NORTIC A4 2022

NORMA PARA LA INTEROPERABILIDAD ENTRE LOS ORGANISMOS DEL ESTADO DOMINICANO

Santo Domingo, República Dominicana
Diciembre 2022

ogtic

GOBIERNO DE LA REPÚBLICA DOMINICANA

NORTIC A4:2022
NORMA PARA LA INTEROPERABILIDAD ENTRE LOS ORGANISMOS DEL ESTADO DOMINICANO

Edición: 1era
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

Dirección de Transformación Digital Gubernamental
Departamento de Normas y Estándares

Año de publicación: 2022
Versión 2.0

Diagramado y Diseñado por la Dirección de Comunicaciones, OGTIC.
Impreso en República Dominicana

CONTENIDO

CAPÍTULO 4

CAPÍTULO 5

PRÓLOGO

El Presidente Luis Abinader se ha propuesto la aspiración de que la República Dominicana logre alcanzar una transformación sistémica, que la convierta en uno de los países más prósperos y competitivos del mundo.

Para esto ha puesto en marcha la Estrategia Nacional de Competitividad, acompañada de un proceso de reformas y programas, dentro de los que se encuentra el Programa Burocracia Cero, coordinado por el Ministerio de la Administración Pública (MAP), el apoyo de la Oficina Gubernamental de las Tecnologías de la Información y Comunicación (OGTIC), bajo la dirección ejecutiva del Consejo Nacional de Competitividad (CNC).

El Programa Burocracia Cero tiene por objetivo elevar la eficiencia del gobierno a través de la implementación de reformas que permitan reducir las trabas regulatorias fomentando así el aumento de la productividad de los ciudadanos y las empresas, además de generar un entorno favorable para la inversión y la creación de empleos.

Este programa ha priorizado 157 trámites y servicios que deberán ser intervenidos en este 2022, dentro de los que se encuentran 10 proyectos, 4 de los que corresponden a ventanillas únicas de servicios, sin embargo, el éxito de estas ventanillas depende no solo de la voluntad de las instituciones involucradas, sino de la capacidad de interoperabilidad que deben contener los sistemas tecnológicos de las instituciones. Es en este sentido que reviste vital importancia que el país adopte un marco normativo para la Interoperabilidad entre los Organismos del Gobierno Dominicano.

La NORTIC A4, que hoy presentamos establece las directrices que deben seguir las instituciones a fin de lograr el intercambio de información de manera efectiva entre diferentes sistemas de los órganos que componen la administración pública.

Sin dudas poder implementar esta norma de interoperabilidad en el Estado Dominicano ayudará a reducir los trámites burocráticos y costos, garantizando una mayor eficiencia y calidad de los servicios públicos. Estos avances sin duda alguna tendrán impacto positivo en la disminución de las trabas del país para incrementar sus niveles de competitividad, acercándonos cada vez más a la aspiración de nuestro Presidente de lograr de la República Dominicana un país más competitivo.

Lic. Dario Castillo Lugo
Ministro
Ministerio de Administración Pública (MAP)

Lic. Pedro Quezada
Director General
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

Peter Albert Prazmowski
Director Ejecutivo
Consejo Nacional de Competitividad

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), creado mediante el Decreto Núm. 1090-04 del 3 de septiembre del 2004 y su modificación en el decreto Núm. 54-21 del 2 de febrero del 2021, como organismo desconcentrado 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.

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 regurarizaión y estándarización 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), las cuales fueron creadas y están en proceso de implementación desde el año 2013, siendo concebidas para sistematizar, estandarizar y tener una herramienta efectiva de auditoría para el correcto uso e implementación de las TIC en la administración pública, con el objetivo de crear ciclos de mejora continua de los procesos de los organismos 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 de esto, atendiendo a los nuevos avances tecnológico y como un fomento a la continuidad de la modernización del Estado, la OGTIC ha realizado una revisión y actualización a esta norma publicando su segunda versión en la NORTIC A4:2022, orientada a lograr interoperabilidad entre organismos, permitiendo así el intercambio de información de una manera efectiva y segura entre los diferentes sistemas de los órganos que componen la administración pública.

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 presentados a continuación:

1. P1. Para el tratamiento de los derechos sobre la protección de datos personales, esta norma se ampara en la propia **Constitución de la República Dominicana** del 26 de enero de 2010.

    - Artículo 44.- Derecho a la intimidad y el honor personal. Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto:

- 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. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.

- Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley.

- El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley.

2. La **Ley 200-04,** sobre el Libre Acceso a la Información Pública, que establece la implementación de la sección "Transparencia" en los portales del Gobierno Dominicano.

- Artículo 5.- Se dispone la informatización y la incorporación al sistema de comunicación por Internet o a cualquier otro sistema similar que en el futuro se establezca, de todos los organismos públicos centralizados y descentralizados del Estado, incluyendo el Distrito Nacional y los municipios, con la finalidad de garantizar a través de este, un acceso directo del público a la información del Estado. Todos los poderes y organismos del Estado deberán instrumentar la publicación de sus respectivas "páginas web" a los siguientes fines:

    - Difusión de información: Estructura, integrantes, normativas de funcionamiento, proyectos, informes de gestión, base de datos;

    - centro de intercambio y atención al cliente o usuario: Consultas, quejas y sugerencias;

    - trámites o transacciones bilaterales;

    - la información a que hace referencia el párrafo anterior será de libre acceso al público sin necesidad de petición previa.

- Artículo 6.- La administración pública, tanto centralizada como descentralizada, como cualquier otro órgano o entidad que ejerza funciones públicas o ejecute presupuesto público, y los demás entes y órganos mencionados en el Artículo 1 de esta ley, tienen obligación de proveer la información contenida en documentos escritos, fotografías, grabaciones, soportes magnéticos o digitales, o en cualquier otro formato, y que haya sido creada u obtenida por ella o que se encuentre en su posesión y bajo su control.

- Artículo 11.- La información solicitada podrá ser entregada en forma personal, por medio de teléfono, facsímile, correo

ordinario, certificado o también correo electrónico[1], o por medio de formatos disponibles en la página de Internet que al efecto haya preparado la administración a la que hace referencia el Artículo 1 de esta ley.

- Artículo 24.- Las entidades o personas que cumplen funciones públicas o que administren recursos del Estado deberán prever en sus presupuestos las sumas necesarias para hacer publicaciones en los medios de comunicación colectiva, con amplia difusión nacional, de los proyectos de reglamentos y actos de carácter general, a los que se ha hecho referencia en el artículo anterior.

    - Párrafo.- En los casos en que la entidad o persona correspondiente cuente con un portal de Internet o con una página en dicho medio de comunicación, deberá prever la existencia de un lugar específico en ese medio para que los ciudadanos puedan obtener información sobre los proyectos de reglamentación, de regulación de servicios, de actos y comunicaciones de valor general, que determinen de alguna manera la forma de protección de los servicios y el acceso de las personas de la mencionada entidad. Dicha información deberá ser actual y explicativa de su contenido, con un lenguaje entendible al ciudadano común.

    - Debe publicarse el contenido utilizando medios tecnológicos que garanticen la autenticidad de la información, tales como certificados digitales.

3. La **Ley 53-07,** contra Crímenes y Delitos de Alta Tecnología.

    - Artículo l.- Objeto de la Ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de la información y comunicación, y su contenido, así como

[1] *Es un servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.*

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. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de estos, las transacciones y acuerdos comerciales o de cualquier otra índole que se llevan a cabo por su medio y la confidencialidad de estos, son todos bienes jurídicos protegidos.

4. La **Ley 1-12,** sobre estrategia nacional de desarrollo.

    - Artículo 16.- En el diseño y ejecución de los programas, proyectos y actividades en que se concretan las políticas públicas, deberá promoverse 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.

5. 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.

    - 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, que se concreta, entre otros, en los siguientes derechos subjetivos de orden administrativo:

        - Derecho a no presentar documentos que ya obren en poder de la administración pública o que versen sobre hechos no controvertidos o no relevantes.

- Artículo 27. Actos de instrucción o investigación. Los actos de instrucción o investigación podrán consistir, entre otros, en los siguientes medios:
    - Párrafo I. Las actuaciones para la obtención y tratamiento de la información necesaria para adoptar una decisión bien informada podrán consistir en cualquier medio, como la cooperación, asistencia e intercambio de información con otras administraciones competentes, o las consultas a los expertos. En los términos establecidos en la legislación o en convenios internacionales, podrá recabarse la colaboración informativa de otras agencias y administraciones especializadas de otros Estados, o de organismos internacionales, al objeto de adoptar la decisión mejor informada, al servicio de los intereses generales.

6. La **Ley 126-02,** sobre Comercio Electrónico, Documentos y Firma Digital.

7. La **Ley 167-21,** sobre la mejora regulatoria y simplificación de trámites. Establece una serie de lineamientos y atribuciones, en relación con interoperabilidad:

    - Artículo 34 - Interoperabilidad de los sistemas de información. 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, en su calidad de órgano rector:
        - Párrafo: La Oficina Gubernamental de Tecnología 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.

8. El **Decreto 1090-04,** a través del cual se constituye la Oficina Gubernamental de las Tecnologías de la Información y Comunicación (anteriormente Oficina Presidencial de las Tecnologías de la Información y Comunicación) como dependencia directa del poder ejecutivo, donde se establece lo siguiente:

    - 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.

    - 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.

    - 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.

- 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.

9. El **Decreto 229-07,** ratifica las funciones que ya le habían sido dadas a la OGTIC y se le atribuye lo siguiente:

    - Artículo 3.- El Centro de Contacto Gubernamental estará a cargo de la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), institución con la responsabilidad de la implementación y el desarrollo del Gobierno Electrónico en la República Dominicana, y encargada de coordinar, entre todas las instituciones gubernamentales, la estrategia y la ejecución de la Agenda Nacional de Gobierno Electrónico.

