NORTIC A4 2024

NORMA PARA LA INTEROPERABILIDAD ENTRE LOS ORGANISMOS DEL ESTADO DOMINICANO

Santo Domingo, República Dominicana
Julio 2024.

ogtic

GOBIERNO DE LA
REPÚBLICA DOMINICANA

NORTIC A4:2024
NORMA PARA LA INTEROPERABILIDAD ENTRE LOS ORGANISMOS DEL ESTADO DOMINICANO

Edición: 3ra
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

Dirección de Transformación Digital Gubernamental
Departamento de Normas y Estándares

Año de publicación: 2024
Versión 3.0

Diagramado y diseñado por la Dirección de Comunicaciones, OGTIC.

CONTENIDO

PALABRAS DEL DIRECTOR

UNA ARQUITECTURA DIGITAL GUBERNAMENTAL A PRUEBA DE FUTURO

Bartolomé Pujals

Director general de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) y director ejecutivo del Gabinete de Innovación y Desarrollo Digital.

En la era digital, donde la tecnología y la información son vitales, los gobiernos enfrentan el desafío de adaptarse constantemente para cumplir con las expectativas ciudadanas y mejorar la sociedad. En este contexto, la interoperabilidad emerge como un concepto crucial para la eficiencia, la transparencia y la efectividad de los servicios gubernamentales.

La interoperabilidad, entendida como la capacidad de diferentes sistemas y organizaciones para intercambiar información y operar de manera coordinada y armoniosa, se erige como un pilar fundamental del Gobierno Digital e Inteligente. En la República Dominicana, la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) ha asumido el compromiso de liderar y promover la adopción de estándares y prácticas que fomenten la interoperabilidad entre los organismos del Gobierno Dominicano.

La presente normativa marca un punto crucial en nuestro camino hacia la modernización y la eficiencia gubernamental. La actualización presenta mejoras notables que buscan reforzar y estandarizar los procesos de interoperabilidad a nivel nacional. Entre los cambios más destacados se encuentran:

1. La Plataforma Única de Interoperabilidad es la única vía designada para la interoperabilidad gubernamental. Actúa como un sistema integral que garantiza el intercambio seguro y eficaz de datos entre los organismos del Estado dominicano.

2. Para ayudar a las organizaciones a colaborar con entidades externas, se ha creado un "Catálogo de Interoperabilidad". Este catálogo facilita las conexiones con actores externos y fomenta el intercambio de información y la colaboración entre diferentes sectores.

3. Se incluyen elementos adicionales que brindan una orientación clara para aplicar y cumplir con la interoperabilidad, como el objeto de la norma, el campo de aplicación, los sujetos obligados, objetivos generales y específicos, condiciones de aplicabilidad para certificación, procedimiento de certificación y las consecuencias del no cumplimiento.

4. Introducción de un enfoque específico sobre la interoperabilidad de la salud, destacando la capacidad de sistemas y plataformas para compartir datos médicos de manera efectiva entre diversos actores del sector. Esta nueva orientación promete optimizar significativamente la calidad de los servicios médicos al permitir un acceso más rápido y seguro a la información relevante, siempre resguardando la confidencialidad y privacidad de los datos personales.

Estas actualizaciones se alinean estrechamente con la arquitectura digital gubernamental y la estrategia nacional de interoperabilidad. La interoperabilidad no es solo un concepto técnico, sino que es la base del Gobierno Digital e Inteligente, cuyo objetivo es mejorar la vida de los ciudadanos y ayudar al desarrollo económico y social del país.

En resumen, esta normativa es un gran avance en nuestro camino hacia la modernización y la eficiencia gubernamental. Al ponerla en práctica, esperamos no solo optimizar nuestros procesos internos, sino también contribuir a un mejor servicio a todos los ciudadanos de la República Dominicana.

INTRODUCCIÓN

La normativa para la Interoperabilidad entre los Organismos del Gobierno Dominicano establece las directrices que deben seguir las instituciones a fin de lograr los procesos de interoperabilidad de manera efectiva en el ecosistema que compone la Administración Pública.

La interoperabilidad en el Estado dominicano tiene por propósito simplificar los trámites, eliminar la burocracia y reducir los costos. Con la interoperabilidad en el Estado se persigue reducir los riesgos asociados a la movilidad, a la colección de datos análogos del ciudadano en cada institución; así como el esfuerzo de los tiempos empleados para lograr las certificaciones requeridas, que hacen de la vida un espacio de enorme insatisfacción.

La interoperabilidad, en términos funcionales, consiste en colectar por el ciudadano, documentos análogos, ahora convertidos en digitales, requeridos en aspectos de la vida humana o industrial para que los agentes económicos, legales, académicos e industriales lo presenten a requerimiento. La propuesta consiste en evitar que el ciudadano sea el mensajero del Estado.

En términos técnicos, la interoperabilidad tiene la función de conectar todos los servidores que administran información del Estado, interconectarlos y construir productos digitales que satisfagan la demanda del mercado digital.

Para lograr tal nivel de superioridad en el mundo digital, se han creado cuatro (4) pilares de sustentación para la interoperabilidad, que son:

a) La interoperabilidad organizacional;

b) La interoperabilidad semántica;

c) La interoperabilidad jurídica, y;

d) La interoperabilidad técnica.

Las funciones de estos pilares garantizan su instauración y orquestación, de forma que la **interoperabilidad organizacional** aporta directrices que deben aplicar los organismos para asegurar una coordinación apropiada de las actividades contenidas en la implementación de la interoperabilidad, así como la alineación de sus procesos de negocio, responsabilidades y expectativas para lograr los objetivos.

La **interoperabilidad jurídica** registra los acuerdos institucionales sobre los que se aplicarán las reglas de negocios que sustentan el intercambio de datos, su integridad y custodia. Se registran los planes de cooperación interinstitucional para la generación de documentación legal y organizacional necesaria en la ejecución del intercambio de datos y sus propósitos.

Por su parte, la **interoperabilidad semántica,** se concentra en la descripción de los servicios, así como los esquemas de metadatos para darle seguimiento a la información interoperada. Los acuerdos de los diccionarios de datos sobre los cuales se negocia la interoperabilidad.

Finalmente, en la **interoperabilidad técnica,** se establecen las pautas para las interfaces de programación de aplicaciones, los protocolos de intercambio de información y formatos digitales que deben ser utilizados en el desarrollo y/o implementación de toda solución tecnológica en cada organismo gubernamental.

En cuanto a la interoperabilidad técnica, en esta normativa se establece mandatorio realizarla sobre la arquitectura REST y sobre la Plataforma Única de Interoperabilidad, que son los recursos tecnológicos adoptados por la OGTIC (Oficina Gubernamental de la Información y Comunicación) para establecer un estándar de sustentación técnica. El cumplimiento de estos estándares son mandatorios para lograr la certificación emitida por la OGTIC, y, sobre todo, cumplir con los propósitos misionales de cada una de las instituciones que conforman la estructura del Estado.

Todas las instituciones deberán ser certificadas por la OGTIC, a través del Departamento de Normas y Estándares, según el mandato de esta norma. Su cumplimiento y aplicación es mandatorio noventa (90) días posteriores a su publicación.

ANTECEDENTES

La Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) es el organismo del Estado dominicano responsable de fomentar el uso de las Tecnologías de la Información y Comunicación (TIC), creada mediante el decreto No. 54-21 del 2 de febrero del 2021, manteniendo sus funciones en el decreto No. 1090-04 del 3 de septiembre del 2004, dependencia desconcentrada del Ministerio de Administración Pública (MAP), con autonomía financiera, estructural y funcional, a fin de garantizar eficiencia, transparencia, servicios en línea y mecanismos para rendición de cuentas disponibles a favor de la ciudadanía.

En cumplimiento de lo dispuesto en el Decreto Núm. 92-22, sobre el Marco Nacional de Interoperabilidad Gubernamental, en su artículo 5, establece las responsabilidades de la Oficina Gubernamental de Tecnologías de la Información y la Comunicación (OGTIC):

a) Bajo la estructura de gobernanza establecida por el Ministerio de Administración Pública (MAP), desarrollar la Plataforma Única de Interoperabilidad y definir sus protocolos, modelos de interacción e interfaces.

b) Asistir a los entes y órganos de la Administración Pública en la creación y gestión de canales únicos de atención al ciudadano no presencial, de cara a facilitar el acceso interinstitucional, así como a la ciudadanía, las empresas y la sociedad civil.

c) Facilitar la interconexión e intercambio de información espontánea entre los entes y órganos de la Administración Pública.

Como parte de sus funciones, la OGTIC tiene a su cargo la formulación de políticas y la implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado hacia la sociedad de la información, promoviendo la integración de nuevas tecnologías, su compatibilidad, interoperabilidad y estandarización en materia de TIC. Por lo tanto, con el objetivo de cumplir con dicha responsabilidad, la OGTIC crea el departamento de Normas y Estándares, el cual elabora y establece las normativas, lineamientos y estándares tecnológicos que impulsen el gobierno electrónico en el país, mediante la elaboración del Marco Normativo de TIC y Gobierno Digital de la República Dominicana.

El Marco Normativo de TIC y Gobierno Digital es el conjunto de normas, guías y documentos técnicos desarrollados por la OGTIC en conjunto con otros organismos gubernamentales, como un mecanismo enfocado en la regularización y estandarización de la implementación y correcto uso de las TIC en el Estado Dominicano. El componente principal de este marco son las Normas de Tecnologías de la Información y Comunicación (NORTIC), creadas y aplicadas desde 2013, concebidas para sistematizar, estandarizar y tener una herramienta efectiva de auditoría para el correcto uso e implementación de las TIC en la administración pública, para crear ciclos de mejora continua de los procesos gubernamentales y contribuir a la eficiencia en el logro de sus objetivos.

En este mismo orden, en el año 2014, fue elaborada la primera versión de la Norma para la Interoperabilidad entre los Organismos del Estado Dominicano, con el objetivo de impulsar las iniciativas de intercambio y uso de datos entre los organismos gubernamentales de una forma ordenada y bajo el marco de las buenas prácticas. Luego, atendiendo a los nuevos avances tecnológicos y como fomento a la continuidad de la modernización del Estado, la OGTIC realizó una revisión y actualización a esta norma publicando su segunda versión en la NORTIC A4:2022, orientada a la interoperabilidad entre organismos, permitiendo intercambiar información de manera efectiva y segura entre los sistemas de los órganos de la administración pública. Esta es la tercera versión de la normativa, revisada y actualizada en el 2024, como medio para intercambiar datos entre organismos gubernamentales, y la Plataforma Única de Interoperabilidad que opera sobre X-Road.

MARCO LEGAL

La Oficina Gubernamental de las Tecnologías de la Información y Comunicación, en su rol de entidad normalizadora sobre el uso e implementación de TIC en la administración pública, ha establecido las directrices por las cuales debe regirse todo organismo gubernamental del Estado dominicano, tanto para aquellos que están físicamente dentro del país, como para los organismos que se encuentran fuera, como son las embajadas, consulados y misiones en el extranjero.

El marco legal que soporta esta norma está compuesto por las leyes y decretos presidenciales que regulan la creación, custodia y transferencia de información del ciudadano, y sus derechos en cuanto a estas. Es por esto, que esta normativa utiliza como marco:

1. La **Constitución de la República Dominicana** 26 de enero de 2010 establece el tratamiento de los derechos sobre la protección de datos personales y, en su artículo 44, define el derecho a la intimidad y al honor personal, en el cual se describe que:

    a) Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley.

b) Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo.

2. La **Ley 53-07,** contra Crímenes y Delitos de Alta Tecnología, donde en su primer artículo que define el Objeto de la Ley establece la protección integral de los sistemas que utilicen tecnologías de la información de la información y comunicación, y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. Igualmente, define como bienes jurídicos protegidos la confidencialidad e integridad de la información o los datos que se transmiten por los sistemas de información y sus componentes.

3. La **Ley 1-12,** sobre Estrategia Nacional de Desarrollo 2030, específicamente en su artículo 16 donde se llama a promover el uso de las tecnologías de la información y comunicación como instrumento para mejorar la gestión pública y fomentar una cultura de transparencia y acceso a la información, mediante la eficientización de los procesos de provisión de servicios públicos y la facilitación del acceso a los mismos.

4. La **Ley 107-13,** sobre los derechos de las personas en sus relaciones con la administración pública y de procedimiento administrativo, en donde se regulan los derechos y deberes de las personas y sus relaciones con la administración pública y se establecen los principios que sirven de sustento a esa relación, indicando los procedimientos administrativos.

    a) **Artículo 4.** Derecho a la buena administración y derechos de las personas en sus relaciones con la administración pública. Se reconoce el derecho de las personas a una buena administración pública y el derecho a no presentar documentos que ya obren en poder de la administración pública o que versen sobre hechos no controvertidos o no relevantes.

    b) **Artículo 27.** Actos de instrucción o investigación. Donde se establece que las actuaciones para la obtención y tratamiento de la información para adoptar una decisión bien informada podrán consistir en la cooperación

e intercambio de información con otras administraciones competentes al objeto de adoptar la decisión mejor informada al servicio de los intereses generales.

