Fecha Inicio	FechaInicio	Fecha a partir de la cual se da inicio o se marca el comienzo de un hecho, actividad o acción.

Definición de los usos de un elemento de dato

Recurso 8

Descripción general de calidad de datos

Descripción general de calidad de datos

Una de las estrategias más utilizadas para abordar el estudio de calidad de datos para un contexto en específico, es dividir el concepto de calidad por dimensiones. El conjunto de dimensiones de calidad de datos utilizable en un contexto es conocido como “Modelo de Calidad de Datos”. La calidad de datos es un concepto multidimensional y para medirla es necesario descomponerla en características observables en base a las cuales es posible definirla, identificarla y medirla.

Definiciones previas

El modelo propuesto por el estándar ISO/IEC 25012 categoriza los atributos de calidad de datos en 15 características o dimensiones considerados desde dos puntos de vista:

- **Inherente:** La calidad de datos inherente se refiere al grado en el cual las características de calidad del dato tienen el potencial intrínseco para satisfacer las necesidades implicadas cuando el dato es usado bajo condiciones específicas.
- **Dependiente del sistema:** La calidad de datos dependiente del sistema se refiere al grado en el cual la calidad del dato es enriquecida y preservada dentro de un sistema de cómputo cuando el dato es usado bajo condiciones específicas.

A continuación se describen cada una de las dimensiones de calidad de datos:

Características inherentes:

- **Exactitud/Accuracy:** El grado en el cual el dato asociado al atributo representa el valor correcto/exacto del mismo, asociado a un concepto en un contexto específico de uso.
- **Completitud/Completeness:** El grado al cual el dato asociado con una Entidad de Datos representa todos los valores para todos los atributos esperados e instancias de entidad relacionadas en un contexto específico de uso.
- **Consistencia/Consistency:** El grado en el cual el dato asociado al atributo es libre de contradicción y coherente con otros datos, en un mismo contexto específico de uso.
- **Credibilidad/Credibility:** El grado en el cual el dato asociado al atributo es considerado como válido y creíble por los usuarios en un contexto específico de uso. Debe reflejar la actualización mas reciente, con su respectiva fecha y número de versionamiento.
- **Actualidad/Currentness:** El grado en el cual el dato asociado al atributo representa un período correcto -actualizado- en un contexto específico de uso.

Características inherentes y dependientes del sistema

- **Accesibilidad/Accessibility:** El grado en el cual el dato puede ser accedido en un contexto específico de uso, según autenticación y autorización definidas. Accesibilidad son las condiciones físicas en las que los usuarios pueden obtener los datos: dónde y cómo pedirlos, tiempo de entrega, formatos disponibles, otros.

- **Conformidad/Compliance:** El grado en el cual el dato asociado al atributo se adhiere a normas, estándares, formatos, convenciones o regulaciones vigentes y reglas similares relacionadas con la calidad del dato, en un contexto específico de uso.

- **Confidencialidad-Confidentiality:** El grado en el cual el dato asociado al atributo asegura que éste es sólo accesible e interpretable por usuarios autorizados en un contexto específico de uso.

- **Eficiencia/Efficiency:** El grado en el cual el dato asociado al atributo puede ser procesado y proporciona los niveles esperados de funcionamiento -desempeño- usando las cantidades y los tipos de recursos apropiados en un contexto específico de uso.

- **Precisión/Precision:** El grado en el cual el dato asociado al atributo es exacto, preciso y cierto en un contexto específico de uso.

- **Trazabilidad/Traceability:** El grado en el cual el dato asociado al atributo proporciona información sobre el rastro de auditoría o bitácora de acceso a los datos, y de cualquier cambio hecho a los mismos, en un contexto específico de uso.

- **Entendibilidad/Understandability:** El grado en el cual el dato asociado al atributo mantiene un nivel de entendimiento e interpretación adecuado por parte de los usuarios, y es expresado en lenguajes apropiados, estructuración sintáctica y semántica, símbolos y unidades, en un contexto específico de uso.

Características dependientes del sistema

- **Disponibilidad/Availability:** El grado en el cual el dato asociado al atributo es recuperado por usuarios autorizados y/o aplicaciones en un contexto específico de uso.

- **Portabilidad/Portability:** El grado en el cual el dato asociado al atributo es portable, substituido o movido de un sistema a otro, conservando la calidad existente, en un contexto específico de uso.

- **Recuperabilidad/Recoverability:** El grado en el cual el dato asociado al atributo es mantenido y conservado en un nivel determinado de operaciones y calidad, aún en caso de falla, en un contexto específico de uso.

Características de seguridad de datos

Los servicios habilitados por el Estado deben ser de calidad, por lo que debemos especificar algunas características que permitan apreciar la calidad de la prestación de servicios. Algunos de los elementos que debemos tomar en cuenta son:

- **Integridad:** La información producida es de calidad porque no puede ser modificada por quien no está autorizado.

- **Confidencialidad:** La información solo debe ser legible para los autorizados (autenticación correcta de aquellos que participan en el intercambio), la misma debe llegar a destino con la cantidad con que fue prevista.

- **Disponibilidad:** La información debe estar disponible cuando se la necesita. Una métrica posible para esta característica es el tiempo que el servicio permanece disponible al día. La fiabilidad de un servicio puede medirse con el número de fallos en la prestación del servicio en un período de tiempo determinado, ej: número de fallas por año, número de fallas por mes.

- **Irrefutabilidad:** (No-Rechazo o No Repudio). No se pueda negar la autoría de quien provee dicha información.

- **Demanda:** El servicio acepta peticiones. Según el tipo de llamada que se hace al servicio, anónima o autenticada, o según la IP, o el tipo de servicio prestado, se puede limitar el número de solicitudes por hora del servicio.
- **Recuperación:** El Servicio Web siempre envía respuesta.
- **Rendimiento:** Puede medirse en base al desempeño, entendido como el número de solicitudes atendidas en un período de tiempo determinado, y la latencia o tiempo que toma en prestar un servicio, desde que se realiza la solicitud hasta que llega su respuesta.

La métricas que se establecen para cada uno de estos aspectos a tomar en cuenta en la calidad del servicio, sólo pueden medirse si se monitorean los servicios que ofrece el Estado.

Convenciones para la descripción de la calidad de datos

Con el siguiente cuadro, se extiende la especificación de metadatos para la descripción de Entidades de Datos con nuevos atributos para caracterizar la calidad del dato o entidad.

Elemento	Definición	Nivel de Obligación	Propósito
Fecha_ Actualizacion	Fecha de actualización del dato.	Obligatorio	Con esta fecha se puede inferir la vigencia del dato, así podemos tener una medida para su validez y generar cierta confianza.
Fuente	Referencia a la fuente de donde proviene el dato a nivel institucional y técnico.	Obligatorio	Permitir al usuario encontrar elementos de datos que han sido desarrollados sobre la base de un elemento de dato en específico. Este metadato soporta información de manera normativa, legal, de procedimiento o técnica, de la definición y/o justificación de la existencia (origen) del elemento de dato base, conteniendo referencias o citas bibliográficas de los documentos de donde se extrajo o en los cuales se basó la definición del elemento de dato.