10. El **Decreto 709-07,** sobre las normas y estándares elaboradas por la OPTIC.

    - Artículo 1.- Se instruye a toda la administración Pública del Estado Dominicano a cumplir con las normas y los estándares tecnológicos para: (i) el desarrollo de portales gubernamentales, (ii) conectividad interinstitucional, (iii) interoperabilidad tecnológica, (iv) de seguridad, auditoria e integridad electrónica, (v) digitalización de documentos, así como cualquier otra normativa que sea redactada, aprobada y coordinada por la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), en materia de Tecnología de la Información y Comunicación (TIC) y Gobierno Electrónico.

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

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

13. El **Decreto 92-22**, que establece el Marco Nacional de Interoperabilidad Gubernamental.

    - Artículo 5. Responsabilidades. El Marco Nacional de Interoperabilidad recae bajo la rectoría del Ministerio de la Administración Pública (MAP), y la ejecución de la Oficina Gubernamental de Tecnologías de la Información (OGTIC). Sus responsabilidades se distribuyen 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) Placer uso de la Plataforma Única de Interoperabilidad garantizando unadecuado 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.

14. El **Decreto 707-22,** para la ejecución del Programa Gobierno Eficiente (Burocracia Cero).

- Artículo 7.- Con el propósito de lograr el cumplimiento del Programa Gobierno Eficiente (Burocracia Cero), se instruye lo siguiente:

b) A todos los entes y órganos de la Administración pública bajo la dependencia del Poder Ejecutivo en sentido general:

ii. 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).

INTRODUCCIÓN

La Norma para la Interoperabilidad entre los Organismos del Estado dominicano establece las directrices que deben seguir los organismos a fin de lograr el intercambio de información de manera efectiva entre diferentes sistemas de información de los entes que componen la administración pública. La interoperabilidad en el Estado Dominicano busca reducir los trámites burocráticos, costos y esfuerzos implicados en la prestación de los sevicios públicos, tanto de parte de los organismos como por parte del ciudadano en su consumo, garantizando una comunicación sin barreras entre todos los actores asociados e incrementando así la satisfacción y calidad de los servicios brindados.

Para dar a los lectores y a quienes apliquen esta normativa un entendimiento común sobre el término interoperabilidad, en esta se define como la capacidad de las organizaciones, sus sistemas de información y los procesos que los soportan, de interconectarse con el objetivo de intercambiar y compartir datos e informaciones de forma ética, segura y eficiente, bajo un marco de transparencia, que permita obtener beneficios entre los entes involucrados. En consonancia con esta definición, esta norma abarca 4 dimensiones de la interoperabilidad esenciales para su

implementación, las cuales son; interoperabilidad legal, interoperabilidad organizacional, interoperabilidad semántica e interoperabilidad técnica. Cada una de estas dimensiones es abarcada en los diferentes capítulos de esta norma, conteniendo en cada uno las directrices y lineamientos específicos para cada dimensión.

En esta norma, desde el primer capítulo se presenta su alcance, el cual abarca todos los organismos del Estado dominicano de manera mandatoria, tanto para aquellos que están físicamente dentro del territorio dominicano, como para aquellos organismos que se encuentran fuera, como las embajadas, consulados y misiones en el extranjero y, de manera referencial, para los demás poderes del Estado.

Con el objetivo de facilitar la búsqueda de estándares permitidos en la normativa, en el capítulo 2 se ha actualizado el catálogo de estándares interoperables. En dicho capítulo se describen todos los elementos que conforman el catálogo, mostrando una breve descripción de su ciclo de vida, consideraciones relativas a la formación, categorización y requisitos de uso de los estándares especificados, al igual que una descripción del proceso de revisión y actualización llevado acabo.

El capítulo 3 trata la interoperabilidad legal y organizacional, en donde especifican las directrices que deben ser aplicadas por el organismo a los fines de asegurar una coordinación apropiada de las actividades contenidas en la implementación de la interoperabilidad bajo el marco legal que le compete a cada organismo gubernamental y definido para la protección de los datos personales, así como la alineación de sus procesos de negocio, responsabilidades y expectativas en la consecución de un objetivo común. Además, se definen los roles que debe poseer la unidad de administración de proyecto del departamento de TIC y la definición de elementos como el acuerdo de colaboración interinstitucional para la generación de documentación legal y organizacional necesaria en la ejecución del proyecto, complementado con la definición de informes técnicos, donde se describan los acuerdos operacionales y procedimientos de manejo del cambio.

El capítulo 4 aborda la interoperabilidad semántica, en donde se especifican las directrices para la descripción de los servicios y los esquemas de datos y metadatos[1] para la información intercambiada entre los diferentes sistemas informáticos de los organismos, garantizando con esto el correcto entendimiento y aplicación de dicha información.

Para el capítulo final sobre interoperabilidad técnica, se establecen los lineamientos para el uso de la Plataforma Única de Interoperabilidad y para el desarrollo de 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.

[1] *Son un conjunto de información que describe las características de otra información. Es "datos sobre datos".*

CAPÍTULO 1

NORMA TÉCNICA DE INTEROPERABILIDAD EN EL ESTADO DOMINICANO

Esta norma indica las directrices y recomendaciones que debe seguir cada organismo del Estado dominicano para asegurar y garantizar la capacidad de los sistemas de intercambio de información y de los procesos a los que estos dan soporte, de compartir e intercambiar datos e información entre ellos.

Este conjunto de directrices y recomendaciones persigue la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad legal, organizacional, semántica y técnica de los sistemas y aplicaciones empleadas por los organismos del Estado dominicano

Sección 1.01. Alcance

Las directrices de esta norma deben ser aplicadas por todos los organismos pertenecientes al Poder Ejecutivo, ya sean centralizados, descentralizados, o embajadas, consulados y misiones en el extranjero.

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 organismos pertenecientes a los demás Poderes del Estado, así como aquellos que entran dentro de la clasificación de "Organismos Especiales", según el Ministerio de Administración Pública (MAP), también pueden implementar los estándares indicados en esta norma como un modelo de buenas prácticas, en apoyo a la estandarización del Estado Dominicano.

Sección 1.02. 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:

- 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, la cual especifica la notación estándar para la representación de fechas y horas.

- Lineamientos para el desarrollo de Interfaces de Programación de Aplicaciones[1] (APIs) del gobierno canadiense basado en las especificaciones de OpenAPI[2].

- Glosario del Modelo de Metadatos del Gobierno de Dublín (DCMI, por sus siglas en inglés), el cual se dedica a fomentar

[1] *Es un conjunto de herramientas, definiciones y protocolos que se utiliza para integrar los servicios y el software de aplicaciones.*

[2] *Es un estándar para la descripción de las interfaces de programación (API) por excelencia el cual establece un marco común sobre cómo construir y mantener APIs.*

los estándares interoperables de los metadatos y promueve el desarrollo de los vocabularios especializados de metadatos para describir recursos.

- El Esquema de Metadatos para la Gestión del Documento Electrónico[3] (e-EMGDE) y el Australian Government Recordkeeping Metadata Standard[4] (AGRkMS, por sus siglas en inglés) de los cuales se han extraido 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.

- 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.

- 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.

[3] *El e-EMGDE Incluye los metadatos mínimos obligatorios, definidos en las normas técnicas de interoperabilidad de Documento electrónico y Expediente electrónico de España, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos.*

[4] *Describe información sobre registros y el contexto en el que se capturan y utilizan en las agencias del gobierno australiano. El estándar está diseñado para ser utilizado como una herramienta por el personal involucrado en la gestión de información y registros, gestión de datos e información y comunicación.*

Sección 1.03. Historial de cambios

En la actualización de la NORTIC A4 correspondiente al año 2022, se llevaron a cabo los siguientes cambios respecto a su versión del año 2014:

No.	Capítulo	Detalle
1	**Capítulo I**	Se creó la sección 1.05 sobre Principios de Interoperabilidad, para especificar los fundamentos sobre los cuales se impulsan las acciones de interoperabilidad. Se modificó el nombre de la sección 1.06 Conceptos Generales por Dimensiones de la Interoperabilidad, definiendo en qué consisten cada una de las dimensiones abarcadas por esta norma.
2	**Capítulo II**	Se actualizó el Catálogo de Estándares.
3	**Capítulo III**	Fueron eliminadas las secciones 3.03 y 3.04 Gestión de Procesos Interorganizacionales y Gestión de Procesos Interorganizacionales respectivamente y se modificó el nombre de la sección 3.01 Gestión Organizacional por Colaboración Interinstitucional, adaptando su contenido a los nuevos lineamientos de la NORTIC A4. Se creó la subsección 3.01.1 Acuerdo de Colaboración Interinstitucional en donde se detalla los aspectos con los que debe contar dicho acuerdo y la documentación complementaria. Se actualizaron los roles para la gestión de los proyectos de interoperabilidad, incluyendo dos roles adicionales para el manejo de la Plataforma Única de Interoperabilidad y se agregaron acciones para la resolución de conflictos entre los organismos involucrados en dichos proyectos. Fue creada la sección 3.04 Desarrollo y Robustecimiento de Interoperabilidad, de manera que el organismo tome acciones proactivas y planificadas en busca de mejoras continuas para sus operaciones haciendo uso de la interoperabilidad.

4	**Capítulo IV**	Se actualizaron los metadatos propuestos.
5	**Capítulo V**	Se realizaron cambios a la estructura y al contenido del capítulo, agregando lineamientos para el uso de la Plataforma Única de Interoperabilidad, para el desarrollo de APIs. Adicional, se actualizaron los lineamientos técnicos en cuanto a los protocolos de intercambio de información y formatos digitales que deben ser utilizados en el desarrollo e implementación de toda solución tecnológica en cada organismo.

Sección 1.04. Términos y definiciones

Para fines de esta norma el término "Organismo gubernamental" será utilizado en ciertos casos como "Organismo".

Cuando aparezca el término "Catálogo" este hará referencia al "Catálogo de estándares" descrito en el capítulo II.

En el caso del término "Interorganizacional" hace referencia a cualquier actividad que se realiza en conjunto con otros organismos.

Los términos "Software", "Aplicaciones", "Sistemas" y "Sistemas de información", 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 1.05. Principios de interoperabilidad

Los principios de interoperabilidad son aspectos de comportamiento fundamentales para impulsar las acciones de interoperabilidad. Esta sección establece los principios generales de interoperabilidad que son relevantes para el proceso de establecimiento de servicios interoperables.

