República de Panamá

CONSEJO NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

Resolución No. 15
3 de mayo de 2016

"Por la cual se aprueba el Esquema de Interoperabilidad Gubernamental de Panamá como parte del Sistema Nacional de Interoperabilidad y de Seguridad".

EL CONSEJO NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL
en uso de sus facultades legales, y

CONSIDERANDO:

Que mediante la Ley 65 de 30 de octubre de 2009, publicada en la Gaceta Oficial No. 26400-C de 30 de octubre de 2009, creó la "Autoridad Nacional para la Innovación Gubernamental (AIG), anteriormente, Secretaría de la Presidencia para la Innovación Gubernamental".

Que con la citada Ley 65 de 30 de octubre de 2009, también se creó el "Consejo Nacional para la Innovación Gubernamental", como instancia encargada de aprobar las propuestas de políticas y planes nacionales de desarrollo de tecnología, uso eficiente de los recursos tecnológicos e innovación gubernamental que formule la Autoridad Nacional para la Innovación Gubernamental (AIG),.

Que el 9 de noviembre de 2012, fue publicada en la Gaceta Oficial No. 27160, la Ley 83 de 9 de noviembre de 2012, que regula el uso de medios electrónicos para los trámites gubernamentales y modifica la Ley 65 de 30 de octubre de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental (AIG).

Que la Ley 83 de 9 de noviembre 2012, en su artículo 15, crea el Sistema Nacional de Interoperabilidad y de Seguridad, cuyas políticas serán definidas y aprobadas por el Consejo Nacional para la Innovación Gubernamental.

Que las políticas a las que se refiere el artículo 15 antes mencionado, comprenderán el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta en forma obligatoria por todas las entidades públicas, para la toma de decisiones tecnológicas que garanticen la interoperabilidad, y la Autoridad Nacional para la Innovación Gubernamental (AIG), coordinará los procesos de utilización y comunicación de tales normas por parte de la entidades públicas.

Que para ello, y en cumplimiento de lo que establece la Ley se hace necesario expedir las normativas en materia de interoperabilidad aplicables a las entidades públicas, por lo que, el Consejo,

RESUELVE:

PRIMERO: Aprobar el Esquema de Interoperabilidad Gubernamental de Panamá como parte del Sistema Nacional de Interoperabilidad y de Seguridad, cuyo detalle se adjunta como Anexo a la presente Resolución.

SEGUNDO: El presente documento podrá ser modificado cuando el Consejo Nacional para la Innovación Gubernamental lo estime conveniente, apoyándose en las recomendaciones emitidas por el Comité Nacional de Interoperabilidad y Seguridad.

TERCERO: Esta resolución empezará a regir a partir de su aprobación.

CUARTO: La Autoridad Nacional para la Innovación Gubernamental (AIG), está facultada para comunicar a las entidades públicas acerca de la obligatoriedad de cumplir con las normativas o estándares en materia de interoperabilidad.

FUNDAMENTO DE DERECHO: Ley 65 de 30 de octubre de 2009, el Decreto Ejecutivo No. 205 de 9 de marzo de 2010, la Ley 83 de 9 de noviembre de 2012 y el Decreto Ejecutivo No. 719 de 15 de noviembre de 2013.

CÚMPLASE,

EL PRESIDENTE,

FRANCISCO SIERRA
DELEGADO POR EL PRESIDENTE DE LA REPÚBLICA

LOS MIEMBROS,

SALVADOR SÁNCHEZ
DELEGADO POR EL MINISTRO DE LA PRESIDENCIA

EYDA VARELA DE CHINCHILLA
DELEGADA POR EL MINISTRO DE ECONOMÍA Y FINANZAS

LUIS CISNEROS
DELEGADO POR EL SECRETARIO NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN

EL SECRETARIO,

IRVIN A. HALMAN
AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

Esquema de Interoperabilidad Gubernamental de Panamá como parte del Sistema Nacional de Interoperabilidad y de Seguridad

Artículo 1. Se establece el Esquema de interoperabilidad gubernamental, con el objetivo de determinar los principios y las consideraciones necesarias, que garanticen un nivel adecuado de interoperabilidad organizativa, semántica y técnica, tomando en cuenta la arquitectura de interoperabilidad, seguridad y la plataforma de interoperabilidad, como modelo integral, a fin de incrementar la eficiencia operativa de las Entidades Públicas y su relación con la sociedad.