Continúa >>

Elemento	Definición	Nivel de Obligación	Propósito
Fuente	Referencia a la fuente de donde proviene el dato a nivel institucional y técnico.	Obligatorio	Si el elemento de dato es compuesto, igualmente debe especificarse o registrarse las fuentes de los elementos que lo componen (elementos simples). De existir diversas fuentes, se debe establecer quién tomó la decisión sobre la selección de la fuente. Cuando la descripción sea construida (a partir de la experiencia de un experto) se debe indicar la forma mediante la cual se obtuvo la información, el nombre de la persona, ente u organismo en el cual labora, cargo u oficio, ciudad y fecha de obtención. Fuentes y formatos: ☒ Leyes –decretos: Número de la ley/ decreto, año, artículo. Se puede agregar, si aplica: numeral, literal, parágrafo. ☒ Resolución: Número, fecha, parágrafo ☒ Definición aportada por experto: Nombre del experto, cargo, institución, ciudad, fecha de obtención, indicar las fuentes en las cuales se basó

Continúa >>

Elemento	Definición	Nivel de Obligación	Propósito
Fuente	Referencia a la fuente de donde proviene el dato a nivel institucional y técnico	Obligatorio	☒ Referencias o citas bibliográficas: Autor, nombre del libro, fecha de edición, editorial, ciudad de edición, página ☒ Definiciones de Internet (contener dirección URL válida: corresponder a páginas oficiales): Autor, título, dirección URL, fecha de último acceso entre corchetes [aaaa-mm-dd] Si la fuente no está disponible se colocará N/D.
Calidad_ Captura	Nivel de calidad del proceso de captura de los datos.	Obligatorio	Con este nivel se puede tener una medida de la fiabilidad del dato. Se pueden establecer 3 niveles de calidad: Bajo, Medio, Alto. Una Entidad de Datos debe contener estos 3 elementos de forma obligatoria para poder tener una medida de confianza sobre los datos.
Calidad_ Preservación	Nivel de calidad de la preservación del dato.	Obligatorio	Se debe especificar los niveles de seguridad que se aplican en la preservación y administración del dato.

Recurso 9

Especificaciones técnicas

Especificaciones técnicas

Especificaciones técnicas por capas de la arquitectura funcional

CAPA	CLASIFICACIÓN	ESTÁNDAR RECOMENDADO
Aplicación	Consulta	UDDI, LDAP
	Dominio	DNS
Datos	Formatos estándares de representación de los datos	XML RDF JSON XHTML
	Transformación de datos	XSL Transformations (XSLT)
	Definición de los datos para el intercambio	XML Schema WSDL
Comunicación	Servicios Web	SOAP
	Web Semántica	RDF
	Protocolos	HTTP
	Identificadores	URI Web Services Addressing
Transporte	Protocolos de transporte de Internet	UDP, TCP
	Transporte de mensajería electrónica	JMS, SMTP/MIME Utilizar productos de mensajería electrónica que soportan interfaces en conformidad con SMTP/MIME para transferencia de mensajes
	Transporte para la transferencia de archivos e hipertexto	FTP, HTTP

CAPA	CLASIFICACIÓN	ESTÁNDAR RECOMENDADO
Metadatos	Presentación	RDF, XML
	Autenticación e Integridad	WS-I Basic Profile 1.1
	Descubrimiento	WS-MetadataExchange WS-Discovery
Seguridad	Servicios Web	De forma general: Basic Security Profile WS-I Y en lo específico: WS-Security, WS-Policy, WS-Trust Para la autenticación y autorización: SAML, XACML
	Correo Electrónico	S/MIME v3
	Servicios Web	Seguridad en IP:IPSEC, IP ESP Tunel de seguridad: VPN Conexiones seguras: SSL v3.0, TLS v1.0
	Comunicación	HTTPS, SFTP
	Algoritmos de Cifrado	DES, 3DES, DSA,RSA,SHA-1
	Certificados electrónicos acreditados a través de SUSCERTE para los servidores, firma, autenticación y cifrado.	

Especificaciones técnicas por capas de la arquitectura funcional

Para la implementación de las capas de comunicación y transporte, se recomienda que a nivel de seguridad se apliquen las AAA (Autenticación, Autorización y Acceso) y el cifrado considerando:

- Dominio de la data y su criticidad.
- Capacidad de la plataforma tecnológica en cada punto, tomando en consideración la de menor prestación.

También se recomienda el uso de VPN[1] en la capa de transporte.

Fichas descriptivas de los estándares

En el siguiente apartado, se presentan las fichas de todos los estándares definidos y empleados en el documento.

Estándares relacionados a la descripción de Servicios Web

UDDI	
Descripción	Acrónimo de *Universal Description, Discovery and Integration*. Descripción, Descubrimiento e Integración Universal. Es un servicio de directorio en el que las empresas pueden registrar y buscar Servicios Web. UDDI es una estructura independiente de la plataforma para la descripción de los servicios, el descubrimiento de las empresas, y la integración de servicios empresariales a través de Internet.
Referencia	

[1] **VPN:** Virtual Private Network / Red Privada Virtual

WSDL	
Descripción	Acrónimo de *Web Services Description Language*, es un formato XML para describir Servicios Web como un conjunto de variables que operan en mensajes que contienen información ya sea orientada a documentos u orientada a procedimientos. Las operaciones y mensajes se describen de forma abstracta, y luego son unidos a un protocolo de red concreto y formato de mensajes para definir un punto final. WSDL es extensible para permitir la descripción de los puntos finales y sus mensajes, independientemente de los formatos de mensaje o protocolos de red utilizados para comunicarse. WSDL define no sólo el formato y los valores de los datos que fluyen dentro y fuera del servicio, también define los criterios de valoración, las operaciones de soporte, los patrones de intercambio de mensajes (MEP) y todo lo relativo a la descripción operativa de los Servicios Web.
Referencia	http://www.w3.org/standards/techs/wsdl#w3c_all
XML Schemas	
Descripción	Un XML *Schema* es un lenguaje para expresar restricciones sobre los documentos XML. Hay varios lenguajes de esquema diferentes en el uso generalizado, pero los principales son las Definiciones de Tipo Documento (DTDs), Relax NG, Schematron y XSD (XML *Schema Definition*).
Referencia	http://www.w3.org/standards/xml/schema
SOAP v1.2	
Descripción	Acrónimo de *Simple Object Access Protocol*. SOAP Versión 1.2 proporciona la definición de la información basada en XML que puede ser utilizada para el intercambio estructurado entre pares en un entorno descentralizado y distribuido. Un mensaje SOAP es formalmente especificado como un conjunto de información XML que provee una descripción abstracta de su contenido.
Referencia	http://www.w3.org/standards/techs/soap

Estándares relacionados a la seguridad de Servicios Web

Basic Profile Security WS-I	
Descripción	Consiste en un conjunto de especificaciones de Servicios Web no propietarias, junto con las aclaraciones y ampliaciones de esas especificaciones que promuevan la interoperabilidad.
Referencia	http://www.ws-i.org/profiles/basicsecurityprofile-1.0.html
SAML	
Descripción	Acrónimo de *Security Assertion Markup Language*, es un marco basado en XML para la autenticación de usuarios, el derecho y la información de los atributos. SAML permite a las entidades hacer afirmaciones sobre la identidad, atributos y derechos de un sujeto hacia otras entidades.
Referencia	http://saml.xml.org/about-saml
XACML	
Descripción	Acrónimo de *eXtensible Access Control Markup Language*. Es un lenguaje basado en XML para la protección de datos. XACML ha sido desarrollado por la empresa SUN Microsystem y aceptado por el consorcio OASIS como estándar. La implementación de XACML ha sido liberada como software libre y está alojada en SourceForge.
Referencia	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