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

- **Transparencia:** principio que permite:
  - 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.
  - Asegurar la disponibilidad de interfaces con los sistemas de información internos. Los organismos operan un gran número de sistemas de información heterogéneos y dispares en apoyo de sus procesos internos, por lo tanto, el éxito de la interoperabilidad depende de que se garantice la disponibilidad de interfaces a dichos sistemas y los datos que manejan, de forma que se facilite su reutilización permitiendo a estos integrarse en sistemas más grandes.
  - Asegurar el derecho a la protección de datos personales.
- **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 apliquen ciertas restricciones.
- **Neutralidad tecnológica:** garantizando que los organismos gubernamentales se centren en las necesidades funcionales con el fin de minimizar las dependencias tecnológicas, para evitar imponer implementaciones técnicas que no 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.
- **Seguridad y Privacidad:** los ciudadanos y las empresas deben tener la certeza de que cuando interactúan con un organismo gubernamental lo hacen en un entorno seguro y de confianza y

en pleno cumplimiento de las leyes. El organismo debe garantizar la privacidad, confidencialidad, autenticidad, integridad y no repudio de la información facilitada por ciudadanos y empresas, así como la intercambiada entre diferentes organismos.

Sección 1.06. Dimensiones de la interoperabilidad

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 realizan el intercambio de información mediante procesos de interoperabilidad ajustados a marco jurídico existente.

2. Interoperabilidad organizacional.

Dimensión de la interoperabilidad relativa a la capacidad de los organismos y de los procesos que estos manejan para alcanzar de manera mutua una colaboración para el logro de intercambio de información a través de acuerdos realizados con anterioridad relacionados a los servicios que estos ofrecen. La interoperabilidad organizativa involucra todos los aspectos esenciales de los organismos; entre ellos se destacan:

- La estructura del organismo.
- Los procesos.
- La cultura del personal.

El fin de esta dimensión es definir los objetivos y facilitar la colaboración entre organismos que desean intercambiar información, los cuales pueden tener estructuras organizativas y procesos internos diferentes. Para fines de esta normativa, dentro de la dimensión organizacional se han incluido los aspectos legales que deben ser tomado en cuenta durante todo el proceso de implementación de la interoperabilidad y la gestión organizacional entre los entes involucrados.

3. Interoperabilidad semántica.

Dimensión de la interoperabilidad que se encarga de que la información intercambiada entre los diferentes sistemas de información 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 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:

- Interoperabilidad semántica para la visualización.
- Interoperabilidad semántica para el procesamiento.

4. Interoperabilidad técnica.

Esta dimensión comprende aspectos estrictamente técnicos y tecnológicos que deben ser tomados en cuenta a la hora de 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.

CAPÍTULO 2

CATÁLOGO DE ESTÁNDARES DE INTEROPERABILIDAD

En este capítulo se presenta el catálogo de estándares interoperables, mediante el cual se busca facilitar a los organismos el desarrollo de sistemas de intercambio de información que cumplan con los principios de la interoperabilidad presentando alternativas basadas en estándares abiertos que habilitan la independencia tecnológica de los sistemas; junto a este catálogo se incluyen las directrices que rigen su uso.

El catálogo citado se enfoca en presentar estándares abiertos[1], mostrando una breve descripción de su ciclo de vida, consideraciones relativas a la formación, categorización y requisitos de uso de los estándares recogidos en este, al igual que una descripción de su proceso de revisión y actualización.

Sección 2.01. 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 5. Interoperabilidad técnica.**

[1] *Hace referencia a formatos que permiten su uso y manipulación libremente.*

(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 que no se encuentre especificado en el catálogo, debe enviarse la justificación de uso al correo certificacionnortic@ogtic.gob.do para fines de evaluación del requerimiento.

(d) Cada organismo gubernamental que funcione como cliente o consumidor de un servicio electrónico, brindado por un organismo normalizado bajo la NORTIC A4, debe seguir los estándares seleccionados por el organismo emisor del servicio en cuestión.

(e) 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. Ver **sección 2.03. Catálogo de estándares interoperables.**

Sección 2.02. Estructura del catálogo

El catálogo está compuesto únicamente por estándares interoperables. 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:

- **Infraestructura y conectividad:** se refiere al segmento en donde se encuentran todos los estándares tecnológicos utilizados para lograr la interconexión y comunicación de los servidores internamente y para los clientes a los que estos brindan servicios.
- **Integración de datos:** se refiere al segmento en donde se encuentran todos los estándares tecnológicos utilizados

para lograr los modelos necesarios que permiten lograr la interoperabilidad entre sistemas heterogéneos y no heterogéneos, basados en estándares de integración.

- **Integración de aplicaciones y servicios:** se refiere al segmento en donde se realiza o se ejecuta el software o algoritmo[2] necesario para lograr la comunicación entre aplicaciones y/o servicios de forma unidireccional o bidireccional.

- **Accesibilidad y seguridad:** se refiere al segmento en donde se expresan las tecnologías, metodologías y protocolos[3] 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[4] hasta la interfaz de usuario[5] y viceversa.

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

- **Autenticación:** estándares para la verificación de la identidad digital del remitente de una comunicación a través de la red.
    - **Certificados:** estándares de certificados electrónicos.
    - **Firma electrónica:** estándares para firma electrónica.
    - **Política de firma electrónica:** estándares para políticas de creación y validación de firma electrónica.
- **Cifrado de datos**[6]**:** estándares para aumentar la seguridad de un mensaje o de un archivo mediante el cifrado del contenido.
- **Codificación:** estándares de codificación de la información.

[2] *Conjunto ordenado y finito de operaciones que permite encontrar la solución de un problema.*
[3] *Son un conjunto de reglas y procedimientos que deben seguirse para la correcta comunicación entre sistemas de información.*
[4] *Es lo que se encarga del procesamiento lógico de los datos que se encuentran en una aplicación o sistema, permitiendo así generación de resultados en base a los datos suministrados.*
[5] *Es el medio por el cual el usuario puede interactuar con un dispositivo o computador.*
[6] *Es un proceso que utiliza algoritmos matemáticos para la protección de datos.*

- **Codificación de caracteres:** formatos de codificación del lenguaje natural[7] a lenguaje de máquina[8] para los documentos.
- **Idioma:** estándares de internacionalización y de codificación de idiomas.

- **Control de acceso:** estándares de gestión de accesos a los activos de información.
- **Integridad:** algoritmos de función hash criptográfica[9] para la verificación de la integridad de los datos que son transferidos entre sistemas.
- **Métricas:** estándares de medidas y métricas.
- **Protocolos de comunicación:** estándares de conexión, comunicación y transferencia de información.
  - **Servicios web**[10]**:** protocolos y estándares para el intercambio de datos entre aplicaciones web.
  - **Tecnologías de transporte y red:** protocolos de comunicación de red definidos en las capas de transporte y red del modelo OSI[11].

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

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

[7] *Es el lenguaje utilizado por los seres humanos para comunicarse.*
[8] *Se refiere a al conjunto de instrucciones que determinan las acciones que debe ejecutar una máquina.*
[9] *Es un algoritmo que transforma un texto, contraseña o archivo en una cadena alfanumérica.*
[10] *Es una tecnología que se utiliza para intercambiar datos entre aplicaciones, implementando ciertos estándares y protocolos.*
[11] *Es un modelo o marco de referencia utilizado para describir la interconexión de los sistemas de comunicación*

- **Metadatos:** estándares para la descripción de los datos intercambiados.
- **Tecnologías semánticas:** estándares para la representación semántica de la información.

- **Tecnologías de integración de datos:** estándares para la integración de datos que intervienen en un proceso de intercambio de información.
- **Tecnologías para identificación:** técnicas de identificación normalizadas de recursos y localizaciones.

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

- **Nombre:** denominación del estándar.
  - **Nombre común:** forma habitual de nombrar el estándar.
  - **Nombre formal:** nombre correspondiente a la especificación formal del estándar.
- **Tipo:** el cual puede ser:
  - **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.
  - **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.
- **Versión mínima aceptada:** versión a partir de la cual debe utilizarse el estándar.

- **Extensión(es):** listado de extensiones relacionado con la extensión.
- **Estado:** condición en la que se encuentra el estándar, la cual puede ser:
    - **Estable:** se encuentra en su versión final.
    - **En Proceso:** estándar cuyo desarrollo continúa en proceso.

Sección 2.03. Catálogo de estándares interoperables

Segmentos de interoperabilidad	Categoría	Nombre		Tipo	Versión mínima aceptada	Extensión	Estado
		Común	Formal				
Accesibilidad y seguridad	Autenticación – Firma electrónica	XAdES	XML Advanced Electronic Signatures	Abierto	1.2.2	.xml .dsig .xsig	Estable
		XML-DSig	XML Signature Syntax and Processing	Abierto	Segunda edición 2008	.xml .dsig .xsig .sig	Estable
	Autenticación – Política Firma electrónica	ETSI TR 102 272	ETSI TR 102 272 Electronic Signatures and Infrastructures (ESI); ASN. 1 format for signature policies	Abierto	RFC 3125 1.1.1	N/A	Estable
		SSH	Secure Shell	Abierto	1.99 (SSH 2)	N/A	Estable
	Cifrado	TLS	Transport Layer Security (TLS)	Abierto	RFC 5878, RFC 5746 RFC 5705, RFC 5489 RFC 5487, RFC 5469 RFC 5289, RFC 5288	N/A	Estable
	Codificación – Codificación de caracteres	Base16, Base32 y Base64	The Base16, Base32 and Base64 Data Encodings	Abierto	RFC 4648	N/A	Estable
		UCS UTF-8	ISO/IEC 10646:2003 Information technology –Universal multiple – Octet Coded Character Set	Abierto	2003		Estable
	Codificación - Idioma	RFC 4646 ISO 639	RFC 4646 –Tags for Identifying Languages. ISO 639 – Codes for the Representation of Names of Languages	Abierto	2002 – 2008 RFC 4646	N/A	Estable
	Formatos archivos– Compresión de archivos	GZIP	GNU ZIP	Abierto	RFC 1952	.gz	Estable
		ZIP	ZIP RFC 1952	Abierto	N/A	.zip	Estable
		7ZIP	7ZIP	Abierto	9.0	.7zip	Estable