Artículo 2. Definiciones
Para los efectos de esta reglamentación los términos se entenderán según el Glosario de Términos incluidos en el Anexo I.

Artículo 3. Ámbito de aplicación
El ámbito de aplicación será el establecido en el artículo 1 de la ley 83 del 9 de noviembre de 2012.

Artículo 4. El Sistema Nacional de Interoperabilidad y de Seguridad se desarrollará de acuerdo a lo establecido en el artículo 15 de la ley 83 del 9 de noviembre de 2012, a través del Comité Nacional de Interoperabilidad y Seguridad, conforme a algunas facultades que se indican en la excerta legal antes citada, tomando en cuenta estos principios de interoperabilidad:

1. **Accesibilidad.** Las entidades deben facilitar a todos los usuarios, en especial a aquellos con capacidades especiales, el acceso a los trámites y servicios, siguiendo características de acceso reconocidas a nivel internacional.
2. **Asociación.** Facilitar el acceso de otras entidades públicas a la información, datos y conocimiento para la prestación de servicios en línea.
3. **Colaboración.** Las entidades participarán de los procesos de análisis diseño, desarrollo, implementación y operación de los servicios web, las aplicaciones y las arquitecturas para lograr la interoperabilidad en la República de Panamá.
4. **Confidencialidad.** Las entidades deberán seguir los lineamientos establecidos en la legislación nacional para regular el manejo de la confidencialidad, sin perjudicar el derecho que tienen los usuarios de autorizar el uso de información de carácter confidencial.
5. **Disponibilidad**. Garantizar que los sistemas, entidades y usuarios puedan acceder a la información de los trámites y servicios en el momento que así lo requieran. Para información o datos críticos las entidades podrán mantener en sus sistemas la información o datos necesarios que permitan mantener una alta disponibilidad.
6. **Divulgación.** Las entidades públicas deberán habilitar canales o medios para promover la participación de los ciudadanos.
7. **Estandarización.** Se debe utilizar estándares abiertos de manera que se facilite las integraciones y las convergencias.
8. **Gratuidad.**
    a. La tramitación en línea no generará gastos adicionales a los ya establecidos a los ciudadanos. Los servidores públicos no percibirán derechos por su intervención, salvo por disposición legal que disponga lo contrario.
    b. El intercambio y consumo de datos, información o servicios entre instituciones no generará costo alguno.
9. **Igualdad.** Los trámites a través de medios digitales tendrán la misma validez que los realizados de forma presencial y no deberán generar restricciones o limitaciones para los ciudadanos que decidan utilizar medios diferentes al contacto tradicional.
10. **Integridad.** Las entidades deberán garantizar que la información utilizada o generada permanecerá sin alteraciones por personas o procesos no autorizados, a menos que sea modificado por la fuente de confianza correspondiente, en cuyo caso deberán existir registros.
11. **Neutralidad tecnológica.** En ningún caso se podrá implicar la existencia de restricciones o discriminaciones de cualquier naturaleza en el acceso de los usuarios a los trámites electrónicos.
12. **Responsabilidad.** Las entidades serán responsables de cumplir con las políticas, condiciones, protocolos, garantías de seguridad, integridad y disponibilidad, acordadas entre los distintos participantes.
13. **Reutilización**. Las entidades generarán los medios para compartir y poner a disposición la información para las que lo requieran.
14. **Simplicidad.** Los trámites serán desarrollados de forma tal que resulten sencillos, entendibles y sin la exigencia de requisitos que retrasen el proceso.
15. **Seguridad.** Las entidades deberán garantizar la protección y la disponibilidad de la información, infraestructura y recursos informáticos, empleando los procesos y medidas de ciberseguridad.

16. **Transparencia.** Brindar acceso general a los trámites electrónicos, datos públicos y requerimientos, a través de las plataformas de interoperabilidad en el cual cada entidad mantendrá actualizada la información y la relación de servicio o trámites públicos.
17. **Trazabilidad.** Las entidades deberán garantiza que el usuario, ya sea un ciudadano u otra institución, conozca en todo momento el estado de su trámite, que le permitan identificar, analizar situaciones y mantener bitácoras de los servicios.