WS-Security	
Descripción	Es un protocolo de comunicaciones que suministra un medio para aplicar seguridad a los Servicios Web, fue publicado en el 2004 por OASIS-Open. El protocolo contiene especificaciones sobre cómo debe garantizar la integridad y seguridad en mensajería de Servicios Web, a través de la incorporación características de seguridad en el encabezado de un mensaje SOAP, así proporciona seguridad extremo a extremo. El protocolo WS-Security incluye detalles en el uso de SAML y Kerberos, y formatos de certificado tales como X.509.
Referencia	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
WS-Policy	
Descripción	Proporciona un modelo general y la sintaxis correspondiente para describir las políticas de las entidades en un sistema basado en Servicios Web. Esta especificación permite tanto a los programadores como a los clientes de Servicios Web anunciar las políticas relativas a seguridad, calidad de servicio, etc. Define un conjunto básico de construcciones que se pueden utilizar y ampliar por otras especificaciones de Servicios Web para describir una amplia gama de requisitos de servicio y sus capacidades. Forma parte de la familia de especificaciones de tecnologías basadas en Servicios Web del W3C[2] desde el año 2007.
Referencia	http://www.w3.org/TR/ws-policy/

[2] **W3C:** World Wide Web Consortium

Estándares relacionados a la representación de datos

RDF	
Descripción	Acrónimo de *Resource Description Framework*. Marco de Descripción de Recursos. Es un modelo estándar para el intercambio de datos en la Web, tiene características que facilitan la fusión de los datos incluso si los esquemas subyacentes son diferentes, y se apoya específicamente en la evolución de esquemas en el tiempo sin necesidad de realizar cambios en los consumidores de datos.
Referencia	http://www.w3.org/standards/techs/rdf#w3c_all http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/
XML	
Descripción	Acrónimo de *eXtensible Markup Language*. Lenguaje de Marcado Extensible. XML es un formato simple utilizado para el intercambio de información, que contempla un conjunto de reglas que sirven para definir etiquetas semánticas para organizar un documento. Además es un metalenguaje que permite diseñar lenguajes de etiquetas propios.
Referencia	http://www.w3.org/XML/
XACML	
Descripción	JSON es el acrónimo de *JavaScript Object Notation*. Notación de Objetos de JavaScript. Es un formato de texto ligero para el intercambio de datos.
Referencia	http://www.json.org/json-es.html

Estándares relacionados al transporte de mensajes

HTTP	
Descripción	Acrónimo de *Hypertext Transfer Protocol*. Protocolo de Transferencia de Hipertexto. Es un protocolo para sistemas distribuidos, colaborativos e hipermedia. Se trata de un protocolo genérico, sin estado, que puede ser usado para muchas tareas más allá de su uso para hipertexto, como servidores de nombres y sistemas de gestión de objetos distribuidos, a través de la extensión de sus métodos de solicitud, los códigos de error y los encabezados. Está orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Una característica de HTTP es la tipificación y la negociación de la representación de datos, permitiendo a los sistemas ser construidos de manera independiente de los datos que se transfieren.
Referencia	http://www.w3.org/standards/techs/http
FTP	
Descripción	Acrónimo de *File Transfer Protocol*. Es un protocolo para la transferencia de archivos entre sistemas conectados a una red TCP[3], basado en la arquitectura cliente-servidor. Este protocolo permite: promover el intercambio de archivos (programas o datos), fomentar indirecta o implícitamente (a través de programas) el uso de equipos remotos, proteger a los usuarios de las variaciones en los sistemas de almacenamiento de archivos entre anfitriones y transferir datos de forma fiable y eficiente.
Referencia	http://www.w3.org/XML/

[3] **TCP:** Transmission Control Protocol

S/MIME v3	
Descripción	Acrónimo de *Secure/Multipurpose Internet Mail Extensions*. Extensiones de Correo de Internet de Propósitos Múltiples/Seguro. Proporciona un método para enviar y recibir mensajes de correo seguros. Es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME. S/MIME está incluido en las últimas versiones de los clientes de correo electrónico y también ha sido apoyado por otros fabricantes que elaboran productos de mensajería.
Referencia	S/MIME es un estándar propuesto por la IETF[4], se define en los siguientes RFC[5] • RFC 2630 “Sintaxis mensaje cifrado” http://www.ietf.org/rfc/rfc2630.txt • RFC 2631 “Método de clave de Diffie-Hellman Acuerdo” http://www.ietf.org/rfc/rfc2631.txt • RFC 2632 “S/MIME versión 3 - Gestión de certificados” http://www.ietf.org/rfc/rfc2632.txt • RFC 2633 “S/MIME versión 3 - Especificación de mensajes” http://www.ietf.org/rfc/rfc2633.txt http://datatracker.ietf.org/wg/smime/charter/

[4] **IETF:** Internet Engineering Task Force
[5] **RFC:** Request for Comments

Estándares relacionados a la seguridad del transporte de mensajes

IPSEC	
Descripción	Acrónimo de *Internet Protocol Security*. El Protocolo de seguridad IP, desarrolla mecanismos para proteger los protocolos de cliente de la propiedad intelectual. Un protocolo de seguridad en la capa de red se desarrollará para proveer servicios de seguridad criptográfica flexible, que apoyará las combinaciones de autenticación, integridad, control de acceso y confidencialidad. La función del IPSEC es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPSEC también incluye protocolos para el establecimiento de claves de cifrado.
Referencia	http://datatracker.ietf.org/wg/ipsec/charter/
VPN	
Descripción	Acrónimo de *Virtual Private Network*, Red Privada Virtual. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
Referencia	

Estándares relacionados a la seguridad de los mensajes

SSL v3.0	
Descripción	Acrónimo de *Secure Sockets Layer*, Protocolo de Capa de Conexión Segura. Es un protocolo utilizado para la gestión de la seguridad en la transmisión de mensajes en Internet. SSL fue desarrollado por Netscape y su principal objetivo es proporcionar privacidad y confiabilidad entre dos aplicaciones que se comunican, evitando el espionaje, manipulación o falsificación de mensajes. El protocolo SSL se ejecuta por encima de TCP/IP y bajo el nivel superior de protocolos como FTP o HTTP
Referencia	http://wp.netscape.com/eng/ssl3/ http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00
TLS v1.0	
Descripción	Acrónimo de *Transport Layer Security*. Seguridad de la Capa de Transporte. TLS se ha propuesto como el sucesor de SSL. Las diferencias entre TLS 1.0 y SSL v3.0 no son significativas, no obstante, entre ellos no se puede establecer comunicación. El objetivo principal del Protocolo TLS es proporcionar privacidad e integridad de los datos entre dos aplicaciones que se comunican. El IETF ha publicado dos documentos RFC que describen el uso del mecanismo de actualización en HTTP/1.1 para iniciar TLS (RFC 2817) y cómo usar HTTP sobre TLS (RFC 2246).
Referencia	TLS está definido en IETF RFC 2246 “The TLS Protocol Version 1.0” http://www.ietf.org/rfc/rfc2246.txt http://datatracker.ietf.org/wg/tls/charter/

