Presidencia de la República Dominicana

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

DEPARTAMENTO DE ESTANDARIZACIÓN,
NORMATIVAS Y AUDITORÍA TÉCNICA

NORTIC A4 2014

NORMA PARA LA INTEROPERABILIDAD ENTRE LOS ORGANISMOS DEL GOBIERNO DOMINICANO

CAPÍTULO V
INTEROPERABILIDAD TÉCNICA

Santo Domingo, República Dominicana
10 de junio, 2014

Esto es solo un extracto de la NORTIC A4:2014, correspondiente al capitulo V, para mayor información, consultar la norma en su versión completa.

NORTIC A4:2014
Norma para la Interoperabilidad entre los Organismos del Gobierno Dominicano

Edición: 1era.
Departamento de Estandarización, Normativas y Auditoría Técnica
Fecha de aprobación: 22 de enero de 2014
Fecha de lanzamiento: 10 de junio de 2014

Categoría: A
Serie de documento: 1
Año de publicación: 2014
Versión 0.1.0

Impreso en República Dominicana

CONTENIDO

PRÓLOGO

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), es el organismo del Estado Dominicano responsable de fomentar el uso de las tecnologías de la información y comunicación (TIC), creado mediante el decreto No. 1090-04, en fecha 3 de septiembre de 2004, como dependencia directa del Poder Ejecutivo, 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.

Para el aseguramiento del correcto uso e implementación de las TIC en el Estado, la OPTIC crea el departamento de Estandarización, Normativas y Auditoría Técnica (ENAT), el cual elabora y establece las normas y estándares tecnológicos que impulsen el gobierno electrónico en el país.

Estas normas sobre TIC, denominadas NORTIC, son creadas desde el año 2013 por el ENAT, bajo el mandato del Ing. Armando García, director general de la OPTIC, y en el gobierno del Presidente de la República Dominicana, Lic. Danilo Medina.

Las NORTIC fueron concebidas para normalizar, estandarizar y tener una herramienta de auditoría para el efectivo uso e implementación de las TIC en la administración pública, con el fin de llegar a la completa homogeneidad y mejora de los procesos entre los organismo gubernamentales.

En este contexto, se han definido 5 categorías o tipos de NORTIC, según el alcance de estas, para ser difundidas e implementadas en toda la administración pública, como se presenta a continuación:

1. Categoría A (normas universales), para los aspectos normativos que aplican a todos los organismos gubernamentales.

2. Categoría B (normas para los departamentos de TIC), para aquellas

normas necesarias y exclusivas a la efectiva gestión de los departamentos o áreas de TIC dentro de los distintos organismos del Estado Dominicano.

3. Categoría C (normas municipales), para las normas que aplican a las iniciativas de TIC en los ayuntamientos o municipios.

4. Categoría D (normas para embajadas), para las normas que aplican únicamente a las iniciativas de TIC de las embajadas, consulados o misiones en el extranjero.

5. Categoría E (normas especiales), para las normas que aplican a organismos gubernamentales con características específicas dependiendo de sus funciones y estructura orgánica, así como para iniciativas, proyectos o programas de Gobierno, en el cual se haga uso de las TIC.

De modo, que esta Norma para la Interoperabilidad[6] entre los Organismos del Gobierno Dominicano, por tener un alcance universal, pertenece a la categoría A; mientras que por ser la cuarta NORTIC en elaborarse, su denominación sería NORTIC A4:2014, siendo los últimos 4 dígitos los referidos al año de lanzamiento de esta norma.

En algunos casos, esta normativa puede presentarse de la forma siguiente NORTIC A4-1:2014, seguida de trece caracteres (#####-##-######), donde el número "1" que aparece después del guion (-) especifica la serie del documento (1 para directrices, 2 para guías de implementación, 3 para código de buenas prácticas, entre otros) y los demás caracteres, el Número de Identificación Único (NIU) para cada organismo del Estado.

La evaluación de cada NORTIC es realizada por dos comités, la primera evaluación es ejecutada por el Comité Interno para Evaluación de las Normas (CIEN), el cual está conformado por expertos en TIC dentro de la OPTIC, mientras que la segunda evaluación es realizada por el Comité de Estándares de Tecnologías de la Información y Comunicación (COETIC), el cual está conformado por los responsables de TIC de cada organismo gubernamental, o a quienes la máxima autoridad de cada organismo designe.

En vista de la responsabilidad de la OPTIC en la elaboración de políticas, estrategias y controles de TIC y de los avances en el uso de las tecnologías, de los cuales los organismos gubernamentales no quedan al margen, surge esta

[6] Es la capacidad que tiene un sistema de información para intercambiar datos con otros sistemas con la capacidad de procesarlos.

MARCO LEGAL

La OPTIC, 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. El **Decreto 1090-04**, a través del cual se constituye la OPTIC 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.