Segmentos de interoperabilidad	Categoría	Nombre		Tipo	Versión mínima aceptada	Extensión	Estado
		Común	Formal				
Accesibilidad y seguridad	Formatos archivos– Imagen y/o texto	CSV	Comma Separated Values	Abierto	RFC 4180	.csv .txt	Estable
		HTML	HyperText Markup Language	Abierto	4.0.1	.html .htm	Estable
		CSS	Cascading Style Sheets	Abierto	2.1	.css	Estable
		JPEG / JPG	Join Photographic Experts Group	Abierto	ISO/IEC 10918-4:1999, T.86 (06/98)	.jpg .jpeg	Estable
		ODF	Open Document Format	Abierto	1.0	.odt .ods .odp .odg	Estable
		Strict Open XML	Strict Open eXtensible Markup Languaje	Abierto	2012	.docx .xlsx .pptx	Estable
		PDF	Portable Document Format	Abierto	1.4	.pdf	Estable
		PNG	Portable Network Graphics	Abierto	ISO/IEC 15948,[1] IETF RFC 2083	.png	Estable
		SVG	Scalable	Abierto	1.1	.svg	Estable
		TIFF	Vector Graphics	Abierto	2004	.tiff	Estable
		TSV	Tag Image File Format	Abierto	N/A	.tsv .tab	Estable
		TXT	Tab-separated Values	Abierto	N/A	.txt	Estable
		XHTML	Texto Plano	Abierto	1.0	.html .htm	Estable
	Integridad	SHA	Secure Hash Algorithms	Abierto	RFC 4634 RFC3874	N/A	Estable
Infraestructura y conectividad	Control de acceso	LDAP	Lightweigth Directory Access Protocol.	Abierto	RFC 4510	N/A	Estable
	Protocolos de comunicación e intercambio – Tecnologías de transporte y red	AtomPub	Atom Publishing Protocol	Abierto	N/A	.atompub .xml	Estable
		CDN	Content Delivery Network	Abierto	N/A	N/A	Estable

Segmentos de interoperabilidad	Categoría	Nombre		Tipo	Versión mínima aceptada	Extensión	Estado
		Común	Formal				
Infraestructura y conectividad	Protocolos de comunicación e intercambio – Tecnologías de transporte y red	DNS	Network Time Protocol	Abierto	RFC 1035	N/A	Estable
		HTTP	Online Certificate Status Protocol	Abierto	1.1 RFC 2616 RFC 2817	N/A	Estable
		ICAP	Simple Object Access Protocol	Abierto	RFC 3238	N/A	Estable
		IPSec	Representational State Transfer	Abierto	RFC 2401 RFC 4302 RFC 4835	N/A	Estable
		NTP	Abstract Syntax Notation One	Abierto	RFC 5905	N/A	Estable
Integración de aplicaciones y servicios	Autenticación - Certificados	OCSP	Online Certificate Status Protocol	Abierto	RFC 2560	N/A	Estable
	Protocolos de comunicación e intercambio – Servicios Web	RESTful	Representational State Transfer	Abierto	N/A	N/A	Estable
	Tecnologías para identificación	ASN.1	Abstract Syntax Notation One	Abierto	2008	N/A	Estable
		URI	Uniform Resource Identifier	Abierto	RFC 3986 RFC 5785	N/A	Estable
		URL	Uniform Resource Locators	Abierto	RFC 1738	N/A	Estable
		URN	Uniform Resouce Names	Abierto	N/A	N/A	Estable
	Semántica	DCAT	Data Catalog Vocabulary	Abierto	N/A	N/A	Estable

Segmentos de interoperabilidad	Categoría	Nombre		Tipo	Versión mínima aceptada	Extensión	Estado
		Común	Formal				
Integración de datos	Semántica - Metadatos	ISO 8601	Data elements and interchange formats – Information interchange – Representation of dates and times	Abierto	N/A	N/A	Estable
		MoReq	Model Requirements for the management of electronic records	Abierto	N/A	N/A	Estable
		PREMIS	PREservation Metada: Implementation Strategies V2.1	Propietario	N/A	N/A	Estable
	Semántica – Tecnologías semánticas	N3	Notation 3	Abierto	N/A	.n3	Estable
		RDF	Resource Description Framework	Abierto	1.0	N/A	Estable
		RDFa	Resource Description Framework – in - attributes	Abierto	2008	N/A	Estable
	Tecnologías de integración de datos	ATOM	Atom Syndication Format	Abierto	1.0	.atom .xml	Estable
		JSON	JavaScript Object Notation	Abierto	RFC 7159 and ECMA-404	.json .jsonp	Estable
		JSON-RPC	JavaScript Object Notation - Remote Procedure Call	Abierto	1.0	.json .jsonp	Estable
		ODATA	Open Data Protocol	Abierto	2.0	.odata .xml	Estable
		RSS	Really Simple Syndication	Abierto	2.0	.rss .xml	Estable
		XML	Extensible Markup Language	Abierto	1.0	.xml	Estable
		XSD	XML Schema	Abierto	1.0	.xsd	Estable

CAPÍTULO 3

INTEROPERABILIDAD LEGAL Y ORGANIZACIONAL

Para lograr que los diferentes organismos de la administración pública interoperen y trabajen de manera oportuna y eficiente, es necesario que se establezca un proceso adecuado para la coordinación entre los entes involucrados, que permita la ejecución correcta de las actividades, basándose en la colaboración y las responsabilidades definidas.

En ese sentido, este capítulo especifica las directrices que deben ser aplicadas por los organismos a los fines de asegurar una coordinación apropiada de las actividades contenidas en la implementación de la interoperabilidad y garantizar el cumplimiento de los estatutos legales, así como la alineación de sus procesos de negocio, responsabilidades y expectativas en la consecución de un objetivo común. Para lograrlo, se han definido elementos como el acuerdo de colaboración interinstitucional para la generación de documentación legal y organizacional necesaria en la ejecución del proyecto, complementado con la definición de informes técnicos, donde se describan los acuerdos operacionales y procedimientos de manejo del cambio.

Sección 3.01. Lineamientos legales para la interoperabilidad

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

(a) Cada organismo debe determinar los mecanismos y competencias legales necesarios que lo habilitan para el intercambio de información.

(b) Cada organismo debe clasificar la información de carácter personal o confidencial que se encuentra asociada a los servicios de intercambio de información.

(c) Cada organismo debe establer los mecanismos apropiados para licenciar los datos que serán intercambiados y usados por otros organismos, en donde se establezcan datos para arreglos de custodia, propiedad intelectual, condiciones de uso, entre otros criterios a definir.

Sección 3.02. 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, específicamente abarcando los aspectos legales que funcionarán como fundamento básico para la relación entre los organismos.

(a) Cada organismo debe determinar los mecanismos y competencias legales necesarias que lo habilitan para el intercambio de información.

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

(i) El organismo propietario de la iniciativa debe cumplir con las exigencias tecnológicas realizadas por el o los organismos de interés, siempre que estos cumplan con estándares interoperables expuestos en el **Capítulo 5. Interoperabilidad Técnica.**

(ii) Los líderes de proyectos de las áreas de proyectos de TIC de los organismos involucrados deben permanecer en contacto, a fin de garantizar el cumplimiento de los tiempos establecidos.

a) Para cada reunión deben realizarse minutas.

(iii) 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.

(iv) 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 3.02.1. Acuerdo de Colaboración Interinstitucional

(a) Los organismos involucrados en un proceso de interoperabilidad deben realizar un 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 notarizado por un notario público.

(iii) El acuerdo debe estar firmado 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 y cualquier otro elemento que los organismos involucrados determinen necesario.

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

(i) **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:

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

b) **Descripción general del/ los sistemas:** en donde se describa de manera general en qué consiste el sistema y cómo estará beneficiando sus servicios este proyecto.

c) **Interoperabilidad semántica:** en donde se detalle el modelo de información y el catálogo de metadatos utilizados para la comprensión e interpretación de la información transmitida de un punto a otro.

d) **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.

(e) **Acuerdo de nivel de servicio**[1] **(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:

- Contacto de soporte.
- Horas de soporte.
- Disponibilidad del servicio.
- Tiempo de respuesta de soporte.
- Interrupciones programadas.
- Límite de rendimiento.
- Límite de tamaño de mensaje.

(f) **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.

Sección 3.03. Roles para la unidad de TIC

Como una segunda parte del proceso Interoperabilidad Organizacional, se define necesaria la delimitación y asignación apropiada de los roles y responsabilidades que debe ejecutar la Unidad 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, las cuales serán partícipes en todos los proyectos que refieran a la interoperabilidad entre sistemas de información.

[1] *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.*

(b) La unidad de TIC debe tener estructurada la unidad de Proyectos 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 área de administración de proyectos de TIC debe tener el personal adecuado para cumplir con las responsabilidades especificadas en la **NORTIC A1:2014, subsección 2.01.1. Estructura organizacional referente a la administración de proyecto de TIC**, así como con los roles establecidos a continuación para la gestión de los proyectos de interoperabilidad:

(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. Este rol posee la responsabilidad de lograr el correcto planteamiento de las soluciones a los distintos directivos de las áreas que afectan los proyectos definidos, así como también lograr la aceptación final de la máxima autoridad del organismo.

a) Este rol debe ser asumido por una persona que tenga cierto grado de influencia en los departamentos principales del organismo, con destrezas y manejo gerencial con predominante capacidad administrativa y toma de decisiones.

(ii) **Manejador de proyectos:** es el responsable de la administración de los recursos tanto los financieros como los humanos que estén relacionados con los proyectos. Adicionalmente está a cargo de velar por la calidad, tiempos de entrega de las tareas y fases, así como también de la elaboración y entrega de toda la documentación de los proyectos en curso.

a) Este rol debe ser asumido por una persona con un perfil de experiencia en manejo de proyectos y equipos de trabajo.