Algoritmos asociados al cifrado

DES	
Descripción	Acrónimo de *Data Encryption Standard*. Estándar de cifrado de datos. Es un método ampliamente utilizado para el cifrado de datos mediante una clave secreta. Existen más de 72 billones de claves de cifrado, para cada mensaje dado, la clave es elegida al azar de entre esta cantidad de llaves. Tanto el remitente como el el receptor deben conocer y utilizar la misma clave privada. DES es compatible con una longitud de clave de 56 bits.
Referencia	• Normas ANSI[6] X3.92 • Normas ANSI X3.106 • FIPS[7] Publication 46-3: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf • FIPS Publication 81: http://csrc.nist.gov/publications/fips/fips81/fips81.htm

3DES	
Descripción	Acrónimo de *Triple Data Encryption Standard*. Estándar de Cifrado de Datos Triple. 3DES es una versión más fuerte de la DES, la comunicación se cifra dos veces para hacer más difícil de roer. Pertenece al “simétrico” de la familia de algoritmos, es decir, dos partes de una comunicación tienen que estar en posesión de la misma clave secreta antes de usar 3DES. 3DES es compatible con una longitud de clave de 168 bits.
Referencia	• 3DES se define por: • FIPS Publication 46-3: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf • Normas ANSI X9.52-1998

[6] **ANSI:** American National Standards Institute
[7] **FIPS:** Federal Information Processing Standard

Algoritmos asociados a la firma digital

DSA	
Descripción	Acrónimo de *Digital Signature Algorithm*. Algoritmo de Firma Digital. La firma digital DSA es un par de los grandes números representados en un equipo como cadenas de dígitos binarios. La firma digital se calcula utilizando un conjunto de reglas y un conjunto de parámetros de tal manera que la identidad del firmante y la integridad de los datos puede ser verificada. DSA proporciona la capacidad de generar y verificar las firmas. Publicado por el Instituto Nacional de Estándares y Tecnología (NIST[8], por sus siglas en inglés) define tamaños de clave de 512-1024 bits.
Referencia	• DSA se define por el NIST en: • FIPS 186-2 de DSS[9] • http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf
RSA	
Descripción	Acrónimo de los apellidos de Ron Rivest, Adi Shamir y Len Adleman, del Instituto Tecnológico de Massachusetts (MIT[10], por sus siglas en inglés). Rivest, Shamir & Adleman. Es un método alternativo para la generación y comprobación de firmas digitales. Se reconoce por el NIST en el DSS como alternativa a la DSA. RSA es un sistema de criptografía de clave pública de propiedad que proporciona tanto el cifrado como la firma digital. Utiliza la clave pública del destinatario para cifrar datos que sólo puede ser descifrado por el receptor utilizando su clave privada. RSA admite longitudes de clave de 512-2048 bits y recomienda claves de 768 bits para los datos menos valiosos, claves de 1024 bits para uso de empresas y llaves de 2048 bits para datos de gran valor.

[8] **NIST:** National Institute of Standards and Technology
[9] **DSS:** Digital Signature Standard
[10] **MIT:** Massachusetts Institute of Technology

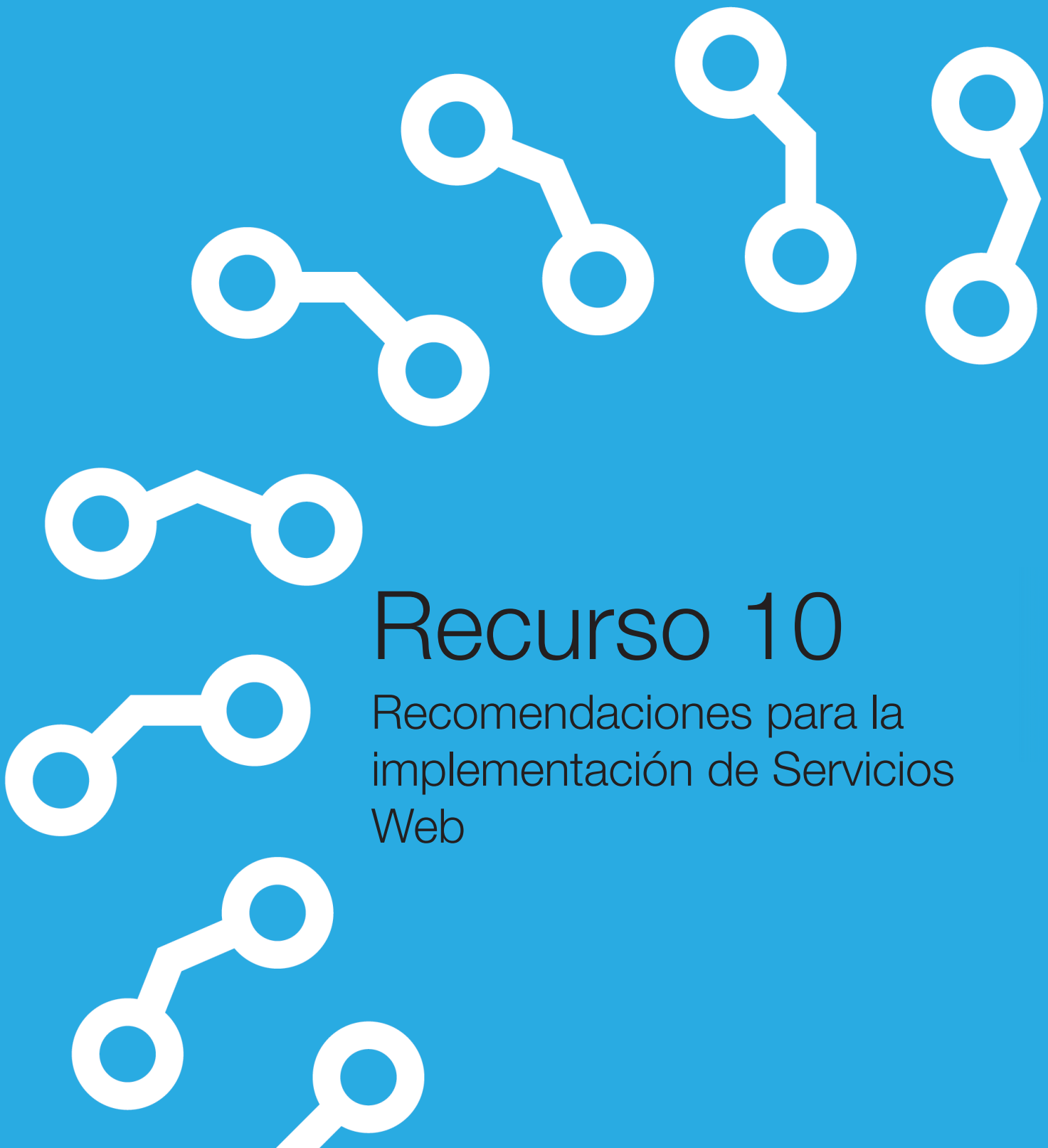
SHA-1	
Referencia	RSA para la firma digital se reconoce en FIPS 186-2 DSS como una alternativa a la DSA: http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf
Descripción	Acrónimo de *Secure Hash Algorithm-1*, Algoritmo de Hash Seguro-1. SHA-1 es un algoritmo de resumen del mensaje (con función de hash criptográfico) diseñado por la Agencia de Seguridad Nacional (NSA[11], por sus siglas en inglés) y publicado por el NIST. Produce una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 264 bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4[12] y MD5[13].
Referencia	RFC 3174: http://www.ietf.org/rfc/rfc3174.txt