2. Para el tratamiento de los derechos sobre la protección de datos[7] 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

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

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.

3. 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.

4. 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 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.

5. 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[8], 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.

6. La **Ley No. 126-02** sobre comercio electrónico, documentos y firma digital.

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

7. 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.

8. El **Decreto No. 229-07**, el cual es el instructivo de aplicación de Gobierno Electrónico, contentivo de las pautas generales para el desarrollo de la Estrategia de Gobierno Electrónico en la República Dominicana.

9. El **Decreto No. 709-07** sobre las normas y estándares elaboradas por la OPTIC.

   - Artículo 1.- Se instruye a toda 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, auditoría 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 la comunicación (TIC) y Gobierno Electrónico.

10. El **Decreto No. 130-05**, que aprueba el reglamento de la Ley General de Libre Acceso a la Información Pública.

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

INTRODUCCIÓN

La normativa para la Interoperabilidad entre los Organismos del Gobierno Dominicano establece las directrices que deben seguir los organismos a fin de lograr interoperar con otros, permitiendo así el intercambio de información de una manera efectiva, con el objetivo de agilizar los procesos de los servicios que realizan dichos organismos reduciendo costos y evitando que el ciudadano suministre información que el Estado posee.

En esta normativa se presentan 3 dimensiones de la interoperabilidad, esenciales para que esta sea posible, las cuales son interoperabilidad organizacional, semántica y técnica. Cada una de estas dimensiones es abarcada en un capítulo diferente, conteniendo en cada uno directrices específicas para cada dimensión.

Por lo tanto, en esta norma se presenta desde el primer capítulo el alcance de la misma, la cual comprende todos los organismos de Estado Dominicano de manera mandataria, 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 elaborado un catálogo de estándares interoperables. En dicho capítulo se describen todos los elementos que conforman el catálogo, y la forma de uso y actualización del mismo.

El siguiente capítulo trata la interoperabilidad organizacional, en donde se indican los diferentes tipos de acuerdos que deben realizar los organismos para los proyectos que se lleven a cabo, siendo estos los siguientes: Acuerdos técnicos, semánticos, organizacionales, políticos, económicos y culturales. Además se definen los roles que debe poseer la unidad de administración de proyecto del departamento de TIC y el procedimiento a seguir para el correcto manejo de los proyectos de interoperabilidad.

El capítulo IV trata sobre la interoperabilidad semántica, en donde se especifican las directrices para la descripción de los servicios y los esquemas de metadatos[4] 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 presenta un conjunto de estándares tecnológicos bajo los cuales deben regirse los organismos para el intercambio de información electrónica, además se especifican las directrices para una correcta administración del código fuente[5].

[4] Son un conjunto de información que describe las características de otra información. Es "datos sobre datos".
[5] Es un conjunto de instrucciones redactas en base a las reglas sintácticas de un lenguaje de programación para desarrollar un software determinado.

CAPÍTULO 5
INTEROPERABILIDAD TÉCNICA

En este capítulo se describen y establecen 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.

Implementación de estándares abiertos

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

(i) Los estándares abiertos[6] deben cumplir con las siguientes cualidades.

- **Disponibilidad**: Deben estar disponibles para su lectura e implementación.
- **Capacidad de elección**: Debe ser posible elegir la implementación a usar del mismo, sin restringir al cliente, un distribuidor o grupo concreto.
- **Sin prebendas**: Su implementación debe estar disponible sin coste de uso.
- **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.

[6] Es una especificación técnica que está disponible al público y que es desarrollada o aprobada, afirmada y mantenida, mediante un proceso basado en el consenso.

- **Sin prácticas abusivas**: Su implementación debe evitar tácticas subversivas y cualquier acción que atente contra la privacidad de los usuarios.

SECCIÓN 5.02.

Protocolos de intercambio de datos

En esta sección se especifican los protocolos a utilizar para la transferencia de archivos, hipertexto y mensajería.

(a) Los protocolos mínimos que deben utilizarse para el intercambio de información por categoría son los siguientes:

(i) Para transferencia de archivos debe utilizarse los siguientes protocolos:

a) El Protocolo de Transferencia de Archivo Seguro (SFTP[7], por sus siglas en inglés) utilizado con el Intérprete de Órdenes Seguras (SSH[8], por sus siglas en inglés).

b) El Protocolo Seguro de Transferencia de Datos (también referido como FTPS, por sus siglas en inglés).

(ii) Para hipertexto y recursos de software debe utilizarse los siguientes protocolos:

a) El Protocolo de Transferencia de Hipertexto (HTTP[9], por sus siglas en inglés).

b) El Protocolo Seguro de Transferencia de Hipertexto (HTTPS[10], por sus siglas en inglés).