(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 técnicos que estará trabajando en el proyecto.

a) Este rol debe ser asumido por una persona con un alto nivel técnico especialmente en el área de desarrollo de software y poseer conocimiento de metodologías de trabajo ágiles para este tipo de proyectos.

(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 tener estructurada la Unidad de Diseño, Desarrollo e Implementación de Servicios y Plataformas TIC, o 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[1] 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 a publicar en la Plataforma única de Interoperabilidad, en base a los líneamientos técnicos especificados en el **Capítulo 5 sobre Interoperabilidad Técnica.**

(e) El organismo debe redactar las descripciones de puestos donde se detallen las funciones y responsabilidades de cada puesto de las áreas impactadas de la Unidad de TIC, detallando los roles asignados, según lo mencionado en las directrices anteriores.

[1] *Es el punto de entrada a la Plataforma Única de Interoperabilidad y es necesario tanto para producir como para consumir servicios a través de la Plataforma. El servidor de seguridad media en las llamadas de servicio y las respuestas de servicio entre los sistemas de información.*

(i) Los roles especificados para la Unidad 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).

(f) En caso de que el organismo no cuente con el personal suficiente para que sean asignados los roles de forma exclusiva, estos deben ser redistribuidos en el área, para asegurar su cumplimiento.

(g) El personal técnico que trabajará en el proyecto sea este interno o externo al organismo, debe asumir el rol de equipo técnico.

(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 sucedan 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 3.04. Desarrollo y robustecimiento de interoperabilidad

Como elemento final 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.

Para estos fines, el organismo debe asegurarse de:

(a) Desarrollar y aprobar una Política de Desarrollo y Robustecimiento de Interoperabilidad, que establezca lineamientos concretos para:

  (i) La realización gradual y bajo planificación de un análisis general de los componentes operativos de la institución, a los fines de detectar actividades, trámites, procesos y servicios que puedan ser mejorados utilizando la interoperabilidad.

  (ii) La elaboración de un plan de acción para aprovechar las oportunidades detectadas durante el análisis y su inclusión en la Planificación Operativa Anual del organismo para fines de cumplimiento.

  (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.*

(b) Para el caso de que el organismo haya realizado la organización de sus servicios utilizando la estructura indicada en la **NORTIC A5:2019, Capítulo 2. Levantamiento y Estrategia para la Presentación de los Servicios Públicos,** debe utilizar los resultados arrojados por el Análisis de Reducción de Trámites y el Plan de Automatización de Servicios levantados durante la implementación.

CAPÍTULO 4

INTEROPERABILIDAD SEMÁNTICA

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

Sección 4.01. 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.

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

Sección 4.02. 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 un conjunto de metadatos para lograr el procesamiento de la información de la forma más efectiva.

(a) Siempre que sea posible deben utilizarse modelos de información comunes o reconocidos.

(i) En caso de tener que diseñar un modelo de información propio, este debe ser independiente de tecnología y plataforma específica.

> *Algunos de los modelos de información reconocidos por la industria se encuentra: NIEM, HR-JSON y HL7.*

(b) La información intercambiada debe estar descrita en función de metadatos.

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

- **Expresividad:** poseer los conceptos necesarios para una explicación real de lo que se desea expresar.
- **Sencillez:** debe ser simple para su fácil comprensión.

- **Singularidad:** cada concepto debe tener un significado único.
- **Precisión:** los conceptos deben estar definidos de forma concisa y exacta.

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

(e) 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.

Subsección 4.02.1. Metadatos propuestos

(a) Debe utilizarse el siguiente esquema de metadatos para la descripción de los elementos de datos:

(i) Los metadatos requeridos son los definidos a continuación:

a) **Nombre:** define el nombre asignado para identificar coherentemente al atributo.

b) **Fecha:** especifica la fecha de un evento del atributo. La fecha debe especificarse siguiendo el estándar ISO 8601, utilizando el sistema horario de 24 horas y organizando el metadato de más a menos significativos como sigue: YYYY-MM-DD hh:mm:ss.

c) **Descripción:** donde se explica de forma breve de qué trata el contenido del atributo.

d) **Organismos relacionados:** donde se especifican los organismos responsables de la creación del atributo.

e) **Características técnicas:** donde se describe la forma y el tamaño del atributo.

i) Para la definición de las características técnicas deben especificarse los siguientes atributos:

- Formato.
  - Nombre del formato.
  - Extensión del formato.
- Tamaño.
  - Dimensiones físicas.
  - Tamaño lógico.
  - Cantidad.
  - Unidades.

f) **Seguridad:** donde se establecen un conjunto de criterios que determinen los privilegios y restricciones de acceso a las diferentes entidades con el objeto de proteger las mismas.

i) Para definir la seguridad debe especificarse lo siguiente:

- Nivel de seguridad.
- Advertencia de seguridad.
- Permisos.
- Nivel de confidencialidad de la información.

g) **Identificador:** clave unívoca que permite al usuario una forma fácil para colocar un nombre técnico resumido que identifique la naturaleza del metadato y con posibilidad de ser común con otros. Como resultado de esta asignación se podrá buscar la

información de una forma más rápida, precisa y menos densa dentro del universo de datos.

h) **Derecho de acceso:** donde se indiquen las políticas y requisitos que regulan o restringen el acceso a terceros.

i) **Estado:** en donde se especifica la etapa actual del elemento de datos. El estado debe definirse en una de las siguientes etapas:

- **En definición:** el elemento de datos está conceptualizada a partir de una solicitud.
- **En desarrollo:** se encuentra en proceso de creación y realización de pruebas funcionales necesarias.
- **Disponible:** se encuentra publicado y listo para su uso.
- **Obsoleto:** se utilizan en algunas aplicaciones, pero no son recomendados para implementaciones tecnológicas.

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

k) **Versión:** en donde se presenta el número de versión actual. Esto debe definirse siguiendo lo especificado en la **Subsección 5.03.2. Diseño de las APIs**

l) **Alias:** en donde se define nombres alternativos por los cuales se le puede conocer al atributo.

m) **Contacto:** en donde se indica la información acerca de cómo contactar con el responsable de darle soporte al dato.

n) **Validación:** en donde se especifican las reglas que deben ser aplicadas en la construcción o definición del atributo.

i) Las validaciones especificadas en el metadato deben ser utilizadas por los servicios que utilicen el atributo. En caso de que no existan validaciones el valor por defecto de este metadato debe ser "No Disponible" (N/D).

(ii) Los siguientes metadatos son requeridos solo cuando aplique su uso:

a) **Público:** en donde se especifica el público o tipo de usuario a los cuales se dirige el atributo.

b) **Relación:** en donde se especifica las relaciones con otros elementos de datos.

c) **Firma:** en donde se señala el tipo de firma electrónica empleada para la autenticación del dato.

(iii) Los metadatos a continuación no son requeridos, el organismo tiene la posibilidad de utilizarlos:

a) **Ubicación:** en donde se especifica la ubicación física del atributo.

b) **Idioma:** en donde se especifica el idioma del contenido interno del atributo.

(b) En caso de que un metadato pueda tener distintos significados y comportamientos, los usos de estos deben ser identificados y documentados.

CAPÍTULO 5

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 5.01. Plataforma única de Interoperabilidad

Los organismos gubernamentales deberán hacer uso de la Plataforma Única de Interoperabilidad para compartir e intercambiar información.

(a) Para hacer uso de la Plataforma Única de Interoperabilidad, los organismos deben cumplir con los siguientes lineamientos:

(i) Ejecutar el proceso de vinculación a la plataforma, para lo cual deben cumplir con:

- Leer y firmar las políticas de condiciones y aceptación provistas por OGTIC para el uso de la Plataforma.

- Tener un servidor de seguridad instalado que cumpla con los requisitos técnicos mínimos.

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

https://docs.x-road.global/Manuals/ig-ss_x-road_v6_security_server_installation_guide.html#13-references

- Poseer el personal necesario para cumplir con los roles requeridos en la Sección 3.03 Roles para la Unidad de TIC.

(ii) Para habilitar el intercambio de información con otros entes, el organismo debe desarrollar sus servicios de intercambio de información siguiendo las directrices especificadas en las diferentes secciónes que componen este capítulo de la norma.

Sección 5.02. Implementación de estándares abiertos

(a) Todos los estándares utilizados por los organismos deben ser abiertos.

(i) Los estándares abiertos deben cumplir con las siguientes cualidades.

- **Disponibilidad:** deben estar disponibles para su lectura e implementación.
- **Capacidad de elección:** deben aprovecharse las herramientas y los marcos de código abierto para la implementación de la API.
- **Sin prebendas:** deben evitarse los protocolos y esquemas de datos patentados por proveedores.

- **Sin discriminación:** la elección de una implementación debe ser por motivos puramente técnicos.
- **Extensión o reducción:** las implementaciones pueden ser ampliadas o utilizar sólo un subconjunto del estándar.
- **Sin prácticas abusivas:** su implementación debe evitar tácticas subversivas y cualquier acción que atente contra la privacidad de los usuarios.

Sección 5.03. Estándares para la creación de APIs

Esta sección especifica las directrices a seguir para el desarrollo, diseño, publicación y documentación de APIs de forma que cumplan con las mejores prácticas en el desarrollo de estas aplicaciones.

(a) Las APIs desarrolladas por o para los organismos gubernamentales deben cumplir con las siguientes directrices:

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

a) Los Localizadores Uniformes de Recursos (URL, por sus siglas en inglés) deben representar entidades y objetos comerciales.

b) 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:

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

ii) Debe evitarse claves de objeto[1] impredecibles o dinámicas como las derivadas de los datos (object keys, por nombre en inglés).

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

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

- GET: recuperar o consultar un recurso.
- POST: crear un nuevo recurso o iniciar una acción.
- PUT: actualizar o reemplazar un recurso existente.
- DELETE: Para eliminar recursos.
- PATCH: Para editar partes concretas de un recurso.

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

(iv) 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.

a) Las URIs deben cumplir con los siguientes requisitos:

- No contener verbos.
- Identificar unicamente a un recurso.

[1] *Es una representación detallada de un elemento o unidad de la realidad y la misma consta de un estado y comportamiento.*

- Mantener una jerarquía lógica.
- Hacer filtrados de información mediante los parámetros HTTP.
- Especificarse usando su forma plural.