5. La **Ley 126-02,** sobre Comercio Electrónico, Documentos y Firma Digital, aplicable a información en forma de documento digital o mensaje de datos, con determinadas excepciones.

6. La **Ley 167-21,** sobre mejora regulatoria y simplificación de trámites, que establece una serie de lineamientos y atribuciones en su artículo 34 sobre interoperabilidad de los sistemas de información, donde establece lo siguiente:

   > Los entes y órganos de la Administración pública deberán utilizar las tecnologías de la información y comunicación en sus relaciones con las demás administraciones y con los usuarios, aplicando medidas informáticas, tecnológicas, organizativas y de seguridad, que garanticen un adecuado nivel de interoperabilidad y la protección de datos de los administrados, conforme las políticas, normativas y lineamientos que establezca el Ministerio de Administración Pública (MAP) , en su calidad de órgano rector.
   >
   > **Párrafo:** La Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), bajo las directrices del Ministerio de Administración Pública (MAP), será la institución responsable de promover y garantizar el uso de las tecnologías de la información y comunicación para la simplificación de trámites.

7. El **Decreto 1090-04,** a través del cual se crea la Oficina Presidencial de las Tecnologías de la Información y Comunicación, el cual establece lo siguiente:

   a) **Artículo 3.-** Serán funciones de la Oficina Presidencial de Tecnologías de la Información y Comunicación, diseñar, proponer y definir las políticas, establecer los lineamientos y elaborar las estrategias, planes de acción y programas para promover, desarrollar y garantizar mayor acceso,

conectividad e implantación de nuevas tecnologías de la información y comunicación, con el fin de fomentar su uso, como soporte del crecimiento económico y competitividad hacia la sociedad de la información, gestionando los proyectos conforme a tales directrices; y que garanticen el acceso equitativo a los mercados y al sector productivo como esfuerzo para la política de generación de empleo, para mejorar la calidad de vida, crear oportunidades de educación, trabajo, justicia, cultura y recreación, y otros.

b) **Artículo 5.-** La Oficina Presidencial de Tecnologías de la Información y Comunicación será responsable de la formulación de políticas y la implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado hacia la sociedad de la información, promoviendo la integración de nuevas tecnologías, su compatibilidad, interoperabilidad y estandarización en materia de TIC.

c) **Artículo 7.-** La Oficina Presidencial de Tecnologías de la Información y Comunicación podrá proponer políticas para difundir y promover la generación de una cultura de TIC en el país.

d) **Artículo 9.-** La Oficina Presidencial de Tecnologías de la Información y Comunicación deberá velar, asistir y supervisar en los aspectos y políticas relativas a la seguridad y privacidad de la información digitalizada y electrónica en el ámbito del sector público.

8. El **Decreto 229-07,** ratifica las funciones que ya le habían sido dadas a la OPTIC y donde pone a su cargo en su artículo 3 el Centro de Contacto Gubernamental e indica la responsabilidad de la institución con la responsabilidad de la implementación y el desarrollo del Gobierno Electrónico en la República Dominicana, y la responsabiliza de coordinar, entre todas las instituciones gubernamentales, la estrategia y la ejecución de la Agenda Nacional de Gobierno Electrónico.

9. El **Decreto 709-07,** sobre las normas y estándares elaboradas por la OPTIC. Donde en su artículo 1 se instruye a toda la Administración Pública del Estado Dominicano a cumplir con las normas y los estándares tecnológicos para la interoperabilidad tecnológica, digitalización de documentos, así como cualquier otra normativa que sea redactada, aprobada y coordinada esa Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), en materia de Tecnología de la Información y Comunicación (TIC) y Gobierno Electrónico.

10. El **Decreto 130-05,** que aprueba el reglamento de la Ley General de Libre Acceso a la Información Pública.

11. El **Decreto 335-03,** que aprueba el Reglamento de Aplicación de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales.

12. El **Decreto 92-22,** establece el Marco Nacional de Interoperabilidad Gubernamental. El artículo 5 del referido decreto, establece que el Marco Nacional de Interoperabilidad recae bajo la rectoría del Ministerio de la Administración Pública (MAP) y la ejecución en la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), distribuyendo las responsabilidades de la siguiente manera:

A la Oficina Gubernamental de Tecnologías de la Información (OGTIC):

a. Bajo la estructura de gobernanza establecida por el Ministerio de Administración Pública (MAP), desarrollar la Plataforma Única de Interoperabilidad y definir sus protocolos, modelos de interacción e interfaces.

b. Asistir a los entes y órganos de la Administración Pública en la creación y gestión de canales únicos de atención al ciudadano no presencial, de cara a facilitar el acceso interinstitucional, así como a la ciudadanía, las empresas y la sociedad civil.

c. Facilitar la interconexión, e intercambio de información espontánea entre los entes y órganos de la Administración Pública.

A las instituciones públicas en sentido general:

d. Hacer uso de la Plataforma Única de Interoperabilidad garantizando un adecuado nivel de interoperabilidad de acuerdo con la normativa vigente.

e. Autorizar la expedición de la documentación resultante de la entrega de servicios digitales mediante firma digital o electrónica del servidor público responsable de la entidad en que presta sus servicios o en su defecto de una autoridad competente de ésta.

13. El **Decreto 707-22,** para la ejecución del Programa Gobierno Eficiente (Burocracia Cero). Donde se instruye en su artículo 7 a todos los entes y órganos de la Administración pública bajo la dependencia del Poder Ejecutivo en sentido general, adoptar las normas y estándares TIC (NORTIC) elaboradas por la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), relativos al diseño y desarrollo de portales, aplicaciones y plataformas, la automatización de servicios, la normalización de tipos, interfaces, estructuras, lenguajes, diccionarios y plataformas para el intercambio seguro de datos, con el fin de asegurar el cumplimiento de los objetivos del Programa Gobierno Eficiente (Burocracia Cero).

14. El **Decreto núm. 54-21,** transforma la Oficina Presidencial de Tecnología de Información y Comunicación (OPTIC), en la Oficina Gubernamental de Tecnología de la Información y la Comunicación (OGTIC), bajo la dependencia desconcentrada del Ministerio de Administración Pública (MAP), manteniendo sus funcione en del decreto núm. 1090-04.

CAPÍTULO 1

NORMA TÉCNICA DE INTEROPERABILIDAD EN EL GOBIERNO DOMINICANO

Esta norma indica mediante directrices, los estándares que deben ser usados por los organismos del Estado dominicano, con el propósito de incorporar arquitecturas, redes, protocolos y programas que hagan posible la interoperabilidad entre todas las instituciones que conforman el ecosistema gubernamental.

Este conjunto de directrices y recomendaciones persigue la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica, jurídica y organizacional de los sistemas y aplicaciones empleados para la prestación de servicios públicos.

Sección 1.01. Objeto, ámbito de aplicación y sujetos obligados

Subsección 1.01.1. Objeto

Esta normativa establece los lineamientos que deben cumplir los organismos del Estado dominicano que intercambien datos con otros organismos en calidad de proveedor de datos, consumidor de datos o ambos.

Subsección 1.01.2. Ámbito de aplicación

Las disposiciones de esta normativa serán aplicables a todos los entes y órganos que conforman la Administración Pública bajo dependencia del Poder Ejecutivo, ya sean centralizados o descentralizados que posean o requieran datos del ciudadano que sean útiles para la prestación de servicios públicos.

Entre los organismos centralizados se encuentran los ministerios y sus dependencias, así como los organismos con nivel de ministerios, viceministerios, organismos adscritos a la Presidencia de la República, consejos y organismos asesores, direcciones generales, oficinas nacionales, procuradurías fiscales, escuelas públicas, hospitales públicos, bibliotecas y museos.

Entre los organismos descentralizados se encuentran los organismos financieros y no financieros, reguladores, seguridad social y empresas públicas.

Los siguientes órganos, instituciones, instancias y grupos que generen datos útiles que puedan ser intercambiados con otros organismos a los fines de mejorar la prestación de servicios públicos, de manera voluntaria, podrán asumir las directrices de esta normativa:

(a) Los poderes Legislativo y Judicial.

(b) Los órganos constitucionales.

(c) Los gobiernos locales.

(d) Las organizacionales no gubernamentales.

(e) Las universidades y academias.

(f) Los grupos organizados de la sociedad civil.

(g) Los grupos organizados del sector privado.

Subsección 1.01.3. Sujetos obligados

Están obligados a cumplir con esta normativa:

(a) Los organismos del Estado dominicano bajo dependencia del Poder Ejecutivo que, en calidad de guardianes de información, tengan la facultad de proveer datos que sean útiles y necesarios para simplificar o reducir la tramitación requerida para la prestación de un servicio correspondiente a otro organismo gubernamental.

(b) Los organismos del Estado dominicano bajo dependencia del Poder Ejecutivo que, para la prestación de alguno de sus servicios, requieran de datos generados, almacenados y custodiados por otros organismos.

Sección 1.02. Objetivos

El objetivo principal de la interoperabilidad gubernamental es mejorar la coordinación y colaboración entre las diferentes entidades gubernamentales a los fines de facilitar la prestación de servicios públicos de manera segura, eficaz, eficiente, transparente y centrada en el ciudadano.

Subsección 1.02.1. Objetivos Específicos

(a) **Mejorar la calidad de los servicios públicos.** La interoperabilidad permite que los ciudadanos y las empresas puedan acceder a los servicios públicos de forma más sencilla y eficiente. Esto se traduce en una mejora en la satisfacción de los usuarios y en un aumento de la productividad.

(b) **Mejorar la transparencia y accesibilidad.** La interoperabilidad mejora la transparencia gubernamental al permitir que otros organismos, los ciudadanos y empresas puedan ver y comprender las reglas y procesos administrativos, datos y toma de decisiones para la prestación de servicios. Igualmente, facilita la participación ciudadana y el acceso a los servicios gubernamentales.

(c) **Reducir costes administrativos.** La interoperabilidad hace posible que las entidades gubernamentales puedan compartir datos y servicios de forma segura y eficiente, lo que reduce la necesidad de duplicar esfuerzos y el gasto de recursos. Esto se traduce en un ahorro de costes para la Administración Pública.

(d) **Aumentar la eficiencia operativa.** La interoperabilidad permite que las entidades gubernamentales puedan utilizar los recursos de forma más eficiente mediante la optimización de los procesos internos. Esto se traduce en un aumento de la eficacia de la Administración Pública.

(e) **Procurar la seguridad de la información.** Mediante la interoperabilidad se busca garantizar la seguridad, integridad y confidencialidad de la información intercambiada entre las entidades gubernamentales.

(f) **Cumplimiento normativo.** La existencia de un estándar asegura que los sistemas y procesos cumplan con las regulaciones gubernamentales, esto a su vez, facilita la adopción de estándares para interoperabilidad que garantizan la consistencia.

(g) **Generar datos útiles.** La interoperabilidad permite el acceso a datos relevantes y útiles de manera oportuna lo cual mejora la toma de decisiones.

Sección 1.03. Términos y terminología utilizada

Subsección 1.03.1. Términos y definiciones

API (Interfaz de Programación de Aplicaciones)

Conjunto de herramientas, definiciones y protocolos que se utiliza para integrar los servicios y el software de aplicaciones. Las APIs habilitan el intercambio de datos entre aplicaciones, independientemente de sus plataformas, arquitecturas y propósitos funcionales.

Protocolo

Es un conjunto de reglas y procedimientos estandarizados que permiten organizar los datos de manera que puedan ser procesados e intercambiados entre diferentes procesadores de información; así como interconectar redes de comunicación entre servidores de datos.

Estándares

Son un conjunto de normas y acuerdos para disponer de una uniformidad en la creación, desarrollo y conexión de los sistemas de información a nivel global. Igualmente se corresponde con el establecimiento de reglas para desarrollar aplicaciones bajo procedimientos homogéneos que garanticen su integridad.

Interoperabilidad

Es la capacidad que tiene un sistema de información para intercambiar datos con otros sistemas con la capacidad de procesarlos. En el contexto gubernamental, es la combinación de protocolos y estándares que permiten el intercambio de datos entre los diversos conjuntos de instituciones que conforman el Estado dominicano, con el propósito de ofrecer servicios en línea y en tiempo real para el ciudadano en su cotidianidad social, política, empresarial y jurídica.

Arquitectura

Se refiere a la organización, estructura lógica, física y nombres asociados a ellas que permiten la administración y controlar eficientemente un ecosistema, cuyo objetivo es que las capacidades blandas puedan acceder a las informaciones para cubrir sus necesidades de datos.

HL7 (Nivel de Salud Siete)

Es un conjunto de estándares para facilitar el intercambio electrónico de información clínica; que utiliza una notación formal del lenguaje unificado de modelado y un metalenguaje extensible de marcado con etiquetas.

JSON (Notación de Objetos de JavaScript)

Es un formato plano de datos que permite su rápida comprensión e interpretación en un ambiente de intercambio de datos.

FHIR (Recurso Rápido de Interoperabilidad Sanitaria)

Se define como un paquete de reglas en el proceso de interoperabilidad de información sanitaria.

SOAP (Protocolo de Acceso a Objetos Simple)

Es un protocolo estándar de comunicación entre dos objetos por medio de XML cuyo propósito es hacer posible la interoperabilidad entre distintas plataformas y aplicaciones, independientemente de su lenguaje.