(iii) Para mensajería debe implementarse y utilizarse los siguientes protocolos, pero solo en su forma segura:

[7] Es un protocolo de red de utilizado para acceder y manejar archivos de manera remota utilizando métodos de encriptación.
[8] Es un protocolo y aplicación por el cual se accede remotamente a una computadora a través de una red de comunicación.
[9] Es un protocolo utilizado para realizar la transferencia de texto o hipervínculos, a través de la web.
[10] Es un protocolo utilizado para realizar la transferencia de texto o hipervínculos de manera segura mediante el uso de cifrado, a través de la web.

a) El Protocolo de Oficina de Correo (POP3[11], por sus siglas en inglés), utilizado con uno de los siguientes protocolos de seguridad:

   - Protocolo de Seguridad de la Capa de Transporte (TLS[12], por sus siglas en inglés) en el puerto 110.
   - Protocolo de Capa de Conexión Segura (SSL, por sus siglas en inglés) en el puerto 995.

b) El Protocolo de Acceso a Mensajes de Internet (IMAP[13], por sus siglas en inglés), utilizado con uno de los siguientes protocolos de seguridad:

   - Protocolo TLS en el puerto 143.
   - Protocolo SSL en el puerto 993.

c) El Protocolo Simple de Transferencia de Correos (SMTP[14], por sus siglas en inglés), utilizado con uno de los siguientes protocolos de seguridad:

   - Protocolo TLS en el puerto 587.
   - Protocolo SSL en el puerto 465.

SECCIÓN 5.03.

Almacenamiento de datos

Para garantizar la correcta integración en el manejo de la información se indican las directrices para lograr que las bases de datos sean compatibles con los estándares actuales de la industria para el manejo y almacenamiento de información.

[11] Es un protocolo utilizado de manera local para la obtención de correos electrónicos almacenados en un servidor remoto.
[12] Se encarga de proporcionar privacidad e integridad de datos entre dos aplicaciones que se comunican a través del internet.
[13] Es un protocolo utilizado para acceder a mensajes y correos electrónicos alojados en servidores en el internet.
[14] Hace referencia a un protocolo simple de envió de correos electrónicos.

Sub-sección 5.03.1. Bases de datos

(a) Debe utilizarse bases de datos relacionales[15] y orientadas a objetos[16] que posean compatibilidad de comunicación vía los siguientes formatos:

- Notación de Objetos de JavaScript (JSON[17], por sus siglas en inglés) y sus variantes.
- Lenguaje de Marcas Extensible (XML[18], por sus siglas en inglés) y sus variantes.
- Valores Separados por Comas (CSV[19], por sus siglas en inglés).
- Valores Separados por Tabulaciones (TSV[20], por sus siglas en inglés).

(b) Cuando se utilicen bases de datos relacionales, estas deben cumplir con las siguientes directrices:

(i) Ser compatibles con el Lenguaje de Consulta Estructurado (SQL, por sus siglas en inglés) y sus variantes.

(ii) El diseño y modelado debe estar creado de forma que cumpla con al menos 3 de las 5 formas normales de normalización de base de datos. Ver **anexo A. Normalización de Bases de datos**.

Entre algunas de las variantes de SQL se encuentran:
- *T-SQL*
- *PL/ SQL*
- *FSQL*

(c) Para la consulta, manipulación y creación de los datos y objetos[21] en base de datos orientada a objetos debe utilizarse la Interfaz de programación de Aplicaciones (API, por sus siglas en inglés), adaptada al lenguaje que esté utilizando para la aplicación o proceso de integración.

Un ejemplo de un API adaptada al lenguaje es para el caso de MongoDB utilizar el C# y .NET MongoDB Driver.

[15] Es una base de datos que permite la interconexión entre los datos almacenados en ella.
[16] Es una base de datos en la cual la información que se relaciona está representada mediante objetos de un lenguaje de programación.
[17] Es un formato ligero usado como alternativa al XML para intercambio de datos.
[18] 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.
[19] Es un formato de archivo de datos que su contenido está separado por comas.
[20] 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.
[21] Es una representación detallada de un elemento o unidad de la realidad y la misma consta de un estado y comportamiento.

Sub-sección 5.03.2. Archivos planos

(a) Los archivos planos[22] deben presentarse en los siguientes formatos descritos a continuación:

- JSON (y sus variantes).
- XML (y sus variantes).
- CSV.
- TSV.

SECCIÓN 5.04.

Extensiones y almacenamiento de archivos

En esta sección se especifican las directrices para el uso de las extensiones de archivo y como debe realizarse el almacenamiento de estos.

(a) Para el uso de extensiones debe seguirse las siguientes directrices:

(i) Puede utilizarse todas las extensiones existentes en el sector tecnológico (sin excepción) para los archivos generados, compilados o interpretados, siempre y cuando estos archivos no contengan códigos de software malicioso[23], programas espías[24] o que comprometa la seguridad de los sistemas y/o servidores del organismo.