Artículo 5. Para lograr la interoperabilidad organizacional las dependencias y entidades, en ámbito de sus atribuciones, deberán:
Para lograr la interoperabilidad organizacional las dependencias y entidades, en ámbito de sus atribuciones, deberán:

1. Establecer la arquitectura empresarial de la institución de acuerdo con la Arquitectura Meta y el documento "Guía para el proceso de Arquitectura Empresarial para Entidades Gubernamentales", establecido por la AIG.
2. Definir y acordar, conjuntamente con las entidades públicas, el alcance de sus responsabilidades al consumir o proveer servicios web.
3. Definir y acordar con las entidades públicas, cumpliendo con lo establecido por el comité de interoperabilidad y seguridad, los objetivos, alcances y procesos de negocios, previo análisis, así como la simplificación y optimización de los mismos para lograr la usabilidad y reducción de tiempos en beneficio del ciudadano. De ser necesario, se procederá a definir y cambiar los procesos existentes o establecer nuevos procesos. Generando los cambios requeridos en el área legal, estructura organizacional de la institución y en la forma de administrar y controlar los procedimientos o procesos con el fin de asegurar la exactitud, confiabilidad y continuidad de los servicios ofrecidos a otras instituciones, negocios y ciudadanos.
4. Emplear las metodologías recomendadas por la Autoridad nacional para la Innovación Gubernamental para la optimización de procesos.
5. Identificar, planificar e implementar proyectos de interoperabilidad en las entidades, cumpliendo con lo establecido por el comité de interoperabilidad y seguridad.
6. Establecer los montos presupuestarios y actividades necesarias para lograr el desarrollo e implementación de proyectos de interoperabilidad.
7. Desarrollar las competencias y habilidades del personal, para que puedan desarrollar, implementar y prestar servicios web de intercambio de información.
8. Establecer y publicar las condiciones de seguridad para el consumo de los servicios, datos y documentos que pongan a disposición al resto de las entidades.
9. En un documento electrónico, se debe especificar las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios, los perfiles de los participantes, protocolos y criterios funcionales o técnicos necesarios para acceder a los servicios, así como las condiciones de seguridad aplicables, cuando tengan bajo su custodia activos críticos.
10. Las entidades públicas difundirán los servicios que prestan y servicios web que posean a las demás entidades, de forma gratuita. Este servicio se publicará en un catálogo de servicios en la Plataforma única de Interoperabilidad del Estado, para garantizar el acceso seguro al resto de las entidades.
11. Las entidades que cuenten con infraestructura tecnológica deberán mantenerla actualizada. Mantener actualizados con componentes de seguridad, auditoria, monitoreo, recuperación ante desastre, respaldos, gestión y actualización de la plataforma.
12. Las entidades deberán utilizar la plataforma de AIG para la interoperabilidad del estado.

Artículo 6. Para alcanzar la interoperabilidad semántica será necesario publicar las fuentes de datos autorizadas y aplicar los modelos de datos de intercambio y todos los relativos a infraestructura, servicios y herramientas comunes. Para alcanzarlo se deberá:

1. Aplicar obligatoriamente los modelos de datos de intercambio que se establecerán a través del Comité Nacional de Interoperabilidad y Seguridad en cuanto al intercambio de información, así como en infraestructura, servicios y herramientas comunes.
2. Establecer y publicar, en colaboración con las entidades, la definición de los modelos de datos requeridos para el intercambio de información con otras entidades, de acuerdo a lo que establezca la norma técnica de interoperabilidad semántica.
3. Las entidades deberán mantener actualizado los modelos de datos establecidos por la Comisión Nacional de Interoperabilidad y Seguridad como parte del esquema de interoperabilidad.
4. Los modelos de datos deben ser conforme a los estándares de interoperabilidad.
5. Las instituciones deberán establecer un plan para compartir información.
6. Aplicar los protocolos para el intercambio de información.
7. Las instituciones deberán administrar el ciclo de vida de la información.

Artículo 7. Para garantizar la interconexión, accesibilidad, la integración e intercambio de datos y la seguridad de la información, es necesario establecer normas y estándares técnicos.