REST (Transferencia de Estado Representacional)

Es una arquitectura que se ajusta a las necesidades de los servicios web y las aplicaciones móviles ligeras. Es una interfaz que se sirve de aplicaciones en protocolos de Internet, cuyo propósito es convertir esas informaciones a formatos JSON, con el fin de permitir la interoperabilidad.

La OGTIC adopta como estándar las interfaces REST porque es una arquitectura, no un lenguaje.

API RESTful

Se definen como programas, no una arquitectura, cuya función es intercambiar datos funcionando como API con una arquitectura REST.

Datos

Hace referencia a un valor íntegro sobre un elemento determinado, el cual por sí solo carece de importancia y a través del procesamiento adecuado logra convertirse en información útil.

Metadatos

Son un conjunto de información que describe las características de otra información, son "datos sobre datos". Es el log de datos en términos de su contenido, características, historia, calidad y disponibilidad, cuyo origen se centra en el servicio que se ofrece al ciudadano y los servicios secundarios que provienen de esos metadatos.

Modelo de información

Es una representación de los conceptos, las relaciones entre ellos, así como las restricciones, reglas y operaciones que les son aplicables en un dominio específico.

SLA (Acuerdo de Nivel de Servicio)

Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

Guardian de información

Para esta normativa, conocido como custodio, se refiere a los organismos gubernamentales que, por su naturaleza y funciones, recopilan información del ciudadano y protegen su confidencialidad e integridad, pero, aunque se responsabiliza de salvaguardar esta información, nunca se les considera dueños de la información ya que el único dueño de esta es el ciudadano en sí mismo.

URI (Identificador Uniforme de Recursos)

Es una dirección exacta y precisa que permite ubicar un recurso en el internet o en una red de cómputos.

Interfaz de usuario

Es el medio por el cual el usuario puede interactuar con un dispositivo o computador.

Librerías

Son un conjunto de códigos, datos o funciones que brindan soporte a un sistema y pueden ser utilizadas de acuerdo con la necesidad para la que se le solicite.

URL (Localizador de Recursos Uniforme)

Se usa para especificar la dirección exacta de un recurso en el portal web.

Parámetros

En programación, es una variable que puede recibirse con un método o procedimiento.

HTTP (Protocolo de Transferencia de Hipertexto)

Es un protocolo utilizado para realizar la transferencia de texto o hipervínculos, a través de la web.

Plataforma Única de Interoperabilidad

Es el medio definido por el Estado dominicano para la interoperabilidad de los organismos que lo componen.

Proxy

Es una tecnología que se utiliza como puente entre el origen y el destino de una solicitud.

Software

Se refiere a todos los componentes lógicos o intangibles de un sistema de información, tales como programas, aplicaciones, sistemas operativos, entre otros.

DCAT (Vocabulario para Catálogo de Datos)

Es un estándar definido por el Consorcio World Wide Web (W3C) y diseñado para facilitar la interoperabilidad entre catálogos de datos publicados en la Web.

Subsección 1.03.2. Terminología utilizada

Toda directriz indicada con las palabras “debe” o “no debe” representa una obligación con la que debe cumplir todo organismo gubernamental para poder certificarse en esta normativa.

Para fines de esta norma el término “organismo gubernamental” será utilizado indistintamente como “organismo” y se refiere a toda entidad abarcada en el alcance de esta normativa que opte por la certificación.

Igualmente, para fines de definir el rol de los organismos dentro de la interoperabilidad, se indicará como “organismo proveedor” o simplemente “proveedor” a aquellos que transmiten información, mientras que se colocará “organismo consumidor” o “consumidor” a aquellos que utilizan o reciben la información. Un organismo para fines de la normativa puede cubrir ambos roles dentro de un acuerdo de interoperabilidad.

En el caso del término “interorganizacional” hace referencia a cualquier actividad conjunta que se realiza entre dos o más organismos.

Además, los términos “software”, “aplicaciones” y “sistemas”, para fines de esta norma, se utilizarán indistintamente.

El término “elemento de datos” hace referencia a una entidad de información relacionada dentro de un proceso de interoperabilidad.

Sección 1.04. Principios y dimensiones de la interoperabilidad

Subsección 1.04.1. Principios de la interoperabilidad

Los principios de interoperabilidad son aspectos de comportamiento fundamentales para impulsar las acciones de interoperabilidad. En esta sección se establecen los principios generales de interoperabilidad relevantes para establecer servicios interoperables.

A continuación, se presenta los principios destinados a establecer comportamientos generales sobre interoperabilidad:

(a) **Transparencia:** principio que permite:

(i) Habilitar la visibilidad dentro del organismo. Se trata de permitir que otros organismos, los ciudadanos y empresas les permitan ver y comprender las reglas y procesos administrativos, datos, servicios y toma de decisiones.

(ii) Asegurar la disponibilidad de interfaces con los sistemas de información internos. El organismo opera un gran número de sistemas de información heterogéneos y dispares en apoyo de sus procesos internos. La interoperabilidad depende de garantizar la disponibilidad de interfaces a estos sistemas y los datos que manejan. En consecuencia, se facilita la reutilización de sistemas y datos permitiendo a estos integrarse en sistemas más grandes.

(iii) Asegurar el derecho a la protección de datos personales.

(b) **Datos Abiertos:** se refiere a la idea de que todos los datos públicos deben estar disponibles gratuitamente para su uso y reutilización por otros, a menos que se aplican restricciones.

(c) **Neutralidad Tecnológica:** garantizando que los organismos se centren en las necesidades funcionales con el fin de minimizar las dependencias tecnológicas, para evitar imponer implementaciones técnicas que puedan

adaptarse al entorno tecnológico en rápida evolución. Los organismos deben facilitar el acceso y la reutilización de sus servicios y datos independientemente de tecnologías o productos específicos.

(d) **Seguridad y Privacidad:** los ciudadanos y las empresas deben tener la certeza de que cuando interactúan con el organismo lo hacen en un entorno seguro y de confianza y en pleno cumplimiento de las leyes. El organismo debe garantizar la privacidad de los ciudadanos, y la confidencialidad, autenticidad, integridad y no repudio de la información facilitada por ciudadanos y empresas, así como la intercambiada entre diferentes organismos.

(e) **Eficiencia:** se trata de disponer de la capacidad instalada para lograr los objetivos de la interoperabilidad. En términos industriales se conoce la eficiencia, como hacerlo correctamente.

(f) **Eficacia:** en este ambiente, consiste en lograr los resultados esperados del proceso de incorporar los estándares que propone la OGTIC. En términos industriales es hacer lo correcto.

(g) **Buena Administración:** este principio define la forma de ejercicio del poder que se caracteriza por rasgos como la eficiencia, eficacia, transparencia, rendición de cuentas, participación de la sociedad civil y el Estado de derecho. La buena gestión refleja la determinación del gobierno de utilizar los recursos disponibles a favor del desarrollo económico y social, y el bienestar del ciudadano.

Para lograr implementar interoperabilidad no basta con normalizar los sistemas, sino que también deben normalizarse los procesos entre los organismos y el correcto entendimiento de la información intercambiada. Debido a esto, la normativa abarca cuatro (4) dimensiones claves de la interoperabilidad:

1. Interoperabilidad legal

Dimensión de la interoperabilidad que abarca el conjunto de normas y estatutos legales que sirven como habilitante para la interoperabilidad entre las diferentes entidades que la apliquen. A través de este dominio, se busca establecer lineamientos que garanticen que los organismos gubernamentales realicen el intercambio de información mediante procesos de interoperabilidad ajustados al marco jurídico existente.

2. Interoperabilidad organizacional

Dimensión de la interoperabilidad sobre la capacidad de los organismos y de los procesos que manejan para alcanzar de manera mutua una colaboración para el logro de intercambio de información, mediante acuerdos previos a los servicios ofrecidos. La interoperabilidad organizativa involucra todos los aspectos esenciales de todo organismo, entre ellos se destacan:

(a) La estructura del organismo.

(b) Los procesos.

(c) La cultura del personal.

El fin de esta dimensión es definir los objetivos y facilitar la colaboración entre organismos que desean intercambiar información y los cuales pueden tener estructuras organizativas y procesos internos diferentes.

3. Interoperabilidad semántica

Dimensión de la interoperabilidad que se encarga de que la información intercambiada entre los diferentes sistemas informáticos de los organismos sea interpretada con un significado inequívoco. La interoperabilidad semántica se refiere a la transmisión de los metadatos.

El objetivo de esta es que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación. La interoperabilidad semántica se separa en dos niveles:

(a) Interoperabilidad semántica para la visualización.

(b) Interoperabilidad semántica para el procesamiento.

4. Interoperabilidad técnica

Esta dimensión comprende aspectos técnicos y tecnológicos que deben considerarse al implementar la interoperabilidad. Entre estos aspectos se encuentran las interfaces, interconexión, integración de datos y servicios, la presentación de la información, accesibilidad y la seguridad.

Sección 1.05. Categorías de certificación

En esta sección se describen las distintas categorías en las que el organismo puede adquirir la certificación en esta normativa, que para los fines son:

(a) **Categoría A. Organismos que otorgan el dato;** para organismos que, en calidad de guardianes de información, tengan la facultad de proveer datos que sean útiles y necesarios para simplificar o reducir la tramitación requerida para la prestación de un servicio correspondiente a otro organismo gubernamental

(b) **Categoría B. Organismos que consumen el dato;** para organismos que, para la prestación de sus servicios, requiera datos de otro organismo.

(c) **Categoría AB. Organismos que otorgan y consumen el dato;** para organismos que cumplan con ambas condiciones, es decir, que provean datos a otros organismos gubernamentales para la prestación de servicios públicos, así como también los reciba para la prestación de sus propios servicios.

Sección 1.06. Comité de implementación y gestión de estándares TIC

El Comité de Implementación y Gestión de Estándares TIC (CIGETIC), se conforma dentro de los organismos con el objetivo de establecer una instancia responsable de la planificación, seguimiento, escalamiento y gestión de recursos para las implementaciones de estándares NORTIC, así como el seguimiento y reporte de los resultados derivados e indicadores afectados. Para la conformación del CIGETIC, el organismo debe cumplir con lo establecido a continuación:

(a) El organismo debe conformar el Comité de Implementación y Gestión de Estándares TIC (CIGETIC), mediante una resolución administrativa interna.

(b) El CIGETIC debe estar conformado mínimamente por los responsables de las áreas listadas a continuación:

(i) Comunicaciones, prensa o relaciones públicas, es el área responsable del contenido que se presenta para los ciudadanos en todos los medios utilizados por el organismo, como sus portales web (exceptuando la sección de transparencia) y las redes sociales, asegurándose de su actualización constante, respuesta a las interacciones con los ciudadanos, así como del mantenimiento de la identidad gráfica y estilo de comunicación.

(ii) Oficina de Acceso a la Información (OAI), teniendo por responsabilidad la gestión del contenido que se presenta en la sección de transparencia del portal web del organismo, así como de su actualización según las periodicidades establecidas por el órgano rector y la normativa vigente.

(iii) Jurídica, área responsable de ofrecer soporte al comité sobre las leyes, decretos, resoluciones, reglamentos, normas, políticas, acuerdos, convenios y cualquier otro tipo de documentación de carácter legal que sea necesaria para el cumplimiento de las responsabilidades del comité.

(iv) Tecnologías de la información y comunicación (TIC), teniendo bajo su responsabilidad el soporte especializado necesario para los portales del organismo y las implementaciones de estándares NORTIC, así como el ofrecimiento de información en términos de TIC, que el comité necesite para el cumplimiento de sus responsabilidades.

(v) Planificación y Desarrollo, responsable de otorgar soporte para la planificación del proyecto de certificación en una NORTIC y su implementación y además, brindar información al Comité sobre el estatus del organismo en los indicadores de medición transversales vigentes en el Estado.

(vi) Cualquier otra área que designe la máxima autoridad del organismo.

(c) La máxima autoridad del organismo debe designar un miembro del Comité con el nivel de autoridad suficiente para desempeñar la función de coordinador, quien tendrá el papel de liderar el CIGETIC para asegurar el cumplimiento de su objetivo, la gestión de los recursos necesarios y fungir como el representante ante la máxima autoridad.

(d) La máxima autoridad del organismo debe designar un miembro del comité para ejecutar la función de secretario del comité, quien tendrá la responsabilidad de dar el soporte logístico al coordinador en términos de manejo de informes, convocatorias a reunión, registros de actividades y seguimiento.

(e) La resolución debe detallar las responsabilidades generales del CIGETIC, donde se incluyan las siguientes:

(i) Planificación y seguimiento de la implementación de estándares NORTIC.

(ii) Monitorear el mantenimiento de los estándares NORTIC implementados.

(iii) Gestionar la capacitación del personal sobre el Marco Normativo de Arquitectura Digital Gubernamental de la República Dominicana a los fines de facilitar los procesos de implementación y certificación de los estándares NORTIC.

(iv) Realizar reuniones periódicas, con la finalidad de efectuar la gestión correspondiente para el cumplimiento de los objetivos planificados, como el avance de las implementaciones y el mantenimiento de los estándares.

(v) Poner en conocimiento a la máxima autoridad, a través de informes periódicos, sobre el estado de las implementaciones NORTIC y sus derivados.