(ii) Debe documentarse el uso de cada extensión por cada sistema desarrollado o implementado y categorizado como sigue:

- Archivos de documentos[25].

[22] Es un tipo de archivo que no contiene ningún tipo de formato.
[23] También conocido como Malware, es un software que tiene como fin, ingresar sin consentimiento del usuario al computador o sistema para causar daños.
[24] También conocido como Spyware, es in tipo de software malintencionado el cual recopila la información o datos de un computador y los envía sin consentimiento del usuario persona u organismo externo.
[25] Son archivos que contienen de manera ordenada un conjunto de documentos.

- Archivos de configuración[26].
- Archivos de recursos[27].
- Archivos temporales[28].

(b) Para el almacenamiento de archivos debe seguirse las directrices a continuación:

(i) Los archivos deben ser almacenados en espacios digitales seguros.

a) Para el almacenamiento seguro de la información, ver la **NORTIC A1:2014, sub-sección 6.02.3 Almacenamiento de la información**.

(ii) Cuando el almacenamiento se realiza de manera local, los servidores del organismo deben cumplir con lo siguiente:

a) La tecnología utilizada en los servidores para el almacenamiento de archivos por el organismo debe permitir la generación de accesos externos, mediante servicios web o vía HTTPS permitiendo la integración directa y segura con otros sistemas.

b) Almacenar los archivos en servidores, donde el sistema operativo provea seguridad a la información.

c) Los nombres de los archivos deben obedecer a un esquema o patrón definido por el organismo, el cual debe estar presente en la documentación del sistema.

d) Los nombres de los archivos no deben ser mayor de 64 caracteres.

(iii) Cuando el almacenamiento de archivos se realiza en una nube computacional[29] esta debe cumplir con las directrices especificadas en la **NORTIC A1:2014, sección 4.03. Computación en la nube**.

[26] Son un conjunto de archivos que contienen los datos o valores de las variables de un sistema, los cuales pueden ser cambiados o modificados de acuerdo a la función que se desee realizar.
[27] Son archivos que contiene la información necesaria para la realización de alguna tarea o función del sistema, como cadenas, rutas de accesos entre otros.
[28] Son archivos creados por un programa o sistema cuando la cantidad de memoria asignada en el computador no es suficiente para la realización algún proceso o tarea.
[29] Es una tecnología que permite la utilización de servicios de cómputos por medio de Internet.

a) El servicios seleccionados para el almacenamiento en nube computacional debe cumplir con al menos 2 de las siguientes certificaciones:

- ISO/IEC 27001:2005, sobre técnicas de seguridad de la información y administración de sistemas. Certificada y auditada por la ISO.
- Controles de la Empresa de Servicios 1 y 2 (SOC 1, SOC 2, por sus siglas en inglés) junto con la Declaración sobre Normas de Auditoria 16 y el Estándar Internacional en Aseguramiento de Compromisos 340 (SSAE 16/ISAE, por sus siglas en inglés), para medir el control de las informaciones financieras de una organización o empresa de servicios.
- Matriz de control en la Nube (CCM, por sus siglas en inglés), de la Alianza de Seguridad en la Nube (CSA, por sus siglas en ingles), para controles de seguridad en plataformas de clientes y proveedores de servicios computaciones en la nube.
- Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago, Nivel 1(PCI DSS, por sus siglas en inglés), sobre estándares de seguridad establecidos para ayudar a la protección de empresas y consumidores frente al robo de datos y el fraude.

b) La tecnología de almacenamiento para archivos de recursos de sistemas como lo son imágenes, documentos y archivos scripts/styles debe ser preferiblemente de tipo de Red de Entrega de Contenido (CDN[30], por sus siglas en inglés).

[30] 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.

SECCIÓN 5.05.

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 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.

Sub-sección 5.05.1. Repositorio general

(a) Para el correcto cumplimiento de la presente normativa, la administración del código fuente debe regirse bajo los siguientes requisitos:

(i) Para el control de las versiones de aplicaciones debe utilizarse la tecnología de manejo distribuido de versiones GIT[31].

(ii) El código fuente solo debe estar disponible localmente en el computador de trabajo de los desarrolladores y en el repositorio remoto de GIT asignado por la OPTIC.

(iii) Debe colocarse un comentario detallado de forma obligatoria en cada "Commit[32]" que se realice en la plataforma.

(iv) Cada versión completamente funcional de la solución debe estar separada por "Branches[33]" dentro del repositorio de GIT para la corrección.

(v) El código fuente de todas las soluciones desarrolladas para cualquier organismo gubernamental debe estar guardado en su última versión en los servidores de GIT autorizados por la OPTIC.

[31] 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.
[32] Es una confirmación de algún cambio en el repositorio GIT.
[33] Es un apuntador móvil dirigido a una de las confirmaciones o "commit".