1) Los estándares recomendados para iniciar la implantación de la interoperabilidad deberán seguir las siguientes pautas:

   a) Ser estándares abiertos o, a falta de estos, estándares de uso generalizado aprobados previamente por la Autoridad de Innovación Gubernamental, para garantizar la independencia en la elección, escalabilidad y en la neutralidad tecnológica. Por lo tanto los documentos, servicios y aplicaciones que se pongan a disposición se deberán encontrar mediante estándares abiertos.
   b) En caso de que las entidades no dispongan de un estándar abierto que satisfaga la funcionalidad del sistema en cuestión, se recomienda diseñar un plan para la migración hacia estándares abiertos.
   c) Para la selección de estándares, en general y, para el establecimiento del catálogo de estándares, en particular, se atenderá a los siguientes criterios:
      - La definición de estándares abiertos establecida en el Anexo I.
      - A las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, internacionalmente aceptados, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

2) En ámbito de sus atribuciones las Entidades deberán:
   a) Poner a disposición de las entidades, las aplicaciones desarrolladas por sí o que hayan sido objeto de contratación, y se posean los derechos de propiedad intelectual o industrial, en una plataforma de control de versiones del estado, mediante la celebración de un convenio.
   b) Utilizar las recomendaciones y directrices generadas por Organismos Internacionales en materia de interoperabilidad, sistemas de información o aplicaciones observando los principios de seguridad, integridad, y confidencialidad.
   c) Aplicar las normas técnicas, estándares, requisitos y condiciones para el acceso y utilización de servicios web e información entre las instituciones.
   d) Establecer los términos y condiciones de contratación que garanticen la portabilidad de las aplicaciones, servicios web, bases de datos y plataformas a través del tiempo.
   e) Establecer procesos y estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad, bajo la coordinación del comité de interoperabilidad y seguridad.
   f) Aplicar obligatoriamente los estándares técnicos que establezca la AIG.

Artículo 8. La Arquitectura de interoperabilidad determina el modelo de arquitectura que relacionará los servicios web brindados por las entidades con las TIC's para el intercambio de información e integración de los servicios o trámites.

Artículo 9. La infraestructura de servicios estará definida por los documentos técnicos que serán emitidos por la Comisión Nacional de Interoperabilidad y Seguridad.

Anexo
Glosario de Términos

1. Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.
2. Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.
3. Ciberseguridad: a la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada;
4. Escalabilidad: capacidad de una computadora, producto o sistema, de expandirse para dar servicio a un gran número de usuarios sin incurrir en fallas
5. Especificación técnica: definición de las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

6. Estándares abiertos: las especificaciones cuya utilización esté disponible de manera gratuita o que no suponga una dificultad de acceso, y que su uso y aplicación no esté condicionada al pago de un derecho de propiedad intelectual o industrial;
7. Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.
8. Fuente de confianza: a la dependencia o entidad o a las unidades administrativas de éstas, que en atención a sus atribuciones y por la relevancia, confiabilidad y veracidad de la información que administran, proporcionan información de consulta de uso común a través de medios digitales;
9. Interoperabilidad: capacidad de las organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las dependencias y entidades compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicaciones;
10. Interoperabilidad organizacional: los mecanismos que establecen la forma de colaboración entre las dependencias y entidades para asegurar la coordinación y alineación de los procedimientos administrativos que intervienen en la provisión de los servicios de gobierno digital;
11. Interoperabilidad semántica: los mecanismo y modelo de datos que garantiza el significado preciso de la información para que pueda ser utilizada por cualquier sistema o aplicación;
12. Interoperabilidad técnica: especificaciones técnicas que garantizan que los componentes tecnológicos de los sistemas de información están preparados para interactuar de manera conjunta;
13. Modelo de datos: conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.
14. Neutralidad tecnológica: opción de elegir la alternativa tecnológica más adecuada a las necesidades de las dependencias y entidades, con el propósito de no excluir, restringir, condicionar o favorecer alguna tecnología o modelo de negocio informático en particular;
15. Portabilidad: al conjunto de características que permiten la transferencia de la información de un sistema o aplicación a otro.
16. Servicios: Conjunto de prestaciones desarrolladas por una institución pública para satisfacer una necesidad social determinada.
17. Servicio Web: es una tecnología que utiliza un conjunto de protocolos y estándares que sirve para que distintas aplicaciones desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma puedan intercambiar datos.
18. Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.
19. Trámite Electrónico: a los trámites que el usuario realiza mediante el uso de las tecnologías de la información y la comunicación.
20. TIC: a las tecnologías de la información y comunicaciones.