(vi) Funcionar como primera instancia para la resolución de conflictos que pudieran surgir durante la implementación de los estándares NORTIC.

(vii) Escalar a la máxima autoridad, a través del coordinador, situaciones que requieran la intervención de ésta, como la necesidad de recursos o la resolución de conflictos que no puedan solucionarse a nivel del comité.

(viii) Velar por la capacitación de los integrantes del comité, el personal bajo su cargo y demás involucrados, en las Normas de Tecnologías de la Información y Comunicación (NORTIC).

(ix) Otras responsabilidades que la máxima autoridad delegue.

(f) La máxima autoridad del organismo debe concretar, mediante un artículo de la resolución de conformación, las atribuciones que concede al Comité, en las que se incluya la potestad de:

(i) Convocar a reunión, a colaboradores de la institución que no sean miembros del comité.

(ii) Asignar responsabilidades y tareas a los miembros (y no miembros) del Comité y personal bajo el cargo de estos, siempre que estas sean necesarias para la implementación de estándares NORTIC.

(iii) Otras atribuciones que la máxima autoridad considere necesarias.

(g) La resolución debe establecer, de forma separada a las responsabilidades, las directrices para la entrega de los informes a la máxima autoridad, indicando:

(i) La periodicidad de entrega.

(ii) La estructura de contenido de los informes.

(iii) Otras directrices que la máxima autoridad entienda necesarias.

(h) La resolución del CIGETIC debe estar firmada y sellada por la máxima autoridad del organismo.

(i) Luego de ser aprobada, la resolución de conformación del CIGETIC debe ser notificada a los miembros designados y comunicada a todas las áreas del organismo.

Sección 1.07. Responsabilidades del organismo solicitante

En esta sección se abarcan las responsabilidades de cada organismo que solicite la certificación en la NORTIC A4, las cuales se detallan a continuación:

(a) El organismo solicitante, en persona de su titular, debe conformar mediante resolución oficial, el Comité de Implementación y Gestión de Estándares TIC (CIGETIC), que se encargará de planificar la implementación y certificación de las NORTIC, designar a los responsables específicos para trabajarlas, y supervisar el avance sobre planificación, así como el mantenimiento y recertificación bajo estos estándares.

(b) El CIGETIC debe construir y remitir a la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) un plan revisado por sus miembros y aprobado por la Máxima Autoridad Ejecutiva, conteniendo la planificación y responsables específicos para la implementación y certificación bajo los estándares establecidos por el Marco Normativo de Arquitectura Digital Gubernamental de la República Dominicana, así como las Normas de Tecnologías de la Información y Comunicación (NORTIC) y documentos técnicos que lo conforman.

(c) El CIGETIC conformado debe gestionar con la OGTIC, una capacitación sobre el Marco Normativo de Arquitectura Digital Gubernamental de la República Dominicana para sus miembros y personal de técnico de interés, como forma de facilitar los procesos de implementación y posterior certificación de los estándares NORTIC.

(d) El organismo solicitante, a través del CIGETIC, debe determinar y gestionar los recursos e infraestructura necesaria para implementar, certificar y mantener los estándares exigidos en las NORTIC, lo cual debe ser proporcionado por la Máxima Autoridad Ejecutiva de la institución.

(e) El CIGETIC conformado debe mantener a la Máxima Autoridad Ejecutiva del organismo enterada, a través de informes presentados ante la misma a intervalos planificados, sobre el avance en la ejecución de los procesos de certificación en los que está inmerso el organismo, frente a la planificación que fuera aprobada.

(f) Al momento de realizar la solicitud de certificación o recertificación, el organismo, a través del CIGETIC, debe asegurarse de que todo el personal responsable e involucrado en estos procesos, haya leído detenidamente las normativas correspondientes, es consciente de la pertinencia e importancia de su rol en el proceso y de cómo contribuye para el logro de los objetivos institucionales a través las implementaciones y certificaciones NORTIC que se están trabajando.

(g) El organismo debe cumplir con los requerimientos establecidos en las Normas de Tecnologías de la Información y Comunicación (NORTIC) para obtener las certificaciones correspondientes, asegurándose de mantener estos estándares durante el tiempo de validez de la certificación

y comunicando a la OGTIC cualquier cambio a los medios, sistemas o plataformas certificados, para la evaluación y validación adecuadas.

(h) El organismo usará y pondrá visibles los certificados físicos NORTIC entregados por esta Oficina Gubernamental, evitando copiar o duplicar el certificado otorgado, siguiendo los lineamientos del Manual de Uso de Marca NORTIC vigente.

(i) El organismo solo utilizará y pondrá visible los Sellos de Certificación NORTIC que son entregados por esta Oficina Gubernamental, evitando la sustitución de estos por imágenes, la utilización de sellos de otras instituciones y en general haciendo uso de sellos digitales que no hayan sido entregados expresamente por este organismo. El uso de los sellos debe ser acorde al Manual de Uso de Marca NORTIC vigente.

(j) El organismo solicitante deberá estar en contacto frecuente con la OGTIC durante el proceso de certificación, debe informar sobre los avances logrados al menos cada 15 días, debiendo responder a los seguimientos de los consultores, para mantener el proceso de certificación activo.

(k) Si un organismo entiende, tras un análisis del CIGETIC, que una o más de las NORTIC no son aplicables, por razones contextuales o de operación, debe solicitar al Departamento de Normas y Estándares la verificación, quienes después de un análisis emitirán una decisión sobre la aplicabilidad de la o las normativas, lo que se comunicará a las áreas de medición correspondientes.

Sección 1.08. Responsabilidades y atribuciones de la OGTIC

En esta sección se indicar las responsabilidades que posee OGTIC con el organismo solicitante de la certificación NORTIC A4, así como también las atribuciones pertinentes, las cuales se detallan a continuación:

(a) La OGTIC asignará analistas y auditores de normas y estándares al organismo solicitante, en las etapas que corresponda, quienes serán los

responsables del acompañamiento y evaluación del organismo durante todo el proceso de certificación o recertificación.

(b) El equipo de Normas y Estándares, que trabaja con los organismos solicitantes aplicará las políticas y procedimientos aprobados para cada certificación o recertificación, al tiempo que sigue los lineamientos éticos, de conducta y confidencialidad definidos por la OGTIC.

(c) El tiempo de respuesta de los analistas y auditores de normas y estándares dependerá de la cantidad de organismos que estén en evaluación y toda verificación se calendará a la fecha más próxima de disponibilidad, lo que se comunicará a los organismos solicitantes.

(d) Los organismos que fueron evaluados por los analistas y estén listos para finalizar el proceso de certificación, serán verificados en el mismo orden que en que entran a la fase de Auditoría NORTIC del proceso, lo que implica que el tiempo de duración de esta verificación dependerá de la cantidad de organismos en cola.

(e) Cancelar cualquier proceso de certificación en curso cuando se evidencie el incumplimiento del organismo solicitante con las políticas definidas en el punto 2 "Políticas de Certificación", especialmente las políticas de tiempo.

(f) Retirar con previo aviso cualquier certificación activa cuando, luego de haberse otorgado la certificación, se evidencie la violación de los estándares certificados y estos no sean corregidos según el procedimiento de Monitoreo de Normas establecidos en el departamento.

Sección 1.09. Condiciones para la revocación de la certificación NORTIC A

En esta sección se abarcan las condiciones que provocarán la revocación de la certificación NORTIC a cualquier organismo que la posea en estado activo y vigente, las cuales se detallan a continuación:

(a) **Vencimiento:** una vez transcurridos los dos años de vigencia de certificación sin que se haya agotado un proceso de recertificación, se procederá de manera automática con la revocación.

(i) La revocación por vencimiento se llevará a cabo igualmente aún el organismo tenga un proceso de recertificación activo. Por tanto, el organismo es responsable de solicitar el proceso de recertificación con tiempo suficiente como para finalizarlo antes de la fecha de vencimiento definida.

(b) **Incumplimiento:** si se determina que el organismo incumple con cualquiera de los elementos de la normativa certificada, se le notificará al organismo de la falta vía correo electrónico o por comunicado.

Si el organismo no corrige la falta levantada y notificada (cuando aplique), se revocará la certificación notificando al organismo el motivo por el que se realizó.

CAPÍTULO 2

REQUISITOS Y PROCEDIMIENTO PARA LA CERTIFICACIÓN NORTIC A4

En este capítulo se tratan todos los elementos que deben tener en cuenta los organismos solicitantes de esta certificación, iniciando por los requisitos para poder aplicar a la certificación, seguido del procedimiento de certificación.

Sección 2.01. Requisitos para la certificación

Para poder solicitar la certificación en la NORTIC A4 el organismo debe cumplir con los siguientes requerimientos iniciales:

(a) Remitir una comunicación de parte de la máxima autoridad en la cual solicite el servicio de certificación NORTIC; esta comunicación debe estar firmada digitalmente.

(b) Enviar una declaración de compromiso con el proceso de certificación NORTIC de parte de la máxima autoridad ejecutiva donde indique aceptación con las políticas vigentes de certificación NORTIC y estar firmada digitalmente.

(c) Tener conformado mediante resolución el Comité de Gestión e Implementación de Estándares TIC (CIGETIC).

    (i) El organismo debe evidenciar que lleva a cabo las actividades definidas para el CIGETIC y mostrar evidencias de su cumplimiento.

(d) Evidenciar constancia del intercambio de datos a través de la Plataforma Única de Interoperabilidad.

(e) Poseer un Acuerdo interinstitucional vigente entre los organismos que están interoperando.

(f) Tener un Informe técnico de los sistemas que se encuentran interoperando.

(g) Constancia de firma digital cualificada y vigente.

(h) Cumplir con los todos los requisitos legales, organizacionales, técnicos y semánticos definidos en esta normativa.

Sección 2.02. Procedimiento para la certificación NORTIC

El organismo solicitante deberá someterse al procedimiento indicado, debiendo aprobar el proceso de auditoría para obtener la certificación NORTIC. En esta sección se establece en primera instancia el procedimiento de asistencia en la preparación para la certificación NORTIC, el cual, tal como su nombre indica, ayuda a guiar a los organismos solicitantes a prepararse para someterse al procedimiento de auditoría, siendo este el que le permitirá obtener la certificación. Estos procesos son independientes uno del otro.

Subsección 2.02.1. Procedimiento de auditoría para certificación NORTIC

Articulo 1.- Auditoría NORTIC: Es el proceso orientado al seguimiento y verificación del cumplimiento de los requerimientos, directrices y criterios establecidos, a fines de obtener una Certificación NORTIC. Es realizado por el Departamento de Normas y Estándares de la OGTIC, con el apoyo de la Dirección de Arquitectura Digital Gubernamental, Dirección de Servicios Digitales Institucionales y Seguridad de la Información.

PÁRRAFO: El procedimiento iniciará con el cumplimiento de los requisitos iniciales indicados en el capítulo I, los cuales, de no ser cumplidos, requerirán la constancia de asistencia previa.

Articulo 2.-Sobre la solicitud: El Organismo realizará la solicitud del servicio a través del formulario del servicio de Auditoría Para Certificación NORTIC, en el portal institucional de OGTIC, en el enlace: https://ogtic.gob.do/servicio/consultoria-y-auditoria-en-las-nortic/.

Párrafo. Las instituciones que no cumplan con los requisitos de la normativa y requieran de una asistencia, deben solicitar el servicio de asistencia para la preparación en las NORTIC, ver subsección 2.04.2

Articulo 3.- Plan de Auditoria. El Departamento de Normas y Estándares recibe y asigna la solicitud al personal de auditoría, que, mediante la validación de los requerimientos iniciales, programará levantamiento in situ, informando previamente por correo electrónico en un plazo de diez (10) días laborales, sobre las fechas y acciones a desarrollar:

1. Calendarizar y comunicar a la institución, la fecha de realización de la etapa de revisión documental inicial para construir el programa de auditoría, el cual tendrá como tiempo de respuesta cinco (5) días laborales.

2. Construir el programa de auditoría NORTIC que será ejecutado en las instalaciones de la institución, indicando la información general, fechas, horas y procesos a ser auditados, utilizando el formato definido por el Departamento de Normas y Estándares el cual tendrá como tiempo de respuesta cinco (5) días laborales.

3. Una vez concluido este plazo, el departamento de Normas y Estándares remite vía correo electrónico, el programa de auditoria NORTIC al Organismo para fines de revisión y aceptación de las fechas propuestas y condiciones establecidas en el mismo.

4. El Organismo solicitante, después de recibir y verificar el programa, debe confirmar su aceptación y aprobación en un plazo no mayor a diez (10) días calendario. En caso de exceder este plazo para dar respuesta, la solicitud será desestimada.

Articulo 4.- Desarrollo del Plan de Auditoria. Se realizan las actividades asignadas en el plan de auditoría, conforme a las fechas previamente establecidas. Una vez concluido, se redacta el Informe de Auditoría, indicando la información general, hallazgos, evidencias y oportunidades de mejora detectados durante la auditoría, utilizando el formato establecido por la OGTIC.

PÁRRAFO: Se presentan los resultados de la auditoría de forma preliminar en la reunión de cierre, previo a su remisión.