Sub-sección 5.05.2. Comentarios y formatos

(a) Debe utilizarse nombres descriptivos para entidades 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 y seguir un modelo basado en los aspectos siguientes:

- Incluir en cada clase una breve descripción, su autor y fecha de última modificación.
- Incluir por cada método[34], una descripción de su objeto y funcionalidades, así como de los parámetros[35] y resultados obtenidos.

(ii) Los comentarios deben explicar de manera breve la funcionalidad de un método antes de su declaración[36].

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 el código fuente para permitir una mejor compresión del lector.

Ejemplos de documentación por lenguaje de programación:

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

[34] Es un fragmento de código el cual puede ser utilizado o invocado por otro sistema para la realización de una tarea en específica.
[35] Es una variable la cual puede ser recibida por un método o procedimiento.
[36] Consiste en la asignación de un nombre a una entidad en específico.

(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.

SECCIÓN 5.06.

Interoperabilidad web

Se especifican los protocolos y lenguajes que permitirán un efectivo intercambio de datos entre aplicaciones.

(a) Los lenguajes de programación que deben utilizarse para interfaces de usuario son los siguientes:

(i) La interfaz de usuario de las aplicaciones deben estar codificadas en los siguientes lenguajes:

- Lenguaje de Marcas de Hipertexto, versión 5 (HTML5, por sus siglas en inglés).
- HTML[37] extensible (XHTML[38], por sus siglas en inglés).

(ii) Para los lenguajes de estilo deben utilizarse las Hojas de Estilos en Cascada (CSS[39], por sus siglas en inglés).

a) Solo serán permitidas las versiones 2.1 o superiores.

b) Solo serán permitidas las librerías[40] basadas en archivos de órdenes que sirvan para la creación y manipulación de estilos de forma dinámica.

Ejemplos de libreria basadas en archivos de órdenes más utilizadas: LESS, SASS y Stylus.

[37] Es el lenguaje de programación utilizado para la creación de páginas web.
[38] 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.
[39] Es un lenguaje de programación para la web destinado a dar estilo visual.
[40] Son un conjunto de códigos, datos o funciones que brindan soporte a un sistema y pueden ser utilizadas de acuerdo a la necesidad para la que se le solicite.

(iii) Debe utilizarse solo las tecnologías de lenguajes interpretados basadas en JavaScript.

Ejemplos de marcos de trabajo de programación basados en Javascript: AngularJS, EmberJS, KnockoutJS, BackboneJS.

(b) Para el intercambio de información debe cumplirse con lo siguiente:

(i) Debe utilizarse servicios web, utilizando protocolos de transferencia estándares en la web[41], como lo son:

- JSON- Llamada a Procedimiento Remoto (JSON-RPC, por sus siglas en inglés).
- JSON- Protocolo de Servicio Web (JSON-WSP[42], por sus siglas en inglés).
- Transferencia de Estado Representacional (REST, por sus siglas en inglés).
- Protocolo de Acceso de Objeto Simple (SOAP[43], por sus siglas en inglés).
- Servicio de Procesamiento Web (WPS, por sus siglas en inglés).
- Lenguaje de Descripción de Servicios Web (WSDL[44], por sus siglas en inglés).

SECCIÓN 5.07.

Aspectos generales de seguridad

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

(b) En caso de utilizar otro método para la interoperabilidad con otros sistemas debe enviarse la justificación de uso al correo electrónico enat@optic.gob.do para que fines de evaluación del requerimiento.

[41] Es un sistema de documentación de hipertexto distribuido, los cuales se encuentran interconectados y son accesibles desde el internet.
[42] Es un protocolo de servicio Web usado por JSON para la descripción de servicios, respuestas y solicitudes.
[43] Es un protocolo estándar de comunicación entre dos objetos por medio de XML.
[44] Es un protocolo basado en XML que se utiliza para describir servicios web.

GLOSARIO DE TÉRMINOS

Archivo de órdenes

También conocido como Scripts, es un tipo de programa comúnmente creado en base a un archivo de texto plano, utilizado para la realización de una o más tareas.

Archivos de configuración

Son un conjunto de archivos que contienen los datos o valores de las variables de un sistema, los cuales pueden ser cambiados o modificados de acuerdo a la función que se desee realizar.

Archivos de documentos

Son archivos que contienen de manera ordenada un conjunto de documentos.

Archivos de recursos

Son archivos que contiene la información necesaria para la realización de alguna tarea o función del sistema, como cadenas, rutas de accesos entre otros.

Archivos planos

Es un tipo de archivo que no contiene ningún tipo de formato.

Archivos temporales

Son archivos creados por un programa o sistema cuando la cantidad de memoria

Branches / Ramas

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

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 / Confirmación de cambio

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.

Datos

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

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.

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.

Capa de presentación

Es donde se presenta de manera visual la información que provee el sistema al usuario de forma que este pueda entenderla e interactuar con ella.