[11] **NSA:** National Security Agency
[12] **MD4:** Message-Digest Algorithm 4
[13] **MD5:** Message-Digest Algorithm 5

Otros estándares

DNS	
Descripción	Acrónimo de *Domain Name System*. Sistema de Nombres de Dominio. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
Referencia	• DNS está definido en el IETF en los siguientes RFC: • RFC 1034, “Domain Names - Concepts and Facilities” • http://www.ietf.org/rfc/rfc1034.txt • RFC 1035, “ Domain Names - Implementation and Specification” • http://www.ietf.org/rfc/rfc1035.txt

XSLT v2.0	
Descripción	Acrónimo de *Extensible Stylesheet Language Transformations*. Transformaciones XSL. Es un lenguaje para transformar documentos XML en otros documentos XML, documentos de texto o documentos HTML.
Referencia	http://www.w3.org/standards/xml/transformation



Recurso 10

Recomendaciones para la implementación de Servicios Web

Recomendaciones para la implementación de Servicios Web

Objetivo

Describir una serie de recomendaciones para la implementación de intercambios de información entre organismos basados en Servicios Web (Web Services - WS).

Definiciones, premisas y requerimientos

Servicios Web

Un Servicio Web permite la comunicación entre un cliente y un servidor implementado por aplicaciones o componentes de aplicaciones de forma estándar a través de protocolos comunes y de manera independiente al lenguaje de programación, plataforma de implantación, formato de presentación o sistema operativo.

Un WS es un componente de software que encapsula funciones específicas y hace que estas puedan ser utilizadas desde aplicaciones externas con las siguientes características:

a) Utiliza un formato para describir la interfaz del componente (sus métodos y atributos) basado en XML; normalmente implementado por Web Service Description Language (WSDL).

b) Utiliza un protocolo de aplicación basado en mensajes que permite que una aplicación externa interaccione con él; normalmente implementado por Simple Object Access Protocol (SOAP).

c) Utiliza un protocolo de transporte que se encarga de transportar los mensajes por Internet; normalmente implementado por Hiper-Text Transport Protocol (HTTP o HTTPS).

d) Implementan funciones encapsuladas, es decir que la forma en que han sido implementadas no es visible para el

cliente.

e) Requieren de escaso acoplamiento, es decir que el cliente no necesita conocer nada acerca de la implementación del servicio al que está accediendo, salvo la definición WSDL.

f) Son contractuales, gracias a que existen descripciones públicamente disponibles que especifican su comportamiento, cómo deben ser invocadas y parámetros de entrada y salida.

g) Soporta comunicación sincrónica (RPC) y asincrónica (mensajería).

h) Implementa un conjunto de métodos o funciones con alguna coherencia funcional o temática entre ellos[1].

Premisas de diseño

El presente modelo de implementación de Servicios Web se basa principalmente en las premisas que se describen a continuación:

a) Limitar el intercambio de información a dos organismos, uno que requiere el servicio -Organismo Solicitante- y otro que lo provee -Organismo Proveedor-. Un determinado servicio puede ser solicitado y provisto por más de un organismo.

b) Exigir la existencia previa de acuerdos, en cualquier de sus formas, entre los organismos participantes en el intercambio de información. Esto implica que entre el organismo que provee el servicio y el que lo consuma, debe existir un acuerdo que formalice la relación.

c) Limitar a la provisión de tipos básicos de servicios. No incluir servicios conversacionales, coreografías[2] o comunicaciones con intermediarios.

d) Utilizar estándares abiertos de Servicios Web.

e) Priorizar, dentro de lo posible, como características arquitectónicas: robustez[3], peformance[4], predecibilidad[5], “monitoreabilidad”[6].

f) Estructurar la solución de manera que, dado un avance en la madurez de nuevos estándares, permitiera reemplazar los actuales sin cambios estructurales en el modelo inicial.

g) Asegurar que el modelo pueda ser implementado con componentes de software de libre disponibilidad.

Requerimientos de seguridad

Las características de seguridad que se exigen al presente modelo son las siguientes:

---

[1] En el documento se utiliza el término servicio para referirse a WS, distinguiéndose cuando sea necesario de los métodos (funciones, rutinas, etc.) que implemente.

[2] Según la terminología utilizada en Servicios Web, la coreografía se refiere a la interacción de los servicios con sus usuarios. Cualquier usuario de un WS (automatizado o no), es un cliente del servicio. Estos usuarios pueden ser otros Servicios Web, aplicaciones o humanos. Las transacciones deben estar bien definidas al momento de ejecución, y deben consistir en múltiples interacciones separadas cuya composición constituye una transacción completa. Esta composición (protocolos de mensajes, interfaz, secuencia y lógica asociada) se considera una coreografía.

[3] Capacidad de un componente de software de funcionar con el mínimo de fallas, independientemente de como están programados los aplicativos que los usan y de las condiciones de uso de los servidores donde son ejecutados. Un software robusto al ser exigido puede aumentar su tiempo de respuesta pero nunca deja inhabilitados los servicios que ofrece.

[4] Implica que tanto el diseño como el desarrollo deben estar orientados a maximizar la eficiencia en términos de rendimiento, tiempo de respuesta y disponibilidad minimizando el uso de recursos informáticos disponibles

[5] Capacidad de reproducir los mismos resultados en tiempos similares para solicitudes semejantes.

[6] El diseño y la operación del sistema deben permitir el monitoreo en tiempo real para verificar la correcta operación de todos los elementos del sistema.

a) **Disponibilidad:** Garantizar que los mensajes permanezcan accesibles a los Organismos Solicitantes de información según lo establecido en el acuerdo.

b) **Identificación y autenticación:** Asegurar la presentación de identificaciones que permitan reconocer al otro organismo y distinguirlo fehacientemente de otros.

c) **Autorización:** Asegurar que los servicios sean utilizados exclusivamente por los Organismos Solicitantes expresamente autorizados para hacerlo.

d) **Confidencialidad:** Garantizar que los mensajes sólo puedan ser accedidos por el Organismo Solicitante y el Proveedor.

e) **Integridad:** Garantizar que los mensajes sólo puedan ser procesados por el Organismo Solicitante y el Proveedor, evitando que puedan ser modificados y garantizando que puedan ser detectadas las alteraciones ocasionadas por terceros o por problemas de comunicaciones.

f) **No repudio:** Asegurar que los organismos no puedan negar haber utilizado los servicios.

Requerimientos de confiabilidad

Las características de confiabilidad que se exigen al presente modelo son las siguientes:

a) **Garantía de entrega:** Establecer mecanismos que permitan a las partes conocer la efectiva recepción de los envíos realizados.

b) **Unicidad:** Establecer mecanismos que permitan a las partes procesar sólo una vez los mensajes que se hayan enviado múltiples veces, en los casos en que así corresponda.