Articulo 5.- Revisión de Informe de Auditoría. Se remite el informe de auditoría a la institución, a través del correo institucional, en un plazo de diez (10) días laborables después de la visita in situ.

PÁRRAFO: El Organismo cuenta con un plazo de treinta (30) días calendario para realizar las modificaciones a las observaciones realizadas por el auditor, en caso de no realizarlas en el tiempo establecido el auditor/departamento de Normas y Estándares notificará el cierre de su proceso de certificación.

Articulo 6.- Resultados de Informe de Auditoría: El Departamento de Normas y Estándares debe de comunicar a la institución, vía correo, sobre el cumplimiento o no de los requerimientos de la normativa mediante informe de auditoría final, en un plazo de diez (10) días laborales.

Articulo 7.- Emisión de Certificación. Luego del cumplimiento del informe de auditoría final, la OGTIC procede a la generación y emisión de los Sellos Digitales de Certificación NORTIC en un plazo de cinco (5) días laborales para que lo coloquen en su portal.

PÁRRAFO: En caso de organismos que soliciten la recertificación de la misma normativa, solo se actualizará el sello digital de certificación.

Articulo 8.- Revisión, firma y entrega de Certificado. El certificado es revisado por el Departamento de Normas y Estándares, y enviado para firma al Director General, a través de la plataforma FirmaGOB. Una vez completado, es remitido a la institución en formato digital a través del correo electrónico asignado.

PÁRRAFO: La institución podrá optar por entrega física del certificado, bajo previa coordinación con el Departamento de Normas y Estándares.

Articulo 9.- Registro de Certificación: El Departamento de Normas y Estándares recibirá el registro de acuses de recibo de los certificados entregados para fines de archivo y evidencia.

Subsección 2.02.2. Procedimiento de asistencia en la preparación para certificación NORTIC

Articulo 10.- Asistencia NORTIC. Es un servicio de acompañamiento especializado ofrecido por el Departamento de Normas y Estándares de la OGTIC, cuya función es orientar y acompañar a los organismos gubernamentales interesados en la implementación y certificación de las NORTIC.

Articulo 11.- Sobre la solicitud: El organismo realizará la solicitud del servicio a través del formulario del servicio de Asistencia NORTIC, en el portal institucional de OGTIC, en el enlace: https://ogtic.gob.do/servicio/consultoria-y-auditoria-en-las-nortic/.

Articulo 12.- Sobre la asignación del Analista. El Departamento de Normas y Estándares recibirá y verificará la solicitud de asistencia y la asigna al Analista de Normas y Estándares correspondiente mediante el sistema establecido, en cuatro (4) días laborables.

Articulo 13.- Plan de Asistencia. Recibidas las evidencias del cumplimiento de los requerimientos, el Departamento de Normas y Estándares calendarizará y comunicará la fecha y alcance de dicha asistencia, en un periodo de diez (10) días laborables.

Articulo 14.- Resultados de Asistencia. Al finalizar el Plan de Asistencia, la institución recibirá vía correo un informe con los resultados obtenidos, incluyendo las recomendaciones y plan de capacitación sugerido.

Articulo 15.- Preparación para Certificación: El Organismo solicitante debe aplicar las recomendaciones para poder iniciar la evaluación de Auditoría NORTIC, siendo estas documentadas a través de un plan de trabajo con fechas de término de estas, y enviadas vía correo electrónico, en un periodo no mayor a treinta (30) días calendario, de lo contrario, este proceso de asistencia perderá su vigencia.

CAPÍTULO 3

INTEROPERABILIDAD LEGAL

Para garantizar que los organismos de la administración pública interactúen y compartan información de manera eficaz y segura, hay que establecer lineamientos que habiliten la interoperabilidad. En ese sentido, este capítulo se establecen las directrices que permitirán evitar inconvenientes dentro del marco legal al momento de intercambiar información entre organismos gubernamentales.

Sección 3.01. Lineamientos legales para la interoperabilidad

Los lineamientos legales para la interoperabilidad tienen como objetivo garantizar que existan los mecanismos jurídicos habilitantes para la interoperabilidad y que los organismos involucrados cumplan con dichos mecanismos. Para lograr el cumplimiento de esta dimensión, los organismos gubernamentales deben cumplir las siguientes directrices:

(a) El organismo en calidad de proveedor de datos que intervenga en un proceso de interoperabilidad debe evaluar las competencias legales que lo habilitan para el intercambio de información identificando las regulaciones que incidan en los datos que compartirá.

(b) El organismo debe clasificar la información que será intercambiada mediante interoperabilidad y esta clasificación debe cumplir como mínimo con los siguientes parámetros:

a) **Información pública:** esta información debe estar al alcance, tanto de los empleados del organismo gubernamental como del público externo.

b) **Información valiosa:** esta información se utiliza para las operaciones del organismo gubernamental y debe estar solo al alcance de sus empleados.

c) **Información sensible:** esta información debe estar solo al alcance de personas autorizadas.

(c) Cada organismo debe establecer, cuando aplique, los mecanismos apropiados para licenciar los datos que intercambiarán y usarán otros organismos, donde se establezcan datos para arreglos de custodia, propiedad intelectual, condiciones de uso, entre otros criterios.

(i) Los organismos proveedores al momento de interoperar deben asegurar que los datos compartidos no se encuentren protegidos por derechos de propiedad intelectual.

(d) Al momento de intercambiar información el organismo que consume la información debe cumplir mínimamente con lo siguiente:

(i) Asegurar que los datos personales y/o sensitivos recibidos se traten de manera segura y confidencial.

(ii) Asegurar que la información sensitiva o confidencial recibida no sea accedida por personas no autorizadas.

(iii) No debe compartir la información recibida mediante interoperabilidad con otros organismos o entidades a menos que la institución que otorga el dato lo autorice.

(iv) No debe compartir la información recibida a través la plataforma única de interoperabilidad con otros organismos o entidades no gubernamentales a través de otras vías.

CAPÍTULO 4

INTEROPERABILIDAD ORGANIZACIONAL

Todo proceso de interoperabilidad debe estar adscrito a las reglas de negocio internas de cada institución, a la vez que, deben ser abiertos en la revisión de sus servicios, para identificar si existen trámites que redundan en él. Esta simplificación debe apuntar a que sean servicios digitales y seguros por diseño.

En ese sentido, este capítulo especifica las directrices que deben aplicar los organismos para asegurar una coordinación apropiada de las actividades contenidas en la implementación de la interoperabilidad, y la alineación de sus procesos, responsabilidades y expectativas para lograr un objetivo común. Para los fines, se han definido elementos tales como el acuerdo de colaboración interinstitucional, informes técnicos, políticas de desarrollo y robustecimiento de la interoperabilidad, roles para definir y mantener la interoperabilidad, entre otros elementos descritos en este capítulo.

Sección 4.01. Desarrollo y robustecimiento de la interoperabilidad

Como parte del componente de colaboración interinstitucional que impacta directamente al robustecimiento continuo y holístico de las operaciones del Estado dominicano, se encuentra la gestión interna del desarrollo de las capacidades de interoperabilidad individuales de las instituciones que componen el ecosistema estatal.

Esta gestión se refiere a las acciones proactivas y planificadas que el organismo ejecuta en busca de la mejora continua de sus operaciones haciendo uso de la interoperabilidad, al tiempo que impulsan la cultura de disponibilidad e intercambio de datos que el Estado posee para beneficio de los ciudadanos. Es por esto por lo que:

Debe identificarse el formato de presentación de la información para el intercambio de esta, según su contexto.

(a) El organismo debe realizar un levantamiento de todas las áreas sustantivas o misionales vinculadas con la gestión del trámite o la prestación del servicio público que será optimizado mediante interoperabilidad.

  (i) Todas las áreas definidas en este levantamiento deben participar en las actividades para la optimización del servicio público brindado.

(b) Todo proceso de interoperabilidad debe estar estrictamente adscrito a las naturaleza y funciones de la institución.

(c) El organismo gubernamental debe desarrollar y aprobar una Política de Desarrollo y Robustecimiento de Interoperabilidad, que establezca lineamientos concretos para:

  (i) Realizar un análisis de los componentes operativos de la institución para detectar actividades, trámites, procesos y servicios que puedan mejorarse mediante interoperabilidad.

(ii) La elaboración de un plan de acción para llevar a cabo las acciones de colaboración correspondientes a los fines de interoperar para los servicios y trámites determinados.

(iii) Las acciones de seguimiento que deben implementarse para asegurar el cumplimiento de las actividades planificadas.

(iv) La realización del análisis posterior a la implementación de las acciones determinadas, a los fines de realizar las mediciones de efectividad e impacto de estas.

> Nota: Esta cadena de acciones debe realizarse hasta que todo el flujo de operaciones de la organización sea analizado con estos fines.

(d) La política de desarrollo y robustecimiento de interoperabilidad debe apuntar a que los servicios públicos brindados sean digitales y seguros por diseño.

(e) Si el organismo organiza sus servicios con la estructura indicada en la NORTIC A5:2019, Capítulo 2. **Levantamiento y Estrategia para la Presentación de los Servicios Públicos** o cualquier actualización a la norma de servicios, debe utilizar los resultados arrojados por el Análisis de Reducción de Tramites y el Plan de Automatización de Servicios levantados durante la implementación.

Sección 4.02. Roles para el área de administración de proyectos de TIC

Como parte del proceso Interoperabilidad Organizacional, se define necesaria la delimitación y asignación apropiada de los roles y responsabilidades que debe ejecutar el área de Administración de Proyectos de TIC, con el fin de que la ejecución de las actividades pueda realizarse de manera satisfactoria, traduciéndose esto en que los organismos deben asegurarse de que estas áreas, a lo interno de su estructura, cumplan mínimamente con los criterios que abarca esta sección.

(a) La unidad de TIC debe asignar responsabilidades individuales al personal dentro de la unidad, que participarán en todos los proyectos de interoperabilidad entre sistemas de información.

(b) La gestión del departamento de TIC debe tener estructurada la unidad de administración de proyectos de TIC o bien, el organismo debe disponer de una unidad para la gestión de proyectos con un personal capacitado para administrar proyectos de TIC.

(c) El organismo debe contar con personal adecuado para cumplir con las responsabilidades especificadas a continuación para la administración de proyectos de TIC:

(i) **Líder de proyectos:** responsable de la toma de decisiones sobre la realización de los proyectos según sus prioridades, en base a necesidades, presupuesto e impacto dentro del organismo. Es responsable de lograr el correcto planteamiento de las soluciones a los directivos de las áreas que afectan los proyectos definidos y de lograr la aceptación final de la máxima autoridad del organismo.

(ii) **Manejador de proyectos:** responsable de la administración de los recursos financieros y humanos que estén relacionados con los proyectos. Además, vela por la calidad, cumplimiento de las tareas, sus fases, la elaboración y entrega de la documentación de los proyectos en curso.

(iii) **Líder técnico:** responsable de la coordinación completa del equipo de trabajo técnico, este será el enlace entre el manejador de proyectos y el equipo de técnico que estará trabajando en el proyecto.

(d) Con el objetivo de lograr la integración y el intercambio de información a través de la Plataforma Única de Interoperabilidad, la unidad de TIC debe disponer del personal necesario para desempeñar los siguientes roles:

(i) **Administrador del servidor de seguridad:** responsable de la instalación, configuración y mantenimiento de los servidores de seguridad para la vinculación y el intercambio de información a través de la Plataforma Única de Interoperabilidad.

(ii) **Desarrollador:** responsable de desarrollar los servicios de intercambio de información que se habilitarán en la Plataforma Única de Interoperabilidad, según los lineamientos técnicos del Capítulo 6 sobre Interoperabilidad Técnica.

(e) Con el objetivo de dar seguimiento a la interoperabilidad en funcionamiento, el organismo debe contar con una unidad de Operaciones TIC que lleve a cabo las actividades que permitan mantenerla.

(f) El organismo debe redactar las descripciones de puestos donde se detallen los requisitos de cada puesto de las áreas involucradas en la consecución y mantenimiento de la interoperabilidad, detallando los roles asignados, según mencionado en directrices anteriores.

(i) Los roles para la unidad de administración de proyectos de TIC deben estar descritos o ser cubiertos por las responsabilidades y actividades específicas descritas en los perfiles de cargo o descripción de puestos.

(ii) Las descripciones de puestos redactadas deben cumplir con los requerimientos establecidos por el Ministerio de Administración Pública (MAP).

(g) Si el organismo no tiene personal suficiente para asignar los roles de forma exclusiva, deben redistribuirse en el área para asegurar su cumplimiento.

(h) Todas aquellas personas involucradas en el proyecto con la información completa y necesaria para crear el documento de alcance con los requerimientos solicitados deben asumir el rol de parte interesada.

(i) En caso de que se presenten dificultades o desacuerdos que interfieran en el cumplimiento de los estándares por parte del o los organismos involucrados en el proceso de interoperabilidad y que no puedan ser resueltos de manera interna por la unidad de TIC, deben ser escalados al Comité de Implementación y Gestión de Estándares TIC (CIGETIC), como parte de las actividades de reporte y comunicación que realiza con la máxima autoridad del organismo.