Cifrado de datos

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

Hoja de estilo en cascada (CSS)

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

Interoperabilidad

Es la capacidad que tiene un sistema de información para intercambiar datos con otros sistemas con la capacidad de procesarlos.

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.

Lenguaje de Descripción de Servicio Web(WSDL)

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

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.

Librerías

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

Método

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

Notación de Objetos de JavaScript (JSON)

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

Parámetros

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

Programa espía

También conocido como Spyware, es in tipo de software malintencionado el cual

recopila la información o datos de un computador y los envía sin consentimiento del usuario persona u organismo externo.

Protocolo de Acceso a Mensajes de Internet (IMAP)

Es un protocolo utilizado para acceder a mensajes y correos electrónicos alojados en servidores en el internet.

Protocolo de Acceso a Objetos Simple (SOAP)

Es un protocolo estándar de comunicación entre dos objetos por medio de XML.

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.

Protocolo de Servicio Web JSON (JSON-WSP)

Es un protocolo de servicio Web usado por JSON para la descripción de servicios, respuestas y solicitudes.

Protocolo de Transferencia de Archivos Seguro (SFTP)

Es un protocolo de red de utilizado para acceder y manejar archivos de manera remota utilizando métodos de encriptación.

Protocolo de Transferencia de Archivos/ Capa de Conexión Segura (FTP/SSL)

Es un protocolo utilizado para la transferencia de archivos, el cual utiliza las propiedades de seguridad brindadas por el SSL para la comunicación.

Protocolo de Transferencia de Hipertexto (HTTP)

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

Protocolo Seguro de Transferencia de Hipertexto (HTTPS)

Es un protocolo utilizado para realizar la transferencia de texto o hipervínculos de manera segura mediante el uso de cifrado, a través de la web.

Protocolo para la Transferencia Simple de Correo Electrónico (SMTP)

Hace referencia a un protocolo simple de envió de correos electrónicos.

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.

Seguridad en los Servicios Web (WS-Security)

Es un protocolo de comunicaciones que permite agregar seguridad a los servicios web.

Software malicioso

También conocido como Malware, es un software que tiene como fin, ingresar sin consentimiento del usuario al computador o sistema para causar daños.

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.

ABREVIATURAS Y ACRÓNIMOS

No.	Abreviaturas y Acrónimos	Inglés	Español
1	CCM	Cloud Control Matrix	Matriz de Control en la Nube
2	CDN	Content Delivery Network	Red de Entrega de Contenido
3	CIEN	N/A	Comité Interno para Evaluación de las Normas
4	COETIC	N/A	Comité de Estándares de Tecnologías de la Información y Comunicación
5	CSA	Cloud Security Alliance	Alianza de Seguridad en la Nube
6	CSV	Comma-Separated Values	Valores Separados por Comas
7	ENAT	N/A	Estandarización, Normativas y Auditoría Técnica
8	ESI	Electronic Signatures and Infrastructures Technical Report	Firmas e Infraestructuras Electrónicas
9	ETSI TR	European Telecommunications Standards Institute Technical Report	Reporte Técnico del Instituto Europeo de Normas de Telecomunicaciones
10	Etx.	Extension	Extensión
11	FTP	File Transfer Protocol	Protocolo de Transferencia de Archivos
12	FTPS	File Transfer Protocol / Secure Sockets Layer	Protocolo de Transferencia de Archivos / Protocolo de Capa de Conexión Segura
13	HTML	Hyper Text Markup Language	Lenguaje de Marcas de Hipertexto
14	HTML5	Hyper Text Markup Language, version 5	Lenguaje de Marcas de Hipertexto, versión 5
15	HTTP	Hypertext Transfer Protocol	Protocolo de Transferencia de Hipertexto

15	HTTPS	Hypertext Transfer Protocol Secure	Protocolo Seguro de Transferencia de Hipertexto
16	IEC	International Electrotechnical Commission	Comisión Electrotécnica Internacional
17	IMAP	Internet Message Access Protocol	Protocolo de Acceso a Mensajes de Internet
18	ISAE	International Standard on Assurance Engagements	Estándar Internacional en Aseguramiento de Compromisos
19	JSON	JavaScript Object Notation	Notación de Objetos de JavaScript
20	JSON-RPC	JSON - Remote Procedure Call	JSON- Llamada a Procedimiento Remoto
21	JSON-WSP	JSON – Web Service Protocol	JSON – Protocolo de Servicio Web
22	NORTIC	N/A	Normas sobre Tecnologías de la Información y Comunicación
23	NTI	N/A	Norma Técnica de Interoperabilidad
24	NTP	Network Time Protocol	Protocolo de Tiempo de Red
25	OCSP	Online Certificate Status Protocol	Protocolo de Estado de Certificados Fuera de Línea
26	OPTIC	N/A	Oficina Presidencial de Tecnología de la Información y Comunicación
27	POP3	Post Office Protocol version 3	Protocolo de Oficina de Correo, versión 3
28	REST	Representational State Transfer	Transferencia de Estado Representacional
29	SFTP	Secure File Transfer Protocol	Protocolo Seguro de Transferencia de Archivos
30	SMTP	Simple Mail Transfer Protocol	Protocolo para la Transferencia Simple