No se incluye como requerimiento:

c) **Orden:** Establecer mecanismos que permitan al proveedor procesar los mensajes en el orden que fueron enviados.

Descripción del modelo

El modelo propuesto se basa en los siguientes componentes:

a) **Acuerdo** pre-existente entre los organismos involucrados en el intercambio para la utilización de los Servicios de Información.

b) El acceso a los WS se debe realizar por un **medio de interconexión seguro** establecido entre el emisor y el proveedor para este fin.

c) Salvo las excepciones que se describen más adelante, para utilizar los Servicios de Información se debe tramitar previamente un **servicio de autenticación y autorización**.

La seguridad requerida se implementa por una combinación de las características aportadas por las distintas capas que componen el modelo: seguridad jurídica por el acuerdo, seguridad lógica por el protocolo de transporte, por el canal de comunicaciones, por el protocolo de mensajería y por la adopción de otras específicamente establecidas en el Marco de Interoperabilidad (MIO).

a) **Acuerdo de servicio**
La habilitación para usar un Servicio de Información debe estar precedida y respaldada por un acuerdo entre las partes, llamada acuerdo de servicio.

Se utiliza el término “acuerdo” en un sentido amplio que permita cubrir las distintas figuras legales que puedan implementarse para establecer, entre personas físicas y/o jurídicas, los términos y condiciones del intercambio de información. La figura

jurídica, las formas de publicación y aceptación pueden acomodarse a las circunstancias y a la normativa particular de cada organismo. La implementación puede realizarse de diferentes maneras, utilizando soporte papel o medios electrónicos tanto para la toma de conocimiento, como para la aceptación de los mismos.

Un acuerdo de servicio se debe incluir:

a) **Solicitud de servicio:** donde el organismo, entidad privada o persona física, identificado como el Organismo Solicitante requiere al Organismo Proveedor la provisión de información mediante el presente modelo de intercambio y acepta las obligaciones, las condiciones técnicas y funcionales, y los niveles de servicio de la prestación.

b) **Responsabilidades:** donde se especifican los términos generales acordados o aceptados y las responsabilidades generales de cada organismo.

c) **Definición de WS:** se definen las características funcionales de cada Servicio de Información que intercambiarán.

d) **Condiciones de mantenimiento y cancelación del servicio:** especifican las condiciones para el mantenimiento, modificación, suspensión temporal y cancelación de los servicios acordados.

b) **Medio de interconexión**
La implementación del medio de interconexión por omisión es Internet, pero se deben utilizar componentes complementarios que brinden las condiciones de seguridad requeridas, en caso de no utilizar alguna de las condiciones enunciadas a continuación, se debe describir detalladamente en la documentación técnica relacionada.

a) Canalización segura como VPN (Red Privada Virtual)

b) Protocolización segura tipo HTTPS (como conjunción de HTTP y SSL)

Los organismos deben acordar el direccionamiento IP para el armado del medio de interconexión y del canal de comunicación, implementando NAT de ser necesario o utilizar rangos de direccionamiento IP público.

Es responsabilidad de ambos organismos el establecimiento de condiciones de seguridad desde los extremos del medio de interconexión hacia sus redes internas. Estas condiciones permiten que el modelo no utilice encriptación de mensajes fuera del medio establecido.

c) **Servicio de autenticación y autorización**
Para acceder a los Servicios de Información se debe acceder previamente a un servicio de autenticación y autorización que autentique al Organismo Solicitante y verifique su derecho a hacerlo.
El servicio de autorización se debe Implementar como un Servicio de información particular en los términos que se describen en su respectiva documentación.

Características de métodos y servicios

Se describen a continuación características generales de los diversos tipos de métodos y servicios.

Niveles de seguridad de los servicios

Se distinguen dos niveles de seguridad de los servicios dependientes de la **criticidad de la información** a la que permiten acceder:

a) **Públicos:** son aquellos que no requieren identificación, autenticación ni otras medidas de seguridad para su consumo.

b) **Irrestrictos:** Son aquellos servicios que no requieren autorización para su ejecución. Cualquier emisor que establezca el medio de interconexión según el acuerdo puede acceder a servicios de este nivel y a los métodos por éste implementados. No deben ser considerados servicios públicos.

c) **Autorizables:** Son aquellos servicios, que además del acceso por el medio de interconexión acordado, se requiere de una autorización específica para que el emisor pueda accederlos.

Niveles de seguridad de los mensajes

Se distinguen dos niveles de seguridad de mensajes que se deben utilizar en función de la **criticidad del servicio**:

a) **Firmados:** Cuando el mensaje o parte de éste requieran estar firmados por el Organismo Solicitante antes de ser enviados, fundamentalmente para garantizar el no repudio en base a la autenticación e integridad que aporta la firma.

b) **Planos:** Cuando el mensaje no requiere de ningún tipo firma.

Tipos de servicios

Se definen tres tipos de servicios:

a) **Servicios de Información:** es el conjunto de métodos implementados por el Organismo Proveedor que, recibiendo datos desde el Organismo Solicitante los procesa y genera la correspondiente respuesta. Son los servicios de intercambio de información propiamente dichos. En base a las características de cada Servicio de Información se debe determinar si su nivel de seguridad es irrestricto o autorizable y los mensajes, firmados o planos.

Dependiendo de su criticidad e importancia, los Servicios de Información se caracterizan por su nivel de seguridad. El funcionamiento y las características de los mensajes dependen fuertemente de ello, por lo tanto deben ser descritos por separado.

Servicios irrestrictos

Los Servicios de Información caracterizados como irrestrictos pueden ser accedidos por todo Organismo Solicitante que haya firmado un acuerdo de servicio y haya establecido un canal de comunicación para acceder a los Servicios Web del Organismo Proveedor. Por lo tanto no se realiza ningún tipo de autorización en particular sobre estos servicios.

Una vez recibido un requerimiento de este tipo, el proveedor debe tratar su resolución, devolviendo los resultados en caso satisfactorio y un código error en caso contrario.

Servicios autorizables

Como ya ha sido descrito, para requerir un Servicio de Información de nivel autorizable se debe tramitar previamente un ticket por medio de un servicio de autorización. Una vez que se posea, se puede requerir el servicio de Información correspondiente.Cuando el proveedor reciba un servicio de este tipo, debe validar que el ticket:

- Fue generado por el correspondiente servidor de

autorización.

- Fue generado para el mismo emisor que está solicitando el servicio.
- Fue generado para el Servicio de Información que está solicitando.
- Está vigente.

Si todas las validaciones precedentes son superadas, se debe ejecutar la lógica asociada al método invocado y construir el mensaje de respuesta con los resultados.

b) Servicio de autenticación y autorización: implementa un método irrestricto con mensaje firmado por el cual el Organismo Solicitante requiere autorización de ejecución de un determinado Servicio de Información. Este servicio se debe utilizar para autorizar la solicitud de Servicios de Información de nivel de seguridad autorizable.

Para acceder a un Servicio de Información con nivel de seguridad autorizable, el emisor debe tramitar un ticket. La obtención de éste lo habilita a utilizar el Servicio de Información específico por un determinado lapso de tiempo -especificado en la vigencia del ticket- y se realiza mediante un servicio de autorización ofrecido sin restricciones por el Organismo Proveedor -que no requiera de la tramitación previa de un ticket-.