Sección 4.03. Colaboración interinstitucional

La colaboración interinstitucional, en el marco de un proceso de implementación de un sistema de interoperabilidad entre organismos públicos, se refiere a las actividades de formalización y delimitación de condiciones que deben ejecutar los organismos involucrados en el sistema previo a la realización de cualquier actividad técnica.

Al momento de iniciar un proyecto sobre interoperabilidad, cada organismo debe seguir los pasos especificados a continuación:

(a) El organismo propietario de la iniciativa debe cumplir con las exigencias tecnológicas de los organismos de interés, si cumplen con estándares interoperables expuestos en el Capítulo 6. **Interoperabilidad Técnica.**

(b) Los líderes de proyectos de las áreas de TIC de los organismos involucrados deben permanecer en contacto para garantizar el cumplimiento de los tiempos establecidos.

(c) Los organismos involucrados deben establecer tiempos de respuesta para todas las solicitudes requeridas entre ellos, de manera que se pueda mantener en control del plan de proyecto.

(d) Los organismos involucrados deben establecer tiempos para el envío de reportes sobre el estatus del proyecto, por vía de correo electrónico o cualquier otro medio que los organismos consideren pertinentes.

Subsección 4.03.1. Acuerdo de colaboración interinstitucional

(a) Los organismos involucrados en un proceso de interoperabilidad deben firmar acuerdo de colaboración interinstitucional en donde se especifiquen los términos legales para el intercambio de datos.

(i) El acuerdo debe contener políticas claramente definidas, basadas y sustentadas en las reglas de un marco legalmente viable y flexible que permita la implementación de la interoperabilidad gubernamental.

(ii) El acuerdo debe estar firmado digitalmente por las máximas autoridades de los organismos involucrados en el proceso.

(b) El acuerdo de colaboración interinstitucional debe contemplar mínimamente entre sus artículos, los siguientes elementos:

(i) **Objeto:** donde se establezca el propósito común de las partes para llevar a cabo el acuerdo.

(ii) **Compromisos comunes e individuales entre las partes:** donde se especifiquen las obligaciones comunes e individuales contraídas por cada organismo involucrado en el sistema de interoperabilidad.

(iii) **Especificaciones técnicas generales para utilizar en la interoperabilidad:** donde se incluya una breve descripción de los estándares utilizados en el sistema de interoperabilidad.

(iv) **Confidencialidad:** en donde se abarquen las bases de las reglas de acceso y privacidad de los datos.

(v) **Coordinaciones interinstitucionales:** donde se especifique el equipo involucrado en el proyecto de interoperabilidad según los roles especificados en la sección 3.02. Roles para el área de administración de proyectos de TIC.

(vi) **Vigencia:** donde se especifique la validez o uso del acuerdo en un tiempo determinado.

(c) En caso de aplicar, debe incluir acuerdos económicos, formas de pago, servicios con costo, condiciones para rescisión del acuerdo y cualquier otro elemento que los organismos involucrados determinen necesario.

(d) El acuerdo de colaboración interinstitucional debe estar complementado por los siguientes documentos:

a) Informe técnico: documento que describe los aspectos técnicos que forman el sistema. Los puntos mínimos con los que debe contar este documento son los siguientes:

i) Objetivo del proyecto: donde se especifique la finalidad que persiguen los organismos que interoperan con este proyecto, así como la importancia de los servicios y clientes (empresa, organismo o ciudadanos) que se beneficiarán de esta interoperabilidad.

ii) Descripción general del/los sistemas(s): donde se describa en qué consisten los sistemas y cómo beneficiará a sus servicios este proyecto.

iii) Interoperabilidad semántica: en donde se detalle el catálogo de metadatos utilizados para la comprensión e interpretación de la información transmitida de un punto a otro, así como informaciones importantes de los mismos.

iv) Interoperabilidad técnica: en donde se describa de manera puntual cómo se conectan y transmiten los datos tomando en cuenta las aplicaciones, servicios, accesibilidad y seguridad.

b) Acuerdo de nivel de servicio (SLA): establece las expectativas entre el organismo A y el organismo B y describe los productos o servicios que se entregarán. Como mínimo, el SLA debe definir lo siguiente:

i) Contacto de soporte.

ii) Horas de soporte.

iii) Disponibilidad del servicio.

iv) Tiempo de respuesta de soporte.

v) Interrupciones programadas.

vi) Límite de rendimiento.

vii) Límite de tamaño de mensaje.

c) **Procedimiento de manejo del cambio:** utilizado para asegurar la confiabilidad, exactitud, continuidad y evolución del proyecto de intercambio de información prestado entre los diferentes organismos.

CAPÍTULO 5

INTEROPERABILIDAD SEMÁNTICA

La interoperabilidad semántica es esencial para que diferentes sistemas de información en distintos organismos puedan comunicarse y entenderla de manera correcta, por eso en este capítulo se especifican las directrices que debe seguir el organismo para cumplir con esta dimensión.

Sección 5.01. Interoperabilidad semántica para la visualización

La visualización de información es una de las necesidades más comunes en los sistemas de información. Es frecuente que la información registrada en un sistema informático deba ser visualizada en otro sistema distinto. Todos estos detalles forman parte de la correcta comprensión de la información que se visualiza. Por lo tanto, cada organismo debe cumplir con lo especificado de lo mencionado a continuación:

(a) Debe Identificarse el formato de presentación de la información para el intercambio de esta, según su contexto.

(b) Debe disponerse la información para visualizarse en distintos dispositivos, ya sean móviles como de escritorio.

(c) Debe tomarse en cuenta la resolución de la pantalla para los diferentes dispositivos.

Sección 5.02. Interoperabilidad semántica para el procesamiento

El procesamiento automático de la información es uno de los principios básicos de las TIC y uno de los procesos que agregan mayor valor a los sistemas, por lo que, en esta sección se definen metadatos para procesar la información de forma más efectiva. Por tanto, cada organismo debe cumplir con lo especificado a continuación:

(a) Deben utilizarse modelos de información comunes o reconocidos.

(b) En caso de que el organismo necesite diseñar un modelo de información propio, este debe ser independiente de tecnología y plataforma específica.

(c) La estructuración de los metadatos para los elementos y atributos debe cumplir con los siguientes lineamientos generales:

(i) **Claridad:** poseer los conceptos necesarios para una explicación real de lo que se desea expresar.

(ii) **Sencillez:** debe ser simple para su fácil comprensión.

(iii) **Singularidad:** cada concepto debe tener un significado único.

(iv) **Precisión:** los conceptos deben estar definidos de forma concisa y exacta.

(d) Debe crearse un diccionario de datos para los sistemas de información habilitados en la plataforma única de interoperabilidad, en el cual debe definirse como mínimo lo siguiente para cada dato intercambiado:

(i) **Nombre:** define el nombre asignado para identificar coherentemente al dato.

(ii) **Descripción:** donde se explica de forma breve de qué trata el contenido del dato.

(iii) **Tipo:** indica la clase o naturaleza de datos que se van a procesar.

(e) Debe definirse la estructura de los metadatos mediante el Vocabulario para Catálogo de Datos en su versión 2 (DCAT, por sus siglas en inglés).

(f) Debe utilizarse el Formato de Transformación Unicode de 8 bit (UTF-8, por sus siglas en inglés), para la codificación de caracteres a usar para cada atributo.

CAPÍTULO 6

INTEROPERABILIDAD TÉCNICA

En este capítulo se describen y establecen las pautas para las interfaces de programación de aplicaciones, los protocolos de intercambio de información y formatos digitales que deben ser utilizados en el desarrollo y/o implementación de toda solución tecnológica en cada organismo gubernamental.

Sección 6.01. Plataforma única de interoperabilidad

(a) Los organismos gubernamentales deben hacer uso exclusivo de la Plataforma Única de Interoperabilidad para compartir e intercambiar información con otros organismos gubernamentales.

(b) Si el organismo interopera con entidades no gubernamentales para prestar sus servicios, debe seguir lo establecido en el Anexo A. Catálogo de Estándares para la Interoperabilidad.

(c) Para hacer uso de la Plataforma Única de Interoperabilidad, el organismo debe ejecutar el proceso de vinculación a la plataforma, para lo cual debe:

(i) Leer y firmar las políticas de condiciones y aceptación provistas por OGTIC para el uso de la plataforma.

(ii) Tener un servidor de seguridad instalado que cumpla con los requisitos técnicos mínimos.

Para ver los requisitos mínimos necesarios con los que debe cumplir el servidor de seguridad, visitar el siguiente enlace:

https://github.com/ogticrd/xroad-members

(iii) Poseer el personal necesario para cumplir con los roles requeridos en la Sección 4.02 Roles para la Unidad de TIC.

(d) El organismo debe determinar mediante evaluación la cantidad de servidores de seguridad necesarios para el intercambio de información.

(i) Debe existir al menos un servidor de seguridad (nodo de X-Road) por cada centro de datos físico o virtual donde se alojen APIs o servicios de información que requieran datos provenientes de otras entidades.

(e) Con la finalidad de asegurar la continuidad del servicio, el organismo debe:

(i) Implementar balanceo de carga.

(ii) Asegurar alta disponibilidad.

(iii) Poseer un plan para la recuperación ante desastres.

(iv) El organismo debe crear tantos subsistemas y servicios como sea necesario.

a) Los subsistemas y servicios deben ser descriptivos y seguir la convención establecida en la guía técnica de implementación de la Plataforma Única de Interoperabilidad.

Sección 6.02. Estándares para la creación de API

Esta sección especifica las directrices a seguir para el desarrollo, diseño, publicación y documentación de Interfaces de Aplicaciones Programables (API, por sus siglas en inglés) de forma que cumplan con las mejores prácticas en el desarrollo de estas aplicaciones.

Las API desarrolladas por o para los organismos gubernamentales deben cumplir con las siguientes directrices:

(a) Las API deben desarrollarse siguiendo el modelo de Transferencia de Estado Representacional (RESTful, por sus siglas en inglés), cumpliendo con las siguientes mejores prácticas:

  (i) Siempre que sea posible debe utilizarse la Notación de Objetos de JavaScript (JSON, por sus siglas en inglés) u otras representaciones basadas en JSON aplicando las siguientes directrices:

    a) Deben formularse las respuestas como un objeto JSON (JSON object, por nombre en inglés) y no como una matriz.

    b) Debe evitarse claves de objeto impredecibles o dinámicas como las derivadas de los datos (object keys, por nombre en inglés).

    c) Debe utilizarse mayúsculas y minúsculas coherentes para las claves de objeto.

(b) Cada verbo debe representar una sola operación en un recurso determinado, de forma que estos no se sobrecarguen.

  (i) Los verbos del Protocolo de Transferencia de Hipertexto (HTTP, por sus siglas en inglés) en el contexto de una API RESTful, deben utilizarse para las siguientes acciones únicamente:

    a) **GET:** recuperar o consultar un recurso.

    b) **POST:** crear un nuevo recurso o iniciar una acción.

c) **PUT:** actualizar o reemplazar un recurso existente.

d) **DELETE:** Para eliminar recursos.

e) **PATCH:** Para editar partes concretas de un recurso.

(c) Debe evitarse el uso de parámetros de solicitud para pasar operaciones adicionales.

(d) Para los datos que se devuelven como parte de una respuesta, deben utilizarse los Identificadores Uniforme de Recursos (URI, por sus siglas en inglés) para identificar de manera única los datos como un recurso, de modo que se puedan realizar operaciones futuras sobre ellos.

(i) Las URIs deben cumplir con los siguientes requisitos:

a) No contener verbos.

b) Identificar únicamente a un recurso.

c) Mantener una jerarquía lógica.

d) Hacer filtrados de información mediante los parámetros HTTP.

e) Especificarse usando su forma plural.

(e) La negociación de contenido debe realizarse mediante el enfoque impulsado por agentes (agent-driven, término en inglés) a través de encabezados HTTP y cumplir con las siguientes directrices:

(i) Los encabezados de solicitud ACCEPT y CONTENT-TYPE deben ser obligatorios.

(ii) El encabezado AUTHORIZATION es obligatorio.

(iii) La clave de API (API Key, término en inglés) debe pasarse en el encabezado en lugar de a través de URI.

(iv) Las claves o tokens de API deben configurarse de forma segura.

(v) La respuesta debe contener el encabezado CONTENT-TYPE.

Subsección 6.02.1. Esquemas de mensajes

Las API deben responder con esquemas de mensajes que sean fáciles de entender y consumir, para este fin se han especificado las siguientes directrices:

(a) Deben evitarse las estructuras de datos sin procesar.

(b) Las API deben abstraer la representación de datos físicos del backend del consumidor.

(c) La exposición de estructuras de datos sin procesar de los sistemas de backend debe limitarse a datos abiertos, informes y API estadísticas únicamente.

  (i) Debe evitarse la creación de estructuras de datos para las respuestas JSON.

(d) Las respuestas, incluidos los mensajes de error, deben abstraer los detalles técnicos a los que el consumidor de API no tiene visibilidad.

(e) Los mensajes de error deben incluir un desglose del error, en donde se especifique:

  (i) El código de error.

  (ii) El mensaje que describa el error.

  (iii) El tipo de error.

  (iv) Una lista de errores, si aplica.

(f) Las respuestas deben estar envueltas por defecto para facilitar la inclusión de metadatos adicionales, tales como paginación, clasificación, filtros, entre otros.