(v) 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:

(vi) Siempre que se utilice HTTP para el intercambio de información, debe acompañarse del Protocolo de Seguridad de la Capa de Transporte (TLS, por sus siglas en inglés).

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

a) El encabezado AUTHORIZATION es obligatorio.

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

c) Las claves o tokens de API deben configurarse de forma segura. **Ver la sección 5.05 Aspectos Generales De Seguridad.**

d) La respuesta debe contener el encabezado CONTENT-TYPE.

Subsección 5.03.1. 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. Las API deben abstraer la representación de datos físicos del backend del consumidor.

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

(b) Debe evitarse la creación de estruturas de datos para las respuestas JSON.

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

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

- El código de error.
- El mensaje que describa el error.
- El tipo de error.
- Una lista de errores, en caso de que aplique.

Ejemplo de una respuesta de error:

```
{
 “code”: “validation_failed”,
 “message”: “Validation failed”,
 “type”: “error”,
 “errors”: [
  {
   “code”: “invalid_characters”,
    “message”: “Name should not contain invalid characters”,
   “field”: “name”
  },
  {
   “code”: “required”,
   “message”: “Password is required”,
```

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

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

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

Subsección 5.03.2. Diseño de las APIs

(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 debe permitir la aplicación de diferentes perfiles de acceso a datos, ya sea a la API o en una capa de proxy[2], sin la necesidad de crear API adicionales.

(c) Las APIs deben diseñarse basadas en consulta.

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

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

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

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

(f) Toda API debe estar versionada.

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

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

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

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

- **Importante:** versión significativa que probablemente rompa la compatibilidad con versiones anteriores.
- **Menor:** adición de atributos opcionales o nueva funcionalidad que es compatible con versiones anteriores, pero debe probarse.
- **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.

(iv) La URL debe reflejar solo la versión principal.

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

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

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

(vii) 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.

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

b) 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.

(g) 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[3] pueden 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.

[3] *Es una variable la cual puede ser recibida por un método o procedimiento.*

(h) Las APIs que exponen grandes conjuntos de datos deben admitir alguna forma de segmentación de datos.

(i) 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 está estrictamente prohibida en las API de datos maestros, transaccionales o comerciales.

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

(k) En casos donde las APIs desarrolladas deban participar en escenarios que ameriten que los conjuntos datos masivos estén disponibles entre sistemas o para el público, deben tomarse en cuenta las siguientes consideraciones:

  (i) Los conjuntos de datos más pequeños deben devolverse en formatos de sobrecarga baja, tales como Valores Separados por Coma (CSV, por sus siglas en inglés) o JSON en lugar de XML.

  (ii) Debe evitarse el uso de archivos comprimidos en especial cuando se consumen APIs externas.

  (iii) Utilizar APIs de activación (trigger API, por su nombre en inglés) para iniciar una interfaz fuera de banda y mover grandes volúmenes de datos.

(l) Utilizar API de búsqueda y enlace (search and link API, por su nombre en inglés) en casos donde el conjunto de datos se publique en servidores de archivos disponibles para el consumidor, con el objetivo de devolver un enlace a un archivo específico en función de parámetros de solicitud específicos.

Sección 5.04. Administración de código fuente

La interoperabilidad debe incluir tanto lo referente a la comunicación y almacenamiento de la información, así como también la estandarización y disponibilidad del código fuente[4] utilizado en las soluciones gubernamentales para su reutilización y resguardo seguro, por tal razón, en esta sección se especifican las directrices para la efectiva administración del código fuente.

Subsección 5.04.1. Publicación y documentación

(a) Las APIs deben estar publicadas para ser detectables.

  (i) Cada organismo debe contar con un repositorio GIT[5] de uso interno.

  (ii) Una vez completado, probado y en uso, el código fuente debe colocarse en el repositorio GIT del Gobierno Dominicano github.com/gobdo.

  (iii) Debe publicarse un punto de contacto designado para cualquier equipo que consuma su API en el repositorio del Gobierno Dominicano.

(b) La forma en que se consumirá cada API debe estar claramente documentada.

  (i) La documentación debe ser concisa y actualizada.

  (ii) Debe usarse OpenAPI para API RESTful a la hora de generar la documentación.

[4] *Es un conjunto de instrucciones redactas en base a las reglas sintácticas de un lenguaje de programación para desarrollar un software determinado.*

[5] *Es un sistema de control de versiones de código abierto que registra los cambios realizados sobre un archivo o conjunto de archivos a lo largo del tiempo, y estas versiones específicas puedan ser utilizadas más adelante.*

(c) Deben publicarse pruebas unitarias y datos de pruebas de las APIs colocadas en el repositorio del Estado.

(i) Debe realizarse pruebas de carga de la API en donde se mida el tiempo de respuesta y el rendimiento durante una carga razonable, de manera que se pueda identificar los umbrales donde el API se vuelve inestable.

(ii) Debe medirse y publicarse evaluaciones comparativas de rendimiento.

(iii) Debe evidenciarse que la API cumple con la capacidad adecuada para satisfacer la demanda de uso.

(d) Cada versión completamente funcional de la solución debe estar separada por "Branches[6]" dentro del repositorio de GIT para la corrección.

(e) Debe colocarse un comentario detallado de forma obligatoria en cada "Commit[7]" que se realice en la plataforma.

Subsección 5.04.2. Comentarios del código fuente

(a) Debe utilizarse nombres descriptivos para entidades[8] u objetos.

(b) Los comentarios en el código deben ser concisos:

(i) Debe comentarse los distintos bloques de los que se compone el código, aplicando un criterio uniforme y distinto para cada nivel. Debe seguirse un modelo basado en los aspectos siguientes:

- Incluir en cada clase una breve descripción, su autor y fecha de última modificación.

[6] *Es un apuntador móvil dirigido a una de las confirmaciones o "commit".*
[7] *Es una confirmación de algún cambio en el repositorio GIT.*
[8] *Es una representación de un objeto del mundo real, el cual posee características y atributos únicos.*

- Incluir por cada método[9], una descripción de su objeto y funcionalidades, así como de los parámetros y resultados obtenidos.

(ii) Los comentarios deben explicar de manera breve la funcionalidad de un método antes de su declaración[10].

a) No debe incluirse en el comentario cómo el método realiza su funcionalidad.

(iii) No debe comentarse el código para manejo de cambios.

(iv) Los comentarios en el código fuente deben mantenerse actualizados.

a) Si en algún momento la funcionalidad del código cambia, deben actualizarse los comentarios.

b) De cambiar la naturaleza del algoritmo, debe actualizarse inmediatamente el comentario asociado.

(v) Debe mantenerse el mismo estilo de formato y comentarios en todo el código fuente para permitir una mejor compresión del lector.

(vi) No debe utilizarse palabras o frases indebidas en los nombres de entidades, métodos o comentarios dentro del código fuente.

(vii) Se recomienda utilizar el estándar y/o tecnología de documentación propia del lenguaje de programación utilizado.

Ejemplo de rry/o tecnologías de documentación:

- Para C# el XML Documentation Comments.
- Para Python los Document Strings.

[9] *Es un fragmento de código el cual puede ser utilizado o invocado por otro sistema para la realización de una tarea en específica.*

[10] *Consiste en la asignación de un nombre a una entidad en específico.*

(a) Solo debe utilizarse canales de transferencia seguros como los especificados en cada punto de la normativa.

(b) Las API deben diseñase resistentes a ataques de desbordamiento de búfer y de inyección SQL[11].

(c) En caso de aplicar, debe utilizarse controles adicionales, tales como el cifrado a nivel de mensaje, autenticación mutua y firmas digitales según el nivel de sensibilidad de los datos.

(d) Los datos confidenciales no deben pasarse en las cadenas de URL de solicitud.

(i) En caso de que una consulta involucre datos confidenciales, los parámetros de la consulta deben pasarse como una carga útil de mensaje JSON en lugar de en la cadena de solicitud de URL.

(e) Debe Implementarse un esquema de control de acceso que proteja las API para que no sean invocadas incorrectamente, incluidas funciones no autorizadas y referencias de datos, cumpliendo con los siguientes requisitos:

- Siempre realizar autenticación y autorización antes de cualquier operación para garantizar que el acceso a la API esté restringido al sistema o sistemas autorizados.

- Utilizar estándares abiertos como OpenID Connect y Open Authorization 2.0[12] (OAuth 2.0) para las API RESTful.

[11] *Es una tecnica común de ataque web que aprovecha una vulnerabilidad en un sistema informático para infiltrar código intruso y atacar las bases de datos.*

[12] *Es el protocolo estándar de la industria para la autorización. Se centra en la simplicidad del desarrollador al tiempo que proporciona flujos de autorización específicos para aplicaciones web, aplicaciones de escritorio, teléfonos móviles y dispositivos de sala de estar.*

- Asegurarse de que la clave de API (API key) esté protegida.
- Las APIs de datos abiertos deben protegerse con una clave de API para permitir el seguimiento del uso y brindar la capacidad de identificar y prevenir el uso malintencionado potencial.

(f) Deben implementarse prácticas seguras de gestión de tokens.

(i) Deben utilizarse tokens de estándares abiertos y evitar el uso de esquemas de tokens patentados por el proveedor.

(ii) No deben crearse tokens personalizados.

(iii) Debe utilizarse JSON Web Token[13] (JWT, por sus siglas) para las interacciones de la API RESTful.

(iv) Los tokens de acceso deben caducar en un período de tiempo razonable. En caso de utilizar el estándar SAML, la expiración de la aserción debe configurarse para controlar el período de validez de toda la sesión de autenticación y autorización.

(g) Debe implementarse el uso de Gateways y Proxies en lugar de Whitelists.

[13] *Es un estándar abierto que define una forma compacta y autónoma de transmitir información de forma segura entre las partes como un objeto JSON.*

GLOSARIO DE TÉRMINOS

ACCESIBILIDAD

Es el grado en que las personas, sin importar su capacidad, puedan acceder y manipular un software.

7ZIP

Es un formato libre de almacenamiento y compresión de datos.