Para la obtención del ticket, el Organismo Solicitante debe enviar al servicio de autorización un mensaje firmado. Teniendo en cuenta el contenido del certificado del Organismo Solicitante y la identificación del Servicio de Información requerido, el servicio de autorización del Organismo Proveedor debe efectuar la validación del requerimiento.

Si el requerimiento supera las validaciones, el Organismo Solicitante está autorizado a ejecutar el Servicio de Información requerido, se debe entonces devolver un ticket firmado por el servicio de autorización. Éste debe ser utilizado por el Organismo Solicitante en todas los subsiguientes requerimientos de Servicios de Información para el cual se gestionó la autorización.

El ticket debe ser válido para un único servicio y para un Organismo Solicitante pero podrá utilizarse más de una vez limitándolo sólo por tiempo. Si el mismo emisor precisa acceder a más de un servicio, debe requerir un ticket por cada uno. El ticket se genera con una 'vida útil' o vigencia asignada dinámicamente. La vida útil es el tiempo durante el cual el ticket sigue siendo válido. Su duración máxima se establece en función de la criticidad de la información en cuestión, con un máximo de 24hs. Si un Servicio de Información falla por caducidad del ticket -al término su vida útil-, el Organismo Solicitante debe requerir otro, como si fuera la primera vez, para seguir utilizando el servicio.

El Organismo Solicitante debe administrar la persistencia de los tickets en sus aplicaciones para evitar la solicitud indiscriminada de éstos. El Organismo Proveedor puede aplicar acciones de contención si detecta requerimientos excesivos de servicios de autorización.

La definición de la estructura del ticket y su contenido son atribuciones del Organismo Proveedor, el conocimiento de estas características por parte del Organismo Proveedor queda librado a un acuerdo entre las partes.

c) **Servicios de test:** servicios o métodos que permiten verificar el funcionamiento de las diferentes capas de la solución.

El Organismo Proveedor debe suministrar servicios de test que simulen el comportamiento de cada servicio ofrecido para poder verificar el desempeño funcional de la solución. Estos servicios tienen como objeto permitir al emisor la prueba u homologación de la aplicación cliente.

Se deben proveer valores ficticios -dummy-, tablas de prueba u otros mecanismos sobre las cuales se pueda ejecutar la funcionalidad de test de manera tal que no afecte datos productivos ni devuelva información reservada. Simultáneamente se debe garantizar que los servicios de test tengan un comportamiento lo más parecido posible al servicio que se quiere probar, teniendo la confianza en que si la solución funciona satisfactoriamente con los servicios de test, lo hará satisfactoriamente en los casos reales.

Estos servicios pueden ser implementados en un entorno de homologación o en uno de producción. En el primer caso, se debe garantizar la compatibilidad con el entorno de producción. En el segundo, se debe asegurar que las transacciones realizadas a modo de test no tengan impactos indeseados en producción.

El Organismo Proveedor debe prestar los medios para la verificación del funcionamiento de la infraestructura comprometida en la solución y que, en casos de falla, brinde información suficiente para detectar el origen y facilitar su corrección por el responsable. Estos servicios tienen como objeto permitir al Organismo Solicitante la prueba de su propia infraestructura de WS, la del Organismo Proveedor y del medio de interconexión. Este servicio no ejecuta ninguna funcionalidad sólo devuelve un código de retorno donde marca diferentes condiciones de error que pudiera encontrarse en su ejecución.

Una vez verificado el funcionamiento de la infraestructura, es preciso verificar que los servicios de autorización e información estén disponibles y operen correctamente. Esta funcionalidad de los servicios tiene como objeto permitir al Organismo Solicitante comprobar que éstos y los repositorios de datos asociados del Organismo Proveedor están activos.

En cada uno de estos servicios se deben proveer valores ficticios y tablas de prueba sobre las cuales se pueda ejecutar la funcionalidad de test de manera que no afecte datos productivos ni devuelva información válida. Cada servicio de test debe funcionar lo más parecido posible al Servicio de Información correspondiente.

Convenciones

Se detallan a continuación una serie características de uso obligatorio:

Identificación de organismos

Para identificar exclusivamente a los organismos participantes se debe utilizar la conjunción de los atributos que se detallan más adelante y deben ser explícitos en el acuerdo de servicio.

a) Registro de información fiscal.

b) Nombre distintivo o identificador único que se incluye en los certificados digitales.

Identificación de los servicios

Todo servicio debe tener una identificación

de servicio (IdServicio) única por proveedor. Esta identificación es utilizada para tramitar la autorización de acceso a los servicios y debe estar presente en todos los accesos al servicio específico.

Mensajes de los Servicios de Información

Los mensajes de los Servicios de Información se deben estandarizar de la forma que se define más abajo. Los nombre incluidos entre <> indican que son expresiones XML.

Todos los objetos XML incluidos en los mensajes deben estar definidos en el respectivo WSDL.

Se propone como estructura de parámetros de Request la siguiente:

(<objetoSeguridad>,
<objetoNegocioRequest>)

objetoSeguridad : token, firma, otros

otros : [objetos de seguridad pero definidos por el negocio]

objetoNegocioRequest :[contiene los parámetros propios del request del negocio]

Se propone como estructura de parámetros de Request la siguiente[7]:

(<objetoNegocioResponse>)

objetoNegocioResponse : [contiene los parámetros propios de la respuesta de negocio]

Manejo de la autorización

La autorización se debe aplicar a servicios y no a métodos, es decir, que si un emisor es autorizado a acceder a un servicio, tiene derecho a invocar a todos los métodos por éste implementados. En algunos casos claramente identificados, pueden existir métodos dentro de un servicio que pueden ser invocados sin necesidad de autorización, por ejemplo, el caso de servicios de test para verificar la salud de los distintos componentes.

Un servicio de nivel irrestricto no puede contener métodos que requieran autorización. Por el contrario, un servicio que requiere autorización, puede contener métodos de nivel irrestricto. Si los métodos a implementar tienen niveles de autorización diferentes, deben agruparse en dos o más servicios con igual nivel o asignarse el mayor nivel de autorización a todo el conjunto.

Manejo de confiabilidad

Para asegurar la confiabilidad, todos los servicios deben ser respondidos por el proveedor. Aunque funcionalmente el mensaje no requiera respuesta, el proveedor debe enviar una respuesta con el correspondiente “acuse de recibo”. El emisor, al envío de cada mensaje debe iniciar un tiempo de espera, que en caso de cumplirse sin recibir la respuesta, debe enviar nuevamente el mensaje y repetirlo tantas veces como se hayan fijado los reintentos. Si se agotaron los reintentos, el emisor debe generar un error de aplicación.

El tiempo de espera, la cantidad de reintentos y los métodos de contingencia se deben acordar entre las partes.

Manejo de unicidad

Para tratar la unicidad de procesamiento de los mensajes, el emisor debe agregar un número de identificación de transacción, único por cada Servicio de Información que se solicite. Es responsabilidad del proveedor persistir estas identificaciones de los servicios ya respondidos y, ante cada nueva solicitud, debe verificar que no se haya respondido anteriormente. En caso de recibir un servicio con identificación duplicada, el proveedor deber asumir que ya fue resuelto anteriormente y responderlo de la misma manera que en el llamado original. Por lo tanto, el número de identificación de servicio sólo puede repetirse en el caso de enviarse nuevamente el mismo mensaje.