31	SOAP	Simple Object Access Protocol	Protocolo de Acceso a Objetos Simple
32	SSAE	Statement on Standards for Attestation Engagements	Estándar Internacional en Aseguramiento de Compromisos
33	SSH	Secure Shell	Intérprete de Órdenes Segura
34	SSL	Secure Sockets Layer	Capa de Conexión Segura
35	TIC	N/A	Tecnología de la Información y comunicación
36	TLS	Transport Layer Security	Seguridad de la Capa de Transporte
37	TSV	Tab-Separated Values	Valores Separados por Delimitadores
38	WPS	Web Processing Service	Servicio de Procesamiento Web
39	WSDL	Web Services Description Language	Lenguaje de Descripción de Servicios Web
40	XHTML	eXtensible HyperText Markup Language	Lenguaje de Marcas de Hipertexto Extensible
41	XML	eXtensible Markup Language	Lenguaje de Marcas Extensible

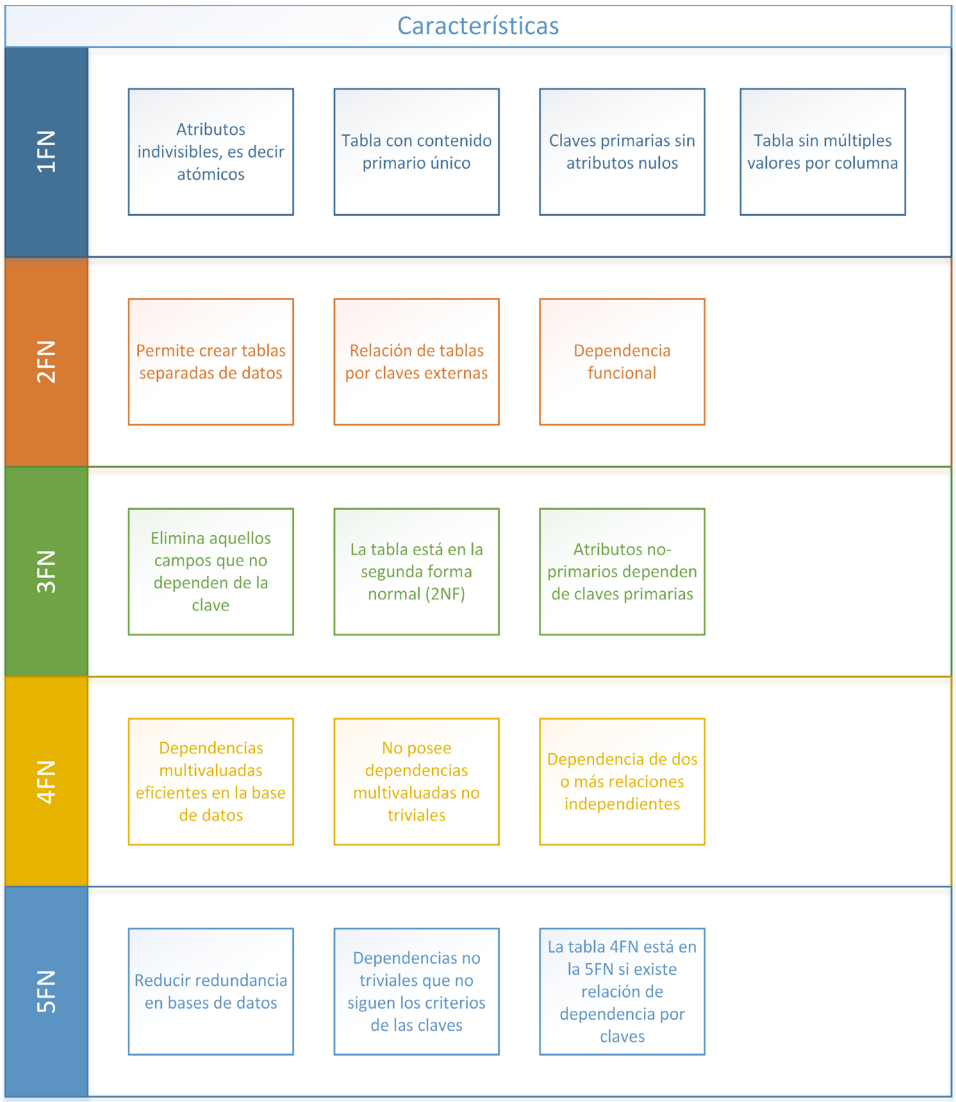
BIBLIOGRAFÍA

- Comisión Económica para América Latina y el Caribe (CEPAL). (2007). Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe. División de Desarrollo Productivo y Empresarial de la CEPAL.
- Consorcio World Wide Web (W3C). (2008). Sintaxis XML Signature y Procesamiento. Segunda Edición. New York.
- Criado, J. I., Mila Gascó, & Carlos E. Jiménez. (2010). Bases para una Estrategia Iberoamericana de Interoperabilidad. Documento para la consideración de la XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado.
- Departamento de Defensa de los Estados Unidos. (1998). Levels of Information Systems Interoperability (LISI). Estados Unidos.
- European Telecommunications Standards Institute. (2003). ETSI TR 102 272. Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies. República Francesa.
- European Telecommunications Standards Institute. (2009). ETSI TS 101 903. XML Advanced Electronic Signatures (XAdES). República Francesa.
- Gobierno Bolivariana de Venezuela. (2010). Marco de Interoperabilidad. Marco de Interoperabilidad para el Estado Venezolano V 1.0. República Bolivariana de Venezuela: Publicsol 50 C.A.
- Gobierno Bolivariano de Venezuela. (2012). Avances en la Implementación de la Interoperabilidad en Venezuela. República Bolivariana de Venezuela: Centro Nacional de Tecnología de información (CNTI).
- Gobierno Bolivariano de Venezuela. (2013). Interoperabilidad en Venezuela. Integrando los Servicios del Estado. República Bolivariana de Venezuela.
- Gobierno de España. (2010). Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. España.
- Gobierno de España. (2011). Guía de Aplicación de la Norma Técnica de Interoperabilidad. Digitalización de Documentos. Madríd: Dirección

- General para el Impulso de la Administracíon Electrónica.