(g) La interacción entre el consumidor y el proveedor de API debe ser sin estado, de forma que las API no tengan que esperar ningún concepto de sesión o gestión de estado por parte del consumidor.

(h) Deben utilizarse los códigos de estado HTTP para APIs RESTful.

Subsección 6.02.2. Diseño de las API

(a) Las API deben diseñarse de tal manera que puedan ser consumidas por los sistemas internos del Gobierno de la República Dominicana, socios confiables y partes externas.

(b) El diseño de las API debe permitir la aplicación de diferentes perfiles de acceso a datos, ya sea a la API o en una capa de proxy, sin la necesidad de crear API adicionales.

(c) Las API deben diseñarse basadas en consulta.

(d) Las API deben crearse en paralelo con un caso de uso interno para su integración.

(e) Debe utilizarse el piloto interno para validar la implementación de la API antes de publicarla para uso externo.

(f) Debe crearse y publicarse nuevas versiones de la API de forma iterativa a medida que cambien los requisitos y/o se introduzcan nuevos.

(g) Debe solicitarse activamente comentarios de los consumidores de API para comprender si la API proporciona el valor adecuado y realice ajustes en futuras iteraciones.

(h) Toda API debe estar versionada.

(i) Para el control de las versiones de aplicaciones debe utilizarse la tecnología de manejo distribuido de versiones GIT.

(j) Cada cambio en una API, por pequeño que sea, debe indicarse con una nueva versión.

(k) Debe seguirse la estructura de control de versiones presentada a continuación:

(i) **Importante:** versión significativa que probablemente rompa la compatibilidad con versiones anteriores.

(ii) **Menor:** adición de atributos opcionales o nueva funcionalidad que es compatible con versiones anteriores, pero debe probarse.

(iii) **Parche:** Corrección interna que no debería afectar el esquema y / o contrato de la API.

Por ejemplo, pasar de la v1.1.0 a la v1.1.1 permitiría una actualización simple de implementación en el lugar, ya que es un parche, mientras que pasar de la v1.1.0 a la v2.0.0 sería un cambio de versión importante y requeriría la versión heredada para mantenerse mientras los consumidores prueban y migran a la nueva versión.

(l) Las versiones no deben pasarse como un parámetro o en el encabezado de la solicitud.

(m) Las URL deben reflejar solo la versión principal del API.

(i) Las versiones secundarias y de parche no necesitan estar en el URL de forma que no se rompa la compatibilidad con versiones menores anteriores.

(n) Debe admitirse al menos una versión principal anterior para garantizar que los sistemas consumidores tengan tiempo de migrar a la última versión de la API.

(i) Cuando se programe la realización de cambios importantes, esta debe notificarse a los consumidores, tomando en cuenta el impacto que pudiera tener.

(ii) El organismo debe elaborar una política de cambio y baja en donde se indiquen los tiempos para las migraciones a nuevas versiones antes de desconectarse las heredadas.

(o) Deben restringirse las consultas con caracteres comodín (wildcard, por su nombre en inglés).

(i) En los casos en los que se permitan caracteres comodín, debe asegurarse de que existan restricciones sobre cuáles y cuántos parámetros puede tener una entrada wildcard.

Los siguientes son algunos patrones comunes para la paginación:

- **page y per_page:** se usa mejor para navegar en grandes conjuntos de datos estáticos (por ejemplo, datos de referencia) donde es probable que se devuelva el mismo conjunto de datos dada la misma referencia de página a lo largo del tiempo.
- **offset y limit:** se utiliza mejor para APIs que se encuentran al frente de backends basados en Lenguaje de Consulta Estructurado (SQL), donde el offset representa el cursor de datos en una columna indexada determinada.
- **since y limit:** se usa mejor para consultas en las que el consumidor está interesado en el delta, ya que la última consulta y la estructura de datos de backend se indexa en función del tiempo.

(p) Las API deben admitir alguna forma de segmentación o filtrado, especialmente cuando exponen grandes conjuntos de datos.

(q) La capacidad de inyectar cadenas de consulta u objetos definidos por el consumidor en una API debe limitarse únicamente a las API de datos abiertos, informes y estadísticas, y estar estrictamente prohibida en las API de datos maestros, transaccionales o comerciales.

(r) Deben restringirse las consultas dinámicas o abiertas, limitando la capacidad de inyectar cadenas de consultas u objetos definidos por el consumidor únicamente a las API de datos abiertos, informes y estadísticas.

Sección 6.03. Aspectos generales de seguridad

En esta sección se abarcan los aspectos generales de seguridad que permiten proteger la confidencialidad, integridad y disponibilidad de los datos. Por tanto, los organismos deben cumplir con lo establecido a continuación:

(a) Los accesos privilegiados a los sistemas deben ser aprobados por la dirección general.

(b) El área de seguridad debe verificar los accesos privilegiados y habilitarlos.

(c) Para el manejo de contraseñas, el organismo debe asegurar que:

(i) Las contraseñas no sean almacenadas en papeles, celulares, medios removibles o cualquier medio a los cuales puedan tener acceso otros usuarios.

(ii) No se deben crear contraseñas que contengan iniciales de nombres, números telefónicos, fechas de nacimientos o cualquier otra información básica que pueda ser descubierta con facilidad.

(iii) Todas las contraseñas de nivel de sistema deben cumplir con las siguientes pautas para su construcción:

a) Tener un mínimo de diez (10) caracteres.

b) Contener en su composición las siguientes clases de caracteres: letras, minúsculas, mayúsculas, número y símbolos (@#$%^&*()+_?>””|?><-).

(iv) Las contraseñas deben ser cambiadas como mínimo cada sesenta (60) días calendario.

(d) El organismo debe asegurarse de que los colaboradores que cuenten con acceso a los sistemas habilitados en la plataforma única de interoperabilidad no realicen las actividades detalladas a continuación:

(i) Acceder a la plataforma para cualquier propósito que no sea para fines de labores que no estén establecidos en la mesa principal, incluso si tiene acceso autorizado.

(ii) Revelar o prestar su cuenta de usuario.

(iii) Ocasionar la interrupción del servicio debido a actualizaciones o mantenimientos no establecidos.

(e) El organismo debe realizar una verificación regular para validar que solo el personal autorizado cuenta con acceso a la plataforma única de interoperabilidad.

(f) El ambiente de producción debe estar separado de los entornos de pruebas.

(g) Se debe hacer uso de VPN para acceder de forma remota a la plataforma única de interoperabilidad.

(h) El organismo debe aplicar Zero Trust a la página de inicio de sesión de la aplicación cuando se publica en internet.

(i) Debe permitirse únicamente el acceso al personal autorizado que estará trabajando con la plataforma única de interoperabilidad.

CAPÍTULO 7

INTEROPERABILIDAD DE LA SALUD

El sector salud es la única excepción a la obligatoriedad del uso de la Plataforma Única de Interoperabilidad (X-ROAD) para el intercambio de datos, imágenes o cualquier otro medio de información sanitaria entre organismos gubernamentales.

Este capítulo establece las directrices obligatorias para la interoperabilidad en el sector salud, asegurando un sistema eficiente, seguro y colaborativo para el intercambio de información sanitaria.

En el caso de salud, es el único ecosistema compuesto, que puede tener escenarios de múltiples plataformas, según el caso de uso:

(a) HL7/FHIR para la interoperabilidad del dato sanitario.

(b) X-ROAD para los casos de interoperabilidad entre órganos rectores.

(c) Blockchain para interoperabilidad con suplidores en temas de medicamentos.

Sección 7.01. Objetivo y alcance

La Arquitectura de Interoperabilidad del Ecosistema de Salud tiene como objetivo principal facilitar el intercambio de información entre los diferentes actores del sistema de salud, con el propósito de mejorar la atención al paciente y la eficiencia del sistema en general.

Sección 7.02. Manejo de información federado

(a) Los organismos de salud deben establecer un protocolo de entendimiento que abarque los contenidos, formatos, diccionarios y aspectos técnicos necesarios para la interoperabilidad.

(b) La interoperabilidad del ecosistema de salud debe contemplar los siguientes componentes:Los organismos gubernamentales deben hacer uso exclusivo de la Plataforma Única de Interoperabilidad para compartir e intercambiar información con otros organismos gubernamentales.

(i) Dominio del concepto de Federación del dato de salud.

(ii) Interoperabilidad organizacional.

(iii) Interoperabilidad jurídica.

(iv) Interoperabilidad semántica.

(v) Interoperabilidad técnica.

Sección 7.03. Estándares universales de interoperabilidad

(a) Todos los organismos del sistema de salud deben adoptar y cumplir con los estándares HL7, los cuales son esenciales para asegurar un intercambio de datos estructurado y estandarizado.

(b) Los estándares HL7 incluyen:

(i) HL7 v.2

(ii) HL7 v.3

(iii) FHIR (Fast Health Interoperability Resources)

(c) El intercambio de datos debe realizarse utilizando formatos como JSON y XML, que permiten la interoperabilidad entre diferentes plataformas.

Sección 7.04. Modelos de interoperabilidad

(a) Los organismos de salud deben implementar uno de los siguientes modelos de interoperabilidad, conforme a sus necesidades y capacidades:

(i) Modelos Descentralizados: Un sistema de archipiélago de datos y conectividad, autosuficiente en sus propios espacios.

(ii) Modelos Centro-Distribuidos: Regionalización del dato con Federación de Datos.

(b) Los datos de salud deben estar federados y cada institución debe tener la capacidad de interoperar en tiempo real con otras entidades del ecosistema.

Sección 7.05. Requisitos específicos para la interoperabilidad de la salud

(a) No debe existir una base de datos centralizada que contenga toda la información sanitaria de los ciudadanos.

(b) No se debe promover un software de atención hospitalaria como herramienta universal obligatoria a nivel nacional.

(c) Cada institución tiene la libertad de contratar servicios de atención de salud que mejor representen sus funciones sanitarias.

(d) Todas las instituciones deben implementar la capa de interoperabilidad HL7/FHIR bajo su sistema de información para intercambiar datos.

(e) Las instituciones del sistema no pueden almacenar registros médicos en servidores externos o en otras instituciones.

(f) La interoperabilidad local o transfronteriza debe recopilar los registros médicos de los pacientes utilizando la plataforma HL7/FHIR, haciéndolos visibles para el médico en la consulta del día.

(g) El acceso a los registros médicos debe hacerse con la autorización explícita del paciente, validada mediante identificaciones que acrediten al paciente como propietario de los datos.

(h) Puede considerarse la creación de una base de datos centralizada para almacenar metadatos con fines estadísticos, de trazabilidad y de control.

Sección 7.06. Estrategias de estandarización

(a) Las estrategias de estandarización deben incluir:

(i) La adopción de HL7 v.2, HL7 v.3 y FHIR.

(ii) La implementación de protocolos como TCP, FTP y HTTP para el intercambio de mensajes HL7.

(b) Los organismos de salud deben seguir las guías y recomendaciones internacionales para la implementación de estos estándares, adaptándose a las necesidades específicas del entorno de salud en la República Dominicana.

Sección 7.07. Supervisión y evaluación

(a) La adopción y aplicación de estos estándares deben ser evaluadas y supervisadas periódicamente para asegurar el cumplimiento y la actualización conforme a las mejores prácticas y avances tecnológicos en el ámbito de la salud.

BIBLIOGRAFÍA

1. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (s.f.). Niveles de Interoperabilidad. Uruguay.

2. Archivo General de la Nación, Gobierno de Colombia. (2015). Guía De Metadatos. Colombia.

3. Archivo Nacional de Australia. (2015). Estándar de Metadatos de Mantenimiento de Registros del Gobierno Australiano. Australia.

4. Consorcio World Wide Web (W3C). (2008). Sintaxis XML Signature y Procesamiento. Segunda Edición. New York.

5. Dirección Distrital de Archivo de Bogotá. (2019). Guía esquema de Metadatos de Bogotá para documentos electrónicos de Archivo - EMBDEA 1.0. Bogotá, Colombia.

6. Dublin Core Metadata Initiative (DCMI). (2005). DCMI Glossary. Dublín.

7. European Telecommunications Standards Institute. (2003). ETSI TR 102 272. Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies. República Francesa.

8. European Telecommunications Standards Institute. (2009). ETSI TS 101 903. XML Advanced Electronic Signatures (XAdES). República Francesa.

9. Gobierno de la Republica Dominicana. (2012). Ley No. 1-12. Ley Orgánica de la Estrategia Nacional de Desarrollo de la República Dominicana 2030. Santo Domingo, Republica Dominicana: Congreso de la República Dominicana.

10. Grupo de Trabajo de Ingeniería de Internet. (1997). Palabras clave para usar en RFC para indicar los niveles de requisitos. RFC 2119. Reston, VA.

11. Le Lous, J., Jean, B., Abdallah, H., & Moulin, C. (2016). Elementos de un Marco de Interoperabilidad Técnica para el Patrimonio Canadiense. Canada.

12. Ministerio de Asuntos Económicos y Transformación Digital, Secretaría de Estado de Digitalización e Inteligencia Artificial y Secretaría General de Administración Digital. (2010). Esquema Nacional de Interoperabilidad. España.