ACUERDO DE NIVEL DE SERVICIO (SLA)

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.

ALGORITMO

Conjunto ordenado y finito de operaciones que permite encontrar la solución de un problema.

BASES DE DATOS RELACIONALES

Es una base de datos que permite la interconexión entre los datos almacenados en ella.

BRANCHES / RAMAS

Es un apuntador móvil dirigido a una de las confirmaciones o “commit”.

CIFRADO DE DATOS

Es un proceso que utiliza algoritmos matemáticos para la protección de datos.

CÓDIGO FUENTE

Es un conjunto de instrucciones redactas en base a las reglas sintácticas de un lenguaje de programación para desarrollar un software determinado.

COMMIT

Es una confirmación de algún cambio en el repositorio GIT.

CORREO ELECTRÓNICO

Es un servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.

DECLARACIÓN

Consiste en la asignación de un nombre a una entidad en específico.

ENTIDAD

Es una representación de un objeto del mundo real, el cual posee características y atributos únicos.

ESTÁNDARES ABIERTOS

Hace referencia a formatos que permiten su uso y manipulación libremente.

ESTÁNDAR DE METADATOS DE MANTENIMIENTO DE REGISTROS DEL GOBIERNO AUSTRALIANO (AGRKMS)

Describe información sobre registros y el contexto en el que se capturan y utilizan en las agencias del gobierno australiano. El estándar está diseñado para ser utilizado como una herramienta por el personal involucrado en la gestión de información y registros, gestión de datos e información y comunicación.

FIRMA ELECTRÓNICA AVANZADA XML (XADES)

Establece un grupo extensiones para firmas electrónicas, las cuales van acorde a las pautas de firmas XML.

FIRMA XML (XML-DSIG)

Es una definición recomendada por la W3C de la sintaxis XML para la firma digital.

FORMATO DE ARCHIVO DE IMAGEN ETIQUETADO (TIFF)

Es un formato utilizado mayormente para el almacenamiento de imágenes, que permite una compresión sin pérdida de la calidad con una profundidad de color de 16 bits.

FORMATO DE DOCUMENTO PORTÁTIL (PDF)

Es un formato de almacenamiento de datos que funciona y puede ser visualizado independientemente de la plataforma, siendo así portátil y multiplataforma para su visualización.

FORMATO DE DOCUMENTO ABIERTO (ODF)

Es un formato de documento abierto para aplicaciones de ofimática.

FORMATO DE REDIFUSIÓN ATOM (ATOM)

Es un fichero en formato XML usado para Redifusión web.

FORMATO DE TRANSFORMACIÓN UNICODE DE 8-BIT (UTF-8)

Es un formato estándar de codificación de caracteres capaz de representar cualquier carácter. Por sus características es recomendado para ser utilizado en la codificación de correos electrónicos y páginas web.

FUNCIÓN HASH CRIPTOGRÁFICA

Es un algoritmo que transforma un texto, contraseña o archivo en una cadena alfanumérica.

GIT

Es un sistema de control de versiones de código abierto que registra los cambios realizados sobre un archivo o conjunto de archivos a lo largo del tiempo, y estas versiones específicas puedan ser utilizadas más adelante.

GNU ZIP (GZIP)

Es un formato de compresión libre con licencia GNU, el cual solo comprime los datos, pero no los conserva.

GRÁFICOS DE RED PORTÁTILES (PNG)

Es un tipo de archivo de imagen rasterizado que goza de muchísima popularidad entre los diseñadores sitio web, debido a su capacidad de procesar los gráficos con fondos transparentes o semitransparentes.

GRÁFICOS VECTORIALES REDIMENSIONABLES (SVG)

Es un formato para presentar gráficos vectoriales bidimensionales estáticos o animados.

GRUPO CONJUNTO DE EXPERTOS EN FOTOGRAFÍA (JPG/JPEG)

Es un comité técnico que desarrolla estándares de imagen.

HOJA DE ESTILO EN CASCADA (CSS)

Es un lenguaje de programación para la web destinado a dar estilo visual.

HR-JSON

Es una organización sin fines de lucro impulsada por miembros que proporciona estándares de intercambio de datos disponibles gratuitamente.

INTERFAZ DE PROGRAMACIÓN DE APLICACIONES (API)

Es un conjunto de herramientas, definiciones y protocolos que se utiliza para integrar los servicios y el software de aplicaciones.

INTERFAZ DE USUARIO

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

INTÉRPRETE DE ÓRDENES SEGURA (SSH)

Es un protocolo y aplicación por el cual se accede remotamente a una computadora a través de una red de comunicación.

INYECCIÓN SQL (SQLI)

Es una tecnica común de ataque web que aprovecha una vulnerabilidad en un sistema informático para infiltrar código intruso y atacar las bases de datos.

JSON- LLAMADA A PROCEDIMIENTO REMOTO (JSON-RPC)

Es en protocolo de llamada de procedimiento remoto ligero.

JSON WEB TOKEN (JWT)

Es un estándar abierto que define una forma compacta y autónoma de transmitir información de forma segura entre las partes como un objeto JSON.

LENGUAJE DE DESCRIPCIÓN DE SERVICIO WEB (WSDL)

Es un protocolo basado en XML que se utiliza para describir servicios web.

LENGUAJE DE MÁQUINA

Se refiere a al conjunto de instrucciones que determinan las acciones que debe ejecutar una máquina.

LENGUAJE DE MARCAS DE HIPERTEXTO EXTENSIBLE (XHTML)

Es el lenguaje estándar de elaboración de páginas web. Este es más estricto a nivel técnico que el HTML y permite la detección de errores más fácil.

LENGUAJE DE MARCAS DE HIPERTEXTO (HTML)

Es el lenguaje de programación utilizado para la creación de páginas web.

LENGUAJE DE MARCAS EXTENSIBLE (XML)

Es un lenguaje desarrollado por el Consorcio World Wide Web (W3C) para almacenar datos en forma legible. Este es utilizado para el intercambio de información entre diferentes plataformas.

LENGUAJE DE MARCADO PARA CONFIRMACIONES DE SEGURIDAD (SAML)

Es un estándar abierto que define un esquema XML para el intercambio de datos de autenticación y autorización.

LENGUAJE NATURAL

Es el lenguaje utilizado por los seres humanos para comunicarse.

LOCALIZADOR DE RECURSOS UNIFORME (URL)

Se utiliza para especificar la dirección exacta de un recurso dentro del portal web.

MARCO DE DESCRIPCIÓN DE RECURSOS (RDF)

Es un modelo estándar del Consorcio World Wide Web (W3C), diseñado para almacenar datos en forma legible e intercambio de datos en la web.

MARCO DE DESCRIPCIÓN DE RECURSOS EN ATRIBUTOS (RDFA)

Es una técnica que permite proporcionar un conjunto de atributos de marcas para aumentar la información visual en la Web.

METADATOS

Son un conjunto de información que describe las características de otra información. Es “datos sobre datos”.

METADATOS PARA LA GESTIÓN DEL DOCUMENTO ELECTRÓNICO (E-EMGDE)

El e-EMGDE Incluye los metadatos mínimos obligatorios, definidos en las normas técnicas de interoperabilidad de Documento electrónico

y Expediente electrónico de España, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos.

METADATOS DE PRESERVACIÓN: ESTRATEGIAS DE IMPLEMENTACIÓN (PREMIS)

Es un grupo de trabajo compuesto por expertos internacionales en la utilización de metadatos aplicados a actividades de preservación digital.

MÉTODO

Es un fragmento de código el cual puede ser utilizado o invocado por otro sistema para la realización de una tarea en específica.

MODELO DE REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS Y REGISTROS (MOREQ)

Es una especificación de la gestión de documentos electrónicos publicados por el Foro DLM que describe los requisitos modulares para sistemas de registros.

MODELO NACIONAL DE INTERCAMBIO DE INFORMACIÓN (NIEM)

Es un vocabulario común que permite un intercambio de información eficiente entre diversas organizaciones públicas y privadas.

MODELO OSI

Es un modelo o marco de referencia utilizado para describir la interconexión de los sistemas de comunicación.

MOTOR DE PROCESAMIENTO DE DATOS

Es lo que se encarga del procesamiento lógico de los datos que se encuentran en una aplicación o sistema, permitiendo así generación de resultados en base a los datos suministrados.

NOMBRE DE RECURSO UNIFORME (URN)

Se utiliza para identificar recursos en la web, sin especificar directamente el lugar donde se encuentra.

NOTACIÓN DE OBJETOS DE JAVASCRIPT (JSON)

Es un formato ligero usado como alternativa al XML para intercambio de datos.

NOTACIÓN SINTÁCTICA ABSTRACTA 1 (ASN.1)

Es una norma con una librería de tipos de datos y constructores que permiten definir estructuras de datos complejas.

NOTACIÓN TURTLE (N3)

Es un estándar de facto para escribir RDF.

PROTOCOLO DE AUTORIZACIÓN ABIERTA (OAUTH)

Es el protocolo estándar de la industria para la autorización. Se centra en la simplicidad del desarrollador al tiempo que proporciona flujos de autorización específicos para aplicaciones web, aplicaciones de escritorio, teléfonos móviles y dispositivos de sala de estar.

OBJETO

Es una representación detallada de un elemento o unidad de la realidad y la misma consta de un estado y comportamiento.

PROTOCOLO DE DATOS ABIERTOS (ODATA)

Es un protocolo abierto para permitir la creación y el consumo de API RESTful consultables e interoperables de una manera simple y estándar.

OPENAPI

Es un estándar para la descripción de las Interfaces de Programación de Aplicaciones (API) por excelencia el cual establece un marco común sobre cómo construir y mantener APIs.

PARÁMETROS

Es una variable la cual puede ser recibida por un método o procedimiento.

PROTOCOLO DE ADAPTACIÓN DE CONTENIDOS DE INTERNET (ICAP)

Es un protocolo abierto simple y ligero. Normalmente se utiliza para transportar mensajes HTTP entre el proxy y los dispositivos que proporcionan soporte antimalware y servicios de prevención de fugas de datos.