- Gobierno de España. (2012). Catálogo De Estándares. Guía de aplicación de la Norma Técnica de Interoperabilidad. España: Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica.
- 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.
- Grupo de Trabajo de la Red de S. Josefsson, Ed. (2003). El Base16, Base32, y Base64 de datos Codificaciones.
- International Organization for Standardization / International Electrotechnical Comission. (2006). ISO 26300. Information Technology - Open Document Format for Office Applications (OpenDocument) v, 1.0. Suiza.
- Moreno, J. L. (s.f.). Gestión estratégica de la interoperabilidad. Necesidades normativas en la adaptación a los cambios sociales y tecnológicos.
- Network Working Group. (2008). The Transport Layer Security (TLS) Protocol).
- Oficina Nacional de Gobierno (ONGEI). (s.f.). Interoperabilidad en el Estado Peruano. República del Perú: Oficina Nacional de Gobierno Electrónico e Informática.
- Organización Internacional de Normalización (ISO). (1986). ISO 8879. Procesamiento de la información - texto y de oficina - sistemas Generalizado Estándar Markup Language (SGML).
- Organización Internacional de Normalización (ISO). (1994). ISO/IEC 7498-1. Information technology - Open Systems Interconnection – Basic Reference Model: The Basic Model.
- República de Colombia. (2010). Marco de Interoperabilidad para Gobierno en línea. Manual para la Interoperabilidad del Gobierno en línea. República de Colombia.

ANEXOS

Anexo A. Normalización de bases de datos



EQUIPO DE TRABAJO

Dirección General
Armando García, Director General

Departamento de Estandarización, Normativas y Auditoría Técnica (ENAT)
Elvyn Peguero, Gerente del ENAT

Ginsy Aguilera, Analista de Estándares y Normativas

Shalem Pérez, Analista de Estándares y Normativas

Winner Núñez, Analista de Estándares y Normativas

Ariel Acosta, Consultor de Estándares y Normativas

Asesor
Luis Guzmán, experto en TIC

Comité Interno para Evaluación de las Normas (CIEN) – Equipo OPTIC
Charli Polanco, Director de TIC

José Luis Liranzo, Director de DiGOB

Miguel Guerra, Gerente Multimedia

Comité de Estándares de Tecnologías de la Información y Comunicación (COETIC)

Dahiri Espinosa
Dirección General de Ética e Integridad Gubernamental (DIGEIG)

Alfonso Espinal
Instituto Dominicano de las Telecomunicaciones (INDOTEL)

Ubaldo Pérez
Ministerio de Hacienda (MH)

Colaboradores

Carmen Feliz, OPTIC

Eliaquín Encarnación, OPTIC

Miguel Rodríguez, OPTIC

Joel Jaime, OPTIC

Samuel Luis, OPTIC

Luis Santiago, DIGEIG

Cecilia Chávez, MH

Juan Ciprián, INDOTEL

Jorge Cabeza, Microsoft Dominicana

Juan Lozada, Microsoft Dominicana

Eduardo Núñez Parodi, Microsoft Corporation