La práctica definida para el manejo de

[7] Con < > se indica que son objetos en XML.

la unicidad es obligatoria en los casos transaccionales de intercambio de datos. En los casos de servicios de consulta, su utilización queda a criterio de las necesidades funcionales.

Manejo de error

Todos los errores que se produzcan deben ser controlados en la capa donde ocurra; el código de error obtenido -Error Interno- y el resto de la información útil para su resolución, deben ser pasados hasta la capa superior del servicio. La capa superior debe:

a) Enviar el Error Interno con el detalle que fuera capturado, más la información adicional que pueda ser útil para el análisis al sistema de monitoreo -según la instrumentación que se defina-. Se recomienda pasar los parámetros de la función específica que controló el error para tener mayor información al momento de analizar el error.

b) Traducir el Error Interno como Error Externo con la leyenda apropiada para el usuario externo y reportarlo a la capa de usuario siempre como SoapException.

Archivos WSDL

Los archivos WSDL que se utilicen deben tener las siguientes características:

a) Deben contener todas las operaciones y objetos necesarios para la interpretación de los mensajes.

b) Todas las etiquetas utilizadas en las respuestas deben estar declaradas en el propio archivo WSDL.

c) No se deben usar declaraciones “Import”.

d) Todos los servicios deben estar configurados con Style = “document”

Registro de transacciones

Los servicios que sean considerados con algún nivel de criticidad deben ser almacenados en un ‘Log de transacciones’. En el acuerdo de servicio se debe determinar y especificar la obligatoriedad del registro de los requerimientos realizados o recibidos. Por cada una de estas obligaciones se debe especificar si el resguardo es parcial o total, el tiempo total de guardo y el tiempo de resguardo en línea. En caso de un resguardo parcial -que no se guarde el mensaje completo-, se deben especificar las partes de los mensajes de requerimiento y respuesta que deben almacenarse.

Log del Organismo Proveedor

Según se estipule en el acuerdo de servicio, cada Organismo Proveedor debe registrar en una nueva entrada de una tabla o archivo cada servicio requerido por algún Organismo Solicitante. Los datos a almacenarse por cada requerimiento de un servicio (de autorización o información) son:

- Identificación del servicio
- Identificación del Organismo Solicitante
- TIMESTAMP[8] de recepción del requerimiento
- TIMESTAMP de envío de respuesta
- Código error
- ticket
- Datos del mensaje de requerimiento
- Datos del mensaje de respuesta.

Los datos de los mensajes de requerimiento y respuesta que deban guardarse en el log pueden reflejarse en el acuerdo de servicio correspondiente. De no especificarse, queda librado a la decisión del organismo.

[8] Formato estándar para almacenar fecha y hora. Cantidad de segundos a partir del 1/1/1970 GMT.

Log del Organismo Solicitante

Según se estipule en el acuerdo de servicio, cada Organismo Solicitante debe persistir en una nueva entrada de una tabla o archivo para cada servicio requerido a algún Organismo Proveedor. Los datos a almacenarse por cada requerimiento de un servicio (de autorización o información) son:

- Identificación del servicio
- Identificación del Organismo Proveedor
- TIMESTAMP de envío del requerimiento
- TIMESTAMP de recepción de la respuesta
- Código error
- ticket
- Datos del mensaje de requerimiento
- Datos del mensaje de respuesta.

Los datos de los mensajes de requerimiento y respuesta que deban guardarse en el log pueden acordarse en el acuerdo de servicio correspondiente. En caso de no especificarse, queda librado a la decisión del organismo.

Documentación de los servicios

Por cada servicio que se desarrolle, el Organismo Proveedor debe producir y entregar la documentación para su utilización. La documentación debe comprender los aspectos necesarios para interpretar la funcionalidad y las especificaciones técnicas para la correcta programación de los aplicativos clientes. Aunque exista una normativa específica que de origen a los servicios, los aspectos funcionales y técnicos necesarios para su utilización deben describirse en la documentación en lenguaje técnico compresible para los analistas funcionales y programadores destinatarios de la misma.

La documentación específica de cada Servicio de Información debe contener los siguientes temas:

a) Descripción de los escenarios de uso.

b) Condiciones generales para su solicitud y utilización.

c) Descripción detallada para la utilización del servicio de autenticación y autorización.

d) Diagramas generales de funcionamiento.

e) Conformación del servicio en métodos.

f) Descripción detallada de cada uno de los mensajes de entrada y salida de cada uno de los métodos.

g) Descripción detallada de los códigos, mensajes de error, su correcta interpretación y las correspondientes medidas para solucionarlo.

h) Nivel de tolerancia de fallos del WS.

También se deben documentar los aspectos relativos al nivel de servicio: cantidad de transacciones por unidad de tiempo, tiempos de respuesta esperados, niveles de contención, medios de contingencia y atención de problemas en operación.

Recomendaciones

Se incluyen a continuación recomendaciones generales con respecto a la implementación de servicios:

a) Incluir en los mensajes de respuesta todas las descripciones asociadas a códigos tabulados.

b) Incluir métodos que permitan obtener las diferentes tablas de codificación utilizadas en los Servicios de Información.

c) Implementar mecanismos tipo RSS para informar a los interesados en los diferentes servicios las novedades con respecto al mismo.

d) Se debe acordar e implementar los mecanismos apropiados para que todas las partes involucradas puedan mantener actualizadas las tablas de codificación utilizadas en los mensajes intercambiados.

e) Cuando se procesen "lotes", dejar la cantidad máxima que se pueda incluir de forma variable y que pueda ser consultado por un método específico incluido en el WS. Así, de ocurrir algún problema de desempeño se debe modificar la dimensión de los requerimientos, no deben hacerse cambios en la lógica. Los clientes deberían consultar periódicamente la dimensión máxima establecida antes de armar los grupos repetitivos a incluir en los mensajes de respuesta.

f) Para asegurar la integridad de los mensajes -especialmente los de gran tamaño-, ya sean tanto de requerimiento como de respuesta, es recomendable agregar una función digesto[9] para calcular la carga de información. La función debe ser aplicada inicialmente por el emisor y verificada posteriormente por el proveedor. En el caso en que falle la comparación que realiza el proveedor entre el cifrado enviado por el emisor y el calculado por él, se debe enviar un mensaje de respuesta con el código error correspondiente. La utilización o no de esta característica debe ser parte de la definición de cada servicio.

g) Se recomienda que el número de identificación de servicio se implemente con un NONCE[10], un número para ser usado por única vez o con un sólo propósito. Este NONCE debe estar generado por los propios entornos de ejecución provistos por los lenguajes de desarrollo y ser independiente de la lógica de las instituciones.

[9] Función de digesto o ("Hash") es un algoritmo o programa que se utiliza como herramienta para dotar a un documento digital de integridad; es decir, se lo utiliza para poder detectar cualquier alteración posterior a su firma

[10] Es un identificador relativamente único, obtenido de una distribución tal que la probabilidad de obtener dos veces el mismo identificador es extremadamente baja.