PROTOCOLO DE ESTADO DE CERTIFICADOS FUERA DE LÍNEA (OCSP)

Es un protocolo creado con la finalidad de determinar el estado de un certificado digital.

PROTOCOLO DE TIEMPO DE RED (NTP)

Es un protocolo de internet creado con el fin de sincronizar los relojes de los sistemas informáticos.

PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO (HTTP)

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

PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS (LDAP)

Es un protocolo ligero de acceso a una librería de datos organizados lógica y jerárquicamente.

PROTOCOLO SEGURO DE INTERNET (IPSEC)

Es un conjunto de protocolos de seguridad para proteger la comunicación IP y transmisión de paquetes en Internet.

PROTOCOLOS

Son un conjunto de reglas y procedimientos que deben seguirse para la correcta comunicación entre sistemas de información.

PROXY

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

RED DE ENTREGA DE CONTENIDO (CDN)

Es una red de computadores en la cual se disponen copias de datos alojados en diferentes lugares de la red, con el objetivo de que los usuarios puedan tener un acceso más rápido a dichos datos.

RFC 4646

Es un estándar de etiquetas para identificar lenguajes de programación.

RFC

Es un documento formal del Grupo de trabajo de ingeniería de Internet (IETF) el cual es resultado de la redacción del comité y la revisión posterior de las partes interesadas.

SEGURIDAD DE LA CAPA DE TRANSPORTE (TLS)

Se encarga de proporcionar privacidad e integridad de datos entre dos aplicaciones que se comunican a través del Internet.

SERVICIOS WEB

Es una tecnología que se utiliza para intercambiar datos entre aplicaciones, implementando ciertos estándares y protocolos.

SINDICACIÓN REALMENTE SIMPLE (RSS)

Es un formato XML para distribuir contenido en la web.

SISTEMAS DE NOMBRE DE DOMINIOS (DNS)

Es un sistema de nombres jerárquicos los cuales son traducidos en direcciones IP.

SOFTWARE

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

TEXTO SIMPLE (TXT)

Es un documento de texto plano.

VALORES SEPARADOS POR COMAS (CSV)

Es un formato de archivo de datos que su contenido está separado por comas.

VALORES SEPARADOS POR TABULACIONES (TSV)

Es un formato de texto simple utilizado para el almacenamiento de información en forma de tablas. En este, cada registro de la tabla representa una línea del archivo de texto.

VOCABULARIO PARA CATÁLOGO DE DATOS (DCAT)

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.

WEB

Es un sistema de documentación de hipertexto distribuido, los cuales se encuentran interconectados y son accesibles desde el Internet.

XML ABIERTO ESTRICTO

Es un formato de archivo abierto destinado para el almacenamiento de hojas de cálculo, gráficas, presentaciones y documentos de texto. También conocido como Strict Office Open XML.

ZIP

Es un formato de compresión de archivos sin pérdida que comprime cada uno de los archivos de forma separada.

ABREVIATURAS Y ACRÓNIMOS

No.	Abreviatura	Inglés	Español
1	AGRkMS	Australian Government Recordkeeping Metadata Standard	Estándar de metadatos de mantenimiento de registros del gobierno australiano
2	ASN.1	Abstract Syntax Notation 1	Notación Sintáctica Abstracta 1
3	API	Application Programming Interface	Interfaz De Programación De Aplicaciones
4	ATOM	Atom Syndication Format	Formato de Redifusión Atom
5	CIGETIC	NA	Comité de implementación y Gestión de Estándares TIC
6	CSS	Cascading Style Sheets	Hojas de Estilo en Cascada
7	CDN	Content Delivery Network	Red de Entrega de Contenido
8	CSV	Comma-Separated Values	Valores Separados por Comas
9	DCAT	Data Catalog Vocabulary	Vocabulario para Catálogo de Datos
10	DNS	Domain Name System	Sistemas de Nombre de Dominios
11	e-EMGDE	NA	Metadatos para la Gestión del Documento Electrónico
12	EIF	European Interoperability Framework	Marco Europeo de Interoperabilidad
13	ESI	Electronic Signatures and Infrastructures Technical Report	Firmas e Infraestructuras Electrónicas
14	ETSI TR	European Telecommunications Standards Institute Technical Report	Reporte Técnico del Instituto Europeo de Normas de Telecomunicaciones
15	FTP	File Transfer Protocol	Protocolo de Transferencia de Archivos
16	FTPS	File Transfer Protocol / Secure Sockets Layer	Protocolo de Transferencia de Archivos / Protocolo de Capa de Conexión Segura
17	GZIP	GZIP	Zip bajo licencia GNU
18	HTML	Hyper Text Markup Language	Lenguaje de Marcas de Hipertexto
19	HTTP	Hypertext Transfer Protocol	Protocolo de Transferencia de Hipertexto
20	ICAP	Internet Content Adaptation Protocol	Protocolo de Adaptación de Contenidos de Internet
21	IEC	International Electrotechnical Commission	Comisión Electrotécnica Internacional

22	IPSec	IP Secure	Seguridad del Protocolo IP
23	JPG/JPEG	Joint Photographic Experts Group	Grupo Conjunto de Expertos en Fotografía
24	JSON	JavaScript Object Notation	Notación de Objetos de JavaScript
25	JSON-RPC	JSON - Remote Procedure Call	JSON- Llamada a Procedimiento Remoto
26	JWT	JSON Web Tokens	No Disponible
27	LDAP	Lightweigth Directory Access Protocol	Protocolo Ligero de Acceso a Directorios
28	MoReq	Model Requirements for the Management of Electronic Documents and Records	Modelo de requisitos para la gestión de documentos electrónicos y registros
29	N/D	NA	No Disponible
30	N3	Notation 3	
31	Notación 3		
32	NIEM	National Information Exchange Model	Modelo De Intercambio De Información Nacional
33	NORTIC	NA	Normas sobre Tecnologías de la Información y Comunicación
34	NTP	Network Time Protocol	Protocolo de Tiempo de Red
35	OAuth	Open Authorization	Protocolo De Autorización Abierta
36	OCSP	Online Certificate Status Protocol	Protocolo de Estado de Certificados Fuera de Línea
37	ODATA	Open Data Protocol	Protocolo de Datos Abierto
38	ODF	Open Document Format	Formato de Documento Abierto
39	OGTIC	NA	Oficina Gubernamental de Tecnología de la Información y Comunicación
40	OSI	Open System Interconnection	Sistemas de Interconexión Abiertos
41	PDF	Portable Document File	Formato de Documento Portátil
42	PNG	Portable Network Graphics	Gráficos de Red Portátiles
43	PREMIS	Preservation Metadata: Implementation Strategies	Metadatos de Preservación: Estrategias de Implementación
44	RDF	Resource Description Framework	Marco de Descripción de Recursos
45	RDFa	Resource Description Framework in Attributes	Marco de Descripción de Recursos en Atributos

46	REST	Representational State Transfer	Transferencia de Estado Representacional
47	RFC	Request for Comments	Solicitud De Comentarios
48	RSS	Really Simple Syndication	Sindicación Realmente Simple
49	SAML	Security Assertion Markup Language	Lenguaje de Marcado para Confirmaciones de Seguridad
50	SHA	Secure Hash Algorithms	Algoritmo Hash Seguro
51	SOAP	Simple Object Access Protocol	Protocolo de Acceso a Objetos Simple
52	SQL	Structured Query Language	Lenguaje De Consulta Estructurada
53	SSH	Secure Shell	Intérprete de Órdenes Segura
54	SSL	Secure Sockets Layer	Capa de Conexión Segura
55	SVG	Scalable Vector Graphics	Gráficos Vectoriales Redimensionables
56	TIC	NA	Tecnología de la Información y comunicación
57	TIFF	Tagged Image File Format	Formato de Archivo de Imagen Etiquetado
58	TLS	Transport Layer Security	Seguridad de la Capa de Transporte
59	TSV	Tab-Separated Values	Valores Separados por Delimitadores
60	TXT	Text File	Documento de Texto
62	URI	Uniform Resource Identifier	Identificador Uniforme de Recursos
63	URL	Uniform Resource Locator	Localizador de Recurso Uniforme
64	URN	Uniform Resouce Names	Nombre de Recurso Uniforme
65	UTF-8	8-bit Unicode Transformation Format	Formato de Transformación Unicode de 8-bit
66	WSDL	Web Services Description Language	Lenguaje de Descripción de Servicios Web
67	WS-I	Web Services Interoperability Organization	Organización para la Interoperabilidad de Servicios Web
68	WS-Security	Web Services Security	Seguridad en Servicios Web
69	XAdES	XML Advanced Electronic Signatures	Firma Electrónica Avanzada XML
70	XHTML	eXtensible HyperText Markup Language	Lenguaje de Marcas de Hipertexto Extensible

71	XML	eXtensible Markup Language	Lenguaje de Marcas Extensible
72	XML-DSig	XML Singnature	Firma XML
73	XSD	XML Schema Definition	Esquema de Definición XML
74	ZIP	ZIP	Su traducción literal sería "Cremallera", aduciendo a su función de comprimir.

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. Capas del modelo OSI.

Anexo B. Normalización de Bases de datos.

Normalización de bases de datos

Características

EQUIPO DE TRABAJO

Ministerio de Administración Pública (MAP)

Dario Castillo Lugo, Ministro

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

Pedro Antonio Quezada Cepeda, Director General

Dirección de Transformación Digital Gubernamental

Armando Manzueta, Director

Departamento de Normas y Estándares (OGTIC)

Ginsy Aguilera, Encargada

Christian Gil, Encargado de la División de Investigación y Documentación

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

Kelvin Osorio, Encargado de la División de Implementación de Normas

Enyer Pérez, Analista de Normas y Estándares

Luis Acosta, Analista de Normas y Estándares

Tahirí Durán, Analista de Normas y Estándares

Jason Crisótomo, Analista de Normas y Estándares

Carlos Guerrero, Especialista de Normas y Estándares

Junior Féliz, Monitor de Normas y Estándares

Colaboradores

Carmen Féliz Arias

Luis Matos

Kevin Jiménez

Oscaury Ventura

Francis Fulgencio

Gustavo Valverde

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