13. Ministerio de Hacienda y Administraciones Públicas. (2012). Norma Técnica de Interoperabilidad de Catálogo de estándares. España.

14. Ministerio de Hacienda y Administraciones Públicas. (2016). Esquema De Metadatos Para La Gestión Del Documento Electrónico (e-EMGDE). España.

15. Network Working Group. (2008). The Transport Layer Security (TLS) Protocol).

16. Organización Internacional de Normalización (ISO). (1986). ISO 8879. Procesamiento de la información - texto y de oficina - sistemas Generalizado Estándar Markup Language (SGML).

17. Organización Internacional de Normalización (ISO). (1994). ISO/IEC 7498-1. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.

18. Organización Panamericana de la Salud. (2021). Introducción a la interoperabilidad semántica. Washington D. C., Estados Unidos.

19. Registros estatales de Australia del Sur. (2015). Mantenimiento de Registros de Australia del Sur. Australia del Sur.

20. Revista Española de Documentación Científica. (2008). Información y documentación - Procesos de gestión de documentos - Metadatos para la gestión de documentos. Parte 1: Principios. ISO 23081-1:2006. España.

21. REVISTA ESPAÑOLA DE DOCUMENTACIÓN CIENTÍFICA. (2008). Procesos de gestión de documentos. Metadatos para. España.

22. Unión Europea. (2017). Marco Europeo de Interoperabilidad. Belgium.

ANEXOS

ANEXO A

CATÁLOGO DE ESTÁNDARES PARA LA INTEROPERABILIDAD

En este anexo se presenta el catálogo de estándares, compuesto por estándares interoperables y sus directrices. El catálogo citado se enfoca en utilizar estándares abiertos y debe ser utilizado para los servicios que requieran interoperabilidad con entidades no gubernamentales y que, por tanto, no puedan operar sobre la plataforma única de interoperabilidad.

USO DEL CATÁLOGO

(a) Todo nuevo servicio de tipo electrónico que desarrolle un organismo gubernamental debe estar alienado a los estándares especificados y permitidos en el capítulo 4. Interoperabilidad técnica.

(b) Debe seleccionarse del catálogo aquellos estándares que se ajusten a las necesidades o funcionalidades que se implementará.

(c) En caso de utilizar un estándar no especificado en el catálogo, debe enviarse la justificación de uso al correo certificacionnortic@ogtic.gob.do para evaluar el requerimiento.

(d) Los estándares y tecnologías definidos en el segmento de integración de aplicaciones y servicios deben ser los utilizados en cualquier sistema o programación que intervenga en la integración de aplicaciones y/o servicios.

ESTRUCTURA DEL CATÁLOGO

La estructura del catálogo se realizó en base a categorías y segmentos de interoperabilidad que engloban los diferentes estándares. Los segmentos de interoperabilidad están definidos como sigue a continuación:

(a) Infraestructura y conectividad: se refiere al segmento donde se encuentran los estándares tecnológicos utilizados para interconexión y

comunicación de los servidores internamente y para los clientes a los que prestan servicios.

(b) **Integración de datos:** se refiere al segmento en donde se encuentran todos los estándares tecnológicos utilizados para obtener los modelos necesarios que permiten lograr la interoperabilidad entre sistemas heterogéneos y no heterogéneos, basados en estándares de integración.

(c) **Integración de aplicaciones y servicios:** se refiere al segmento en donde se realiza o se ejecuta el software o algoritmo necesario para lograr la comunicación entre aplicaciones y/o servicios de forma unidireccional o bidireccional.

(d) **Accesibilidad y seguridad:** se refiere al segmento en donde se expresan las tecnologías, metodologías y protocolos necesarios para garantizar el acceso coherente por parte del usuario final, así como la seguridad de la transferencia de la información que viaja desde el motor de procesamiento de datos hasta la interfaz de usuario y viceversa.

Las categorías y sus respectivas subcategorías establecidas para el catálogo de estándares son las definidas a continuación:

(e) **Autenticación:** estándares para la verificación de la identidad digital del remitente de una comunicación a través de la red.

- **(i)** **Certificados:** estándares de certificados electrónicos.
- **(ii)** **Firma electrónica:** estándares para firma electrónica.
- **(iii)** **Política de firma electrónica:** estándares para políticas de creación y validación de firma electrónica.

(f) **Cifrado de datos:** estándares para aumentar la seguridad de un mensaje o de un archivo mediante el cifrado del contenido.

(g) **Codificación:** estándares de codificación de la información.

- **(i)** **Codificación de caracteres:** formatos de codificación del lenguaje natural a lenguaje de máquina para los documentos.

(ii) **Idioma:** estándares de internacionalización y de codificación de idiomas.

(h) Control de acceso: estándares de gestión de accesos a los activos de información.

(i) Integridad: algoritmos de función hash criptográfica para la verificación de la integridad de los datos que son transferidos entre sistemas.

(j) Métricas: estándares de medidas y métricas.

(k) Protocolos de comunicación: estándares de conexión, comunicación y transferencia de información.

(i) **Servicios web:** protocolos y estándares para el intercambio de datos entre aplicaciones web.

(ii) **Tecnologías de transporte y red:** protocolos de comunicación de red definidos en las capas de transporte y red del modelo OSI.

Para información sobre las diferentes capas que componen el modelo OSI, ver anexo B. Capas del modelo OSI.

(l) Semántica: estándares para lograr la comprensión e interpretación de la información, y su reutilización por diferentes sistemas de información sean estos heterogéneos o no.

(i) **Metadatos:** estándares para la descripción de los datos intercambiados.

(ii) **Tecnologías semánticas:** estándares para la representación semántica de la información.

(m) Tecnologías de integración de datos: estándares para la integración de datos que intervienen en un proceso de intercambio de información.

(n) **Tecnologías para identificación:** técnicas de identificación normalizadas de recursos y localizaciones.

Cada estándar en el catálogo constará de los siguientes campos informativos:

(o) **Nombre:** denominación del estándar.

(i) **Nombre común:** forma habitual de nombrar el estándar.

(ii) **Nombre formal:** nombre correspondiente a la especificación formal del estándar.

(p) **Tipo: el cual puede ser:**

(i) **Abierto:** es una especificación disponible públicamente para lograr una tarea específica, el cual tiene varios derechos de uso asociados a este. Además, puede tener varias propiedades de cómo fue diseñado.

(ii) **Propietario:** son aquellos que para su uso requiere pago por el derecho de propiedad y están sustentados y protegidos con patentes o derecho de autor. Normalmente se restringe la aplicación de ingeniería inversa a este tipo de formato.

(q) **Versión mínima aceptada:** versión a partir de la cual debe utilizarse el estándar.

(r) **Extensión(es):** listado de extensiones relacionados con la extensión.

(s) **Estado:** condición en la que se encuentra el estándar, la cual puede ser:

(i) **Estable:** se encuentra en su versión final.

(ii) **En proceso:** estándar cuyo desarrollo continúa en proceso.

ACTUALIZACIÓN DEL CATÁLOGO

Para lograr el óptimo mantenimiento del Catálogo de Estándares, este se actualizará anualmente y en cada actualización se realizarán las siguientes actividades:

(a) Eliminar aquellos estándares que se encuentren en uno de los siguientes estados:

(i) En abandono, que ya no están siendo actualizados por las compañías u organizaciones creadoras.

(ii) Obsoletos, los cuales se utilizan en algunas aplicaciones, pero no son recomendados para implementaciones tecnológicas.

a) Esta conllevará a la selección de un estándar que sustituya la funcionabilidad cubierta por el estándar obsoleto.

(b) Revisar el resto de los estándares del catálogo, actualizando sus versiones e identificando cuáles estándares se encuentran en estado de "abandono", para que en dicho caso se defina un periodo máximo de uso.

(c) Identificar nuevos estándares a incluir en el catálogo.

(d) Documentar los cambios introducidos para facilitar su localización por parte de los organismos.

ANEXO B

ABREVIATURAS Y ACRÓNIMOS

No.	Abreviaturas y Acrónimos	Inglés	Español
1	API	Application Programming Interface	Interfaz De Programación De Aplicaciones
2	CIGETIC	NA	Comité de implementación y Gestión de Estándares TIC
3	DCAT	Data Catalog Vocabulary	Vocabulario para Catálogo de Datos
4	EIF	European Interoperability Framework	Marco Europeo de Interoperabilidad
5	FHIR	Fast Healtchcare Interoperability Resource	Recurso Rápido de Interoperabilidad Sanitaria
6	HTML	Hyper Text Markup Language	Lenguaje de Marcas de Hipertexto
7	HL7	Health Level Seven	Nivel De Salud Siete
8	HTTP	Hypertext Transfer Protocol	Protocolo de Transferencia de Hipertexto

9	JSON	JavaScript Object Notation	Notación de Objetos de JavaScript
10	N/D	NA	No Disponible
11	NIEM	National Information Exchange Model	Modelo De Intercambio De Información Nacional
12	NORTIC	NA	Normas sobre Tecnologías de la Información y Comunicación
13	OGTIC	NA	Oficina Gubernamental de Tecnología de la Información y Comunicación
14	REST	Representational State Transfer	Transferencia de Estado Representacional
15	SOAP	Simple Object Access Protocol	Protocolo de Acceso a Objetos Simple
16	SQL	Structured Query Language	Lenguaje De Consulta Estructurada
17	TIC	NA	Tecnología de la Información y comunicación
18	URI	Uniform Resource Identifier	Identificador Uniforme de Recursos
19	URL	Uniform Resource Locator	Localizador de Recurso Uniforme
20	URN	Uniform Resouce Names	Nombre de Recurso Uniforme
21	UTF-8	8-bit Unicode Transformation Format	Formato de Transformación Unicode de 8-bit
22	XHTML	eXtensible HyperText Markup Language	Lenguaje de Marcas de Hipertexto Extensible

ANEXO C

REFERENCIAS NORMATIVAS

Para la redacción de esta normativa se utilizaron como marco y soporte de los diferentes capítulos, las siguientes referencias listadas a continuación en conjunto con la documentación citada en el apartado Referencias Bibliográficas de este documento:

1. Conjunto de estándares ISO 639, de la Organización Internacional de Normalización (ISO, por sus siglas en inglés), concerniente a la representación de los nombres y grupos de idiomas. De la misma manera se utilizó la norma ISO 8601, que especifica la notación estándar para la representación de fechas y horas.

2. Lineamientos para el desarrollo de Interfaces de Programación de Aplicaciones (APIs) del gobierno canadiense basado en las especificaciones de OpenAPI.

3. Glosario del Modelo de Metadatos del Gobierno de Dublín (DCMI, por sus siglas en inglés), el cual se dedica a fomentar los estándares interoperables de los metadatos y promueve el desarrollo de los vocabularios especializados de metadatos para describir recursos.

4. El Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE) y el Australian Government Recordkeeping Metadata Standard (AGRkMS, por sus siglas en inglés) de los cuales se han extraído y adaptado únicamente aquellos componentes que no tienen sentido en el ámbito nacional, e incorporando los componentes necesarios para hacerlo compatible con los requisitos de la normativa.

5. El Marco Europeo de Interoperabilidad (EIF, por sus siglas en inglés), el cual ofrece orientación, a través de un conjunto de recomendaciones, a las administraciones públicas sobre cómo mejorar la gobernanza de sus actividades de interoperabilidad, establecer relaciones entre organizaciones, simplificar los procesos que respaldan los servicios digitales de un extremo a otro y garantizar que la legislación existente y nueva lo hagan, comprometiendo los esfuerzos de interoperabilidad.

6. El Esquema Nacional de Interoperabilidad de España, el cual establece los principios y directrices de interoperabilidad en el intercambio y conservación de la información electrónica por parte de Administraciones Públicas.

EQUIPO DE TRABAJO

Ministerio de Administración Pública (MAP)

Lic. Darío Castillo Lugo, Ministro

Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

Bartolomé Pujals, Director General

Diana Rivas, Directora de Gabinete

Edwin Rodríguez, Director de Transformación Digital Gubernamental

Elupina Almonte, Encargada del Departamento de Normas y Estándares

Enyer Pérez, Encargado de División de Investigación y Documentación de Normas

Carlos Guerrero, Analista de Normas y Estándares

Jason Crisóstomo, Encargado División de Implementación de Normas

Leonardo Ceppi, Auditor de Normas y Estándares

Gisselle Tavera, Directora Jurídica

Miguel Vargas, Encargado de Elaboración de Documentos Legales

Camila Beato, Directora de Planificación y Desarrollo

Genry Lizardo, Asesor

Ivan Firestone, Director de Arquitectura Gubernamental Digital

Kevin Jiménez, Desarrollador de Sistemas

Manuel Mayrele, Director de Servicios Digitales Institucionales

José Estevez, Encargado de Seguridad y Monitoreo TIC

Agradecimientos

Emmanuel Reyes, pasado Encargado de División de Auditoría y Monitoreo de Normas

Para visualizar y descargar este documento leer este código

Ave. Rómulo Betancourt #311, Edificio Corporativo Vista 311,
Bella Vista, Sto. Dgo., R.D.
Tel.: 1+ 809.286.1009 | info@ogtic.gob.do
www.ogtic.gob.do | www.gob.do

@OGTICRD @OGTICRDO