Presidencia de la República Dominicana

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

Departamento de Estandarización, Normativas y Auditoría Técnica

NORTIC A1 2014

GOBIERNO ELECTRÓNICO
REPÚBLICA DOMINICANA

NORMA GENERAL SOBRE USO E IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana
15 de Mayo, 2014

Presidencia de la República Dominicana

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

DEPARTAMENTO DE ESTANDARIZACIÓN,
NORMATIVAS Y AUDITORÍA TÉCNICA

NORTIC A1 2014

NORMA GENERAL SOBRE EL USO E IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana
15 de mayo, 2014

NORTIC A1:2014
Norma General sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano

Edición: 1era.
Departamento de Estandarización, Normativas y Auditoría Técnica
Fecha de aprobación: 23 de abril de 2014
Fecha de lanzamiento: 15 de mayo 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 Tecnologías de la Información y Comunicación (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 General sobre Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano, por tener un alcance universal, pertenece a la categoría A; mientras que por ser la NORTIC general, la cual abarca todos los temas de las actuales normativas, su denominación sería NORTIC A1:2014, 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 A1-1:2014, 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

normativa con las directrices y recomendaciones para garantizar el uso efectivo de las plataformas y los procesos tecnológicos que son implementados por cada uno de dichos organismos.

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[1] 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.

[1] 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.

- 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.

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 340-06** sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, en donde se establecen los principios y normas generales que rigen la contratación pública, relacionada con los bienes, obras, servicios y concesiones del Estado.

6. 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[2]: 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[3], 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

[2] Hace referencia a la persona que consume o manipula un producto, servicio o información.
[3] Es un servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.

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[4].

7. La **Ley 126-02** sobre Comercio Electrónico, Documentos y Firma Digital.
8. La **Ley 42-2000** sobre Discapacidad en la República Dominicana.
9. La **Ley 65-00** sobre Derecho de Autor[5].

- Artículo 2.- El derecho de autor comprende la protección de las obras literarias y artísticas, así como la forma literaria o artística de las obras científicas, incluyendo todas las creaciones del espíritu en los campos indicados, cualquiera que sea el modo o forma de expresión, divulgación, reproducción o comunicación, o el género, mérito o destino, incluyendo pero no limitadas a:

  - Los programas de computadoras, en los mismos términos que las obras literarias, sean programas fuente o programas objeto, o por cualquier otra forma de expresión, incluidos la documentación técnica y los manuales de uso;

  - Las bases o compilaciones de datos u otros materiales, legibles

[4] Es un documento digital que permite garantizar la identidad de una persona en la red, a través de una firma electrónica. Se utiliza como una forma segura de garantizar la autentificación, integridad y confidencialidad de la información.

[5] Es el conjunto de leyes y principios que provee protección a los autores, artistas y demás creadores para sus creaciones.

por máquina o en cualquier otra forma, que por la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, pero no de los datos o materiales en sí mismos y sin perjuicio del derecho de autor existente sobre las obras que puedan ser objeto de la base o compilación;

10. El **Decreto 694-09**, que establece el Sistema 311 de Denuncias, Quejas y Reclamaciones como medio principal de comunicación para la recepción y canalización de denuncias, quejas y reclamaciones.

(a) Artículo 5.- Se instruye a todas las instituciones del sector público a incluir un enlace[6] en su portal web[7] hacia www.311.gob.do.

11. El **Decreto 175-08**, que instruye a los organismos de la administración pública a reservar su nombre de dominio bajo las jerarquías de GOB. DO y GOV.DO.

12. El **Decreto 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.

13. El **Decreto 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.

14. El **Decreto 228-07**, que establece el Centro de Contacto Gubernamental *GOB (*462), como canal de voz oficial y principal punto de contacto

[6] Los enlaces, también conocidos como hipervínculos o hiperenlaces, son elementos dentro de un portal web que hacen referencia a otros contenidos que se encuentran dentro del mismo portal web o en un portal externo.

[7] Es un conjunto de páginas electrónicas que presentan información y recursos de interés al usuario.

comunicacional para atención telefónica del ciudadano en el Gobierno Dominicano.

- Artículo 6.- Se instruye para que todas las instituciones públicas aseguren una oferta creciente de servicios normalizados, de atención e información, a través del Centro de Contacto Gubernamental *GOB, y a anunciar sus programas nacionales a través de dicho canal de voz oficial.

15. El **Decreto 615-07**, que instruye a la OPTIC a coordinar el procedimiento para la elaboración de los inventarios[8] respecto a los programas incorporados a las computadoras y su licenciamiento.

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

17. La **Resolución 51-2013**, que aprueba los modelos de estructura organizativa permitidos para las unidades de TIC de todos los organismos del sector público.

[8] Es un registro organizado de los activos pertenecientes o bajo la responsabilidad de un organismo determinado.

INTRODUCCIÓN

La Norma General sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano, es un documento que establece el modelo, directrices y recomendaciones que debe seguir cada organismo del Gobierno Dominicano sobre el uso e implementación de TIC, con el objetivo de estandarizar los procesos y plataformas utilizados en la administración pública, de modo que se pueda lograr una gestión más efectiva de los recursos tecnológicos en cada organismo, así como mejorar la calidad en los servicios prestados por los organismos a los ciudadanos.

En esta norma se presentan cada uno de los aspectos, que en su mayoría, son generales para cada organismo gubernamental y los cuales ameritan de una normativa que regule la gestión de estos. Cada uno de estos temas se presenta como capítulos y describen todo lo necesario para lograr el cumplimiento de esta normativa en toda la administración pública.

En tal sentido, en esta norma también conocida como NORTIC A1, se indica desde el primer capítulo el alcance de la misma, la cual comprende todos los organismos del Estado Dominicano de manera mandataria. Además, se indican aquellas directrices de aplicación general que cada organismo debe cumplir en los diferentes aspectos de TIC.

En el segundo capítulo, el cual tiene por objetivo garantizar la eficiente gestión del departamento de TIC, se establecen las directrices para definir la correcta composición de la estructura y los distintos roles dentro de este departamento. Además, en este capítulo se dispone de las diferentes políticas generales del departamento y la administración de los servicios brindados por los organismos gubernamentales.

En el capítulo siguiente sobre implementación TIC, se indican las directrices que deben seguir los organismos gubernamentales en la gestión de sus proyectos

de TIC, así como también las pautas que deben cumplir al momento de realizar alguna compra o contratación de servicios.

En el capítulo sobre infraestructura de TIC[9], se presentan las directrices para que cada organismo logre estructurar, configurar y mantener su infraestructura TIC a nivel de conectividad, documentación y servicios computacionales en la nube, de modo que pueda ser interoperable y sostenible en el tiempo.

Siguiendo con el quinto capítulo sobre software gubernamental[10], en el cual se indica las directrices en que cada organismo debe seguir para lograr una mejor administración y utilización del software[11]. También se indica la metodología para el desarrollo del software gubernamental y como debe ser utilizado el software de código abierto en la administración pública.

La seguridad TIC, tratada en el capítulo VI, establece las directrices para asegurar la confidencialidad, integridad y disponibilidad del activo de información de los organismos gubernamentales. Además, se abordan las directrices para mantener la continuidad de los servicios y la gestión de riesgos[12] para las operaciones apoyándose en los recursos de TIC.

Para el capítulo final, se indican las directrices y recomendaciones sobre los aspectos que permiten la automatización de los servicios y una administración eficiente de los recursos, como los temas de digitalización de documentos, reducción de papel, canales de acceso, Intranet[13] y un Sistema de Respuesta de Voz Interactiva[14] (IVR, por sus siglas en inglés). Además, en este capítulo se trata el tema de tecnología verde, el cual procura llevar a los organismos a un nivel de optimización de sus recursos tecnológicos, permitiéndole minimizar el impacto ambiental y aumentar el ahorro energético.

[9] Para fines de esta norma, hace referencia al conjunto de equipos y elementos en lo que se sustenta un sistema de información.

[10] Para fines de esta norma, son todas las herramientas aplicaciones y software desarrollados a la medida o para soluciones específicas, utilizadas por el estado.

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

[12] Es la posibilidad de que se produzca una amenaza por decisión previa.

[13] Es una red interna para compartir de forma segura cualquier información o aplicación y evitar que cualquier usuario de Internet pueda ingresar a la red.

[14] Es un sistema telefónico capaz de recibir una llamada e interactuar con el humano, a través de grabaciones de voz y el reconocimiento de respuestas simples, mediante las teclas del teléfono o el móvil.

CAPÍTULO I

NORMA GENERAL SOBRE EL USO E IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Esta norma indica las directrices y recomendaciones que debe seguir cada organismo del Gobierno Dominicano sobre el uso e implementación de TIC, con el objetivo de estandarizar los procesos y plataformas utilizados en la administración pública, de modo que se pueda lograr una gestión más efectiva de los recursos tecnológicos en cada organismo, así como mejorar la calidad en los servicios prestados a los ciudadanos. Esto permitirá establecer la base para la implantación de normas y estándares posteriores que contribuirán al logro del gobierno electrónico en el 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 las instituciones financieras

y las no financieras, organismos reguladores, instituciones de la 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 elaboración de esta norma se tomó como base las normativas elaboradas por la OPTIC en el año 2007, sobre conectividad y el manejo del Protocolo de Internet[1] (IP, por sus siglas en inglés), digitalización de documentos y seguridad informática. La estructura de la NORTIC A1:2014 engloba en sus capítulos estas normativas, respondiendo a los nuevos requerimientos técnicos de estos tiempos, por lo que las normas anteriormente citadas serán derogadas por esta actual normativa.

La NORTIC A1 hace referencia a las normas sobre la creación y administración de portales web del Gobierno Dominicano (NORTIC A2), publicada en junio de 2013, para el tema sobre medios web y a la norma sobre publicación de datos abiertos[2] del Gobierno Dominicano (NORTIC A3), publicada en febrero de 2014, para el tema de la información reutilizable[3] que debe publicar todo organismo gubernamental.

Además, se tomó como referencia el marco de trabajo de buenas prácticas ITIL v3 sobre la gestión y disponibilidad de los servicios de TIC, debido a que este marco busca desarrollar procedimientos de gestión de servicios más eficientes.

Para el tema sobre desarrollo de software a la medida, se utilizó como referencia la norma ISO12207, de la Organización Internacional de Normalización[4] (ISO,

[1] Es un protocolo de comunicación de datos, a través de un medio digital.
[2] Son datos que están disponibles para cualquier persona sin restricciones, los cuales pueden ser utilizados, reutilizados y redistribuidos libremente.
[3] Hace referencia a datos o informaciones del sector público que puedan ser consumidas y/o transformadas por personas físicas o jurídicas, ya sea para fines comerciales o no.
[4] Es una organización encargada de la creación de normas y estándares internacionales en diferentes áreas como tecnologías, seguridad, servicios, entre otros.

por sus siglas en inglés), sobre los procesos del ciclo de vida del software y el marco de desarrollo de la metodología Scrum, el cual es un marco para la gestión y desarrollo de software, permitiendo realizar un desarrollo ágil.

Se utilizó el estándar ANSI/TIA 942 del Instituto Nacional Estadounidense de Estándares y la Asociación de Industria de Telecomunicaciones[5] (ANSI/TIA, por sus siglas en inglés), sobre infraestructura y telecomunicaciones para el centro de datos[6], en conjunto con los estándares IEEE 802 e IEEE 803 del Instituto de Ingenieros Eléctricos y Electrónicos[7] (IEEE, por sus siglas en inglés), en la elaboración del tema sobre los centro de datos y su estructuración, siguiendo el sistema de certificación TIER, creado por el Up Time Institute.

En las definiciones de características físicas con las que deben cumplir los cables de transmisión de datos se tomó el estándar elaborado por la ANSI, la TIA y la Alianza de Industrias Electrónicas[8] (EIA, por sus siglas en inglés), denominado ANSI/TIA/EIA-568B.

Para el tema sobre computación en la nube[9] se utilizó la guía para la seguridad en áreas críticas de atención sobre la nube de la Alianza de Seguridad en la Nube (CSA, por sus siglas en inglés), la cual tiene como objetivo promover las mejores prácticas para proporcionar garantías de gestión efectiva en dicho tema.

La norma ISO 27001:2005 sobre seguridad de la información y COBIT 5 fue utilizada como marco de referencia en el desarrollo del tema sobre la implementación de seguridad de la información.

Sobre la gestión de riesgo, la continuidad de la prestación de los servicios y las operaciones de TIC, se utilizó la norma ISO 31001:2009, la cual provee principios y guías genéricas para la gestión de riesgos, y la ISO 22301:2012 que proporciona un marco de referencia para la gestión de la continuidad del negocio.

También se utilizó como referencia para el tema sobre digitalización de

[5] Promueve el uso de las normas estadounidenses internacionalmente. Además, defiende las posiciones en la política, en cuanto a normas de Estados Unidos y las posiciones técnicas en organizaciones dedicadas a las normas internacionales.

[6] Es un área donde se concentran y operan los equipos que conforman la infraestructura TIC que utilizan los organismos para administrar sus actividades y servicios.

[7] Es una organización profesional dedica al avance de la innovación tecnológica y a la creación de estándares tecnológicos.

[8] EIA, actualmente manejada por la Asociación de Industrias de Componentes Eléctricos (ECIA, por sus siglas en inglés), es una alianza de compañías eléctricas de Estados Unidos; la cual tiene como misión promover el mercado y competitividad de la industria de la alta tecnología.

[9] También llamada nube computacional, es una tecnología que permite la utilización de servicios de cómputos por medio de Internet.

documentos la norma técnica de digitalización de documentos del Gobierno del Principado de Asturias, la cual constituye una guía general para la obtención, control, conservación, y puesta a disposición de imágenes digitales obtenidas a partir de documentos originales. Además para los casos de entidades de intermediación financiera se referenció el instructivo sobre digitalización, truncamiento y compensación de cheques, elaborado por el Banco Central de la República Dominicana en abril de 2013.

En cuanto a la adquisición de los equipos electrónicos en los organismos gubernamentales, se tomó como referencia el programa "*Energy Star*[10]", el cual certifica que estos equipos cumplen con estrictas normas de energía limpia.

SECCIÓN 1.03.

Términos y definiciones

Para fines de esta norma el término "Organismos gubernamentales" será utilizado en ciertos casos como "Organismos".

Cuando aparezca el término "medios web", este se refiere a la agrupación del portal web y la versión móvil del mismo, el sub-portal[11] de transparencia y todos aquellos sitios web desarrollados por los organismos.

Los términos "Portal web" y "Sub-portal web" serán sustituidos solo por las palabras "Portal" u "Sub-portal" respectivamente. Además, en ciertos casos puede aparecer el término "Portal" indistintamente de que el medio web al que se hace referencia sea un sub-portal.

Cuando en la normativa aparezca el término "Activos", este se refiere tanto a los activos físicos como los activos de información.

Cuando se haga mención del "Sistema para la Administración de la Seguridad de la Información", este será sustituido por sus siglas "SASI". De igual manera cuando se haga referencia al "Comité de Continuidad", este será sustituido por el acrónimo "CONTI".

[10] Es un programa de la Agencia de Protección Ambiental de los Estados Unidos (EPA, por sus siglas en inglés) creado en 1992 para promover los productos eléctricos con consumo eficiente de electricidad.

[11] Es un portal web que depende de otro portal, es básicamente una extensión del portal madre, específicamente para presentar una información exclusiva que tiene mucha relevancia, pero que sigue estando relacionado con el portal principal.

Los términos "Interfaz de usuario" e "Interfaz de aplicación", para fines de esta norma se utilizarán indistintamente. En cuanto, a los términos "Interfaz de datos" e "Interfaz de sistema" estos hacen referencia a un tipo de interfaz física, por lo que la definición de este último, aplica para las citadas anteriormente.

Para fines de esta norma el término "Informaciones clasificadas" será utilizado para referirse a informaciones sensitivas y/o confidenciales. Y los términos "Software", "Aplicaciones" y "Programas" se utilizarán indistintamente.

SECCIÓN 1.04.

Compromiso de los organismos gubernamentales

Como una de las funciones de la OPTIC es regular el Estado en el ámbito tecnológico, a través de la publicación de normas, estándares y políticas para ser implementadas por el Estado Dominicano, cada uno de los organismos gubernamentales tiene el compromiso de cumplir con las siguientes directrices:

(a) Implementar y obedecer las normas y estándares en materia de TIC publicados por la OPTIC, de acuerdo con el decreto 709-07.

(b) Cumplir con las políticas y lineamientos establecidos por la OPTIC.

(c) Permitir la supervisión del cumplimiento de las NORTIC, por parte de la OPTIC.

(d) La máxima autoridad del departamento de TIC de cada organismo gubernamental o un representante que este designe debe pertenecer al COETIC.

(e) Suministrar los datos o informaciones requeridas por la OPTIC sobre la implementación de TIC o cualquier aspecto de Gobierno Electrónico de los organismos.

(f) Notificar a la OPTIC sobre los proyectos de TIC que se estén planificando dentro del organismo para que estos sean evaluados dentro del marco establecido en la **sección 3.01. Planificación de proyectos**.

SECCIÓN 1.05.

Directrices generales para los organismos gubernamentales

Contiene un conjunto de directrices, recogidas de los 6 capítulos que conforman esta normativa, así como también las directrices para los temas sobre libre acceso a la información pública e inventario, las cuales son de aplicación general para todo organismo gubernamental independientemente de la función que estos realicen.

(a) La alta gerencia de cada organismo debe velar e involucrarse en el cumplimiento de todas las directrices especificadas en esta normativa y en las demás NORTIC.

(b) Todo organismo debe tener conformado el Comité Administrativo de los Medios Web (CAMWEB). Ver **directriz 1.05.1.c**.

(c) Todo organismo debe establecer mecanismos de acceso a los medios electrónicos para las personas que carecen de ellos.

(d) Los organismos gubernamentales no deben exigirles a los ciudadanos la entrega de un documento que obre en poder de la Administración pública.

(e) Los organismos gubernamentales deben establecer cooperación, asistencia e intercambio de información con otros organismos gubernamentales para la obtención y tratamiento de la información.

(f) Todo organismo debe establecer programas de capacitación continua, en conjunto con el departamento de Recursos Humanos, para el personal del departamento de TIC, así como para las demás áreas que hacen uso de las tecnologías en sus labores diarias, a fin de recibir los entrenamientos pertinentes para su actualización frente a los cambios tecnológicos.

(g) Todo organismo debe poseer como mínimo un servidor[12] con las capacidades necesarias para cumplir con los requerimientos especificados en la normativa. Ver **apartado 4.01.3.4. Administración**

[12] Equipo informático que forman parte de una red de datos y que provee servicios a otros equipos en dicha red, llamados clientes.

de servidores del centro de datos.

(h) Todos los organismos deben implementar el SASI. Ver **sub-sección 6.01.1. Sistema para la Administración de la Seguridad de la Información**.

(i) Los organismos gubernamentales deben implementar las políticas definidas para la conservación de documentos o informaciones. Ver **directriz 6.02.2.a**.

(j) Los organismos gubernamentales deben implementar las políticas para la gestión de accesos de los empleados e invitados. Ver **sub-sección 6.03.4. Gestión de acceso de usuario**.

(k) Todo organismo debe disponer de los medios web indicados en la NORTIC A2. Ver **sub-sección 7.04.1. Medios web**.

(l) Todo organismo debe contar con un correo electrónico institucional personalizado con el dominio registrado por el organismo. Ver **sub-sección 7.04.3. Correo institucional**.

(m) Todo organismo que ofrezca servicios de cara al ciudadano debe tener presencia en el Centro de Contacto Gubernamental (*462) y en el portal del Estado (www.gob.do) y demás medios establecidos para estos fines. Ver **sección 7.04. Canales de acceso**.

(n) Los organismos deben disponer de un IVR estandarizado y acorde a los mandatos de esta normativa. Ver **apartado 7.04.5.1. Respuesta de voz interactiva**.

(o) Los organismos deben contar con una Intranet que les permita a los usuarios internos tener a su disposición herramientas útiles para sus labores. Ver **sección 7.02. Intranet**.

Sub-sección 1.05.1. Acceso a la información pública

Para lograr la efectiva publicación de los datos, cada organismo debe cumplir con las directrices establecidas en la NORTIC A3 sobre publicación de datos abiertos, la cual se tomó como referencia para las directrices presentadas más adelante, permitiendo con esto que los datos estén disponibles para ser reutilizados por parte de la sociedad civil, las empresas privadas u otros organismos gubernamentales.

(a) Cumpliendo con la Ley 200-04 sobre Libre Acceso a la Información Pública, cada organismo tiene que regirse bajo los siguientes criterios:

(i) Todo organismo debe tener el sub-portal de transparencia enlazado al portal institucional. Ver **directriz 7.04.1.d**.

(ii) Cada organismo debe instrumentar la publicación de sus respectivas medios web, a los fines de difundir información, funcionar como centro de intercambio y atención al cliente o usuario, en donde el ciudadano pueda realizar consultas, quejas y sugerencias, y para trámites o transacciones bilaterales.

(iii) Las informaciones solicitadas por los ciudadanos deben ser entregadas en forma personal, informándole al momento de requerir la información el medio por el cual se le estará dando respuesta.

(iv) El contenido debe ser publicado utilizando medios tecnológicos que garanticen la autenticidad de la información, tales como certificados digitales.

(b) Para la publicación de sus datos, todo organismo debe seguir la metodología de gestión de datos abiertos implementada en la NORTIC A3, en donde se sigue el modelo de levantamiento, identificación, estructuración y publicación de información reutilizable.

(c) Para el levantamiento de la información reutilizable el CAMWEB, debe ser el responsable del proceso de apertura de los datos de cada organismo y de que estos estén publicados en el portal web www.datos.gob.do con la periodicidad establecida.

(i) Este comité debe estar conformado mínimamente por los responsables las siguientes áreas:

a) Oficina de Acceso a la Información (OAI), la cual sería el área responsable del levantamiento de la información y del análisis de la misma, así como de la priorización de la información reutilizable.

b) Tecnologías de la Información y Comunicación (TIC), para dar asesoría técnica al comité en cuanto a los diferentes

sistemas de información.

c) Legal, para dar asesoría en materia legal al comité sobre las leyes, norma, políticas o reglamentos de cada una de la información a publicar.

d) Comunicaciones, prensa o relaciones públicas, como asesor técnico y para mantener la coherencia entre la información reutilizable publicada por el organismo y el contenido o línea comunicacional de sus distintos medios.

e) Cualquier otra área que la máxima autoridad cada organismo considere.

(d) No debe seleccionarse para la publicación las siguientes informaciones:

(i) Que puedan atentar contra las estrategias de negocio y competitividad de los organismos gubernamentales.

(ii) Que puedan afectar las relaciones con organismos nacionales e internacionales.

(iii) Que pongan en riesgo la seguridad e integridad de personas naturales.

(iv) Que violen los derechos de propiedad industrial ni de propiedad intelectual.

(v) Aquellas sobre investigaciones de delitos en proceso, así como ningún tipo de material considerado como clasificado por cada organismo.

(e) Todo organismo debe publicar y hacer reutilizable toda información referida al funcionamiento de los mismos, así como cualquier acto o actividad que estos ejecuten, para dar cumplimiento a las exigencias de la Ley 200-04 sobre Libre Acceso a la Información Pública y al Decreto No. 130-05 que indica las informaciones que deben hacerse reutilizables.

(f) Para la protección de datos personales debe acatarse las siguientes directrices:

(i) No debe publicarse ningún dato de la vida privada de alguna persona natural en el portal web www.datos.gob.do ni en las

iniciativas de los organismos gubernamentales sobre medios web para la publicación de información reutilizable, salvo que, por previa solicitud, se haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar.

(ii) Los datos a publicar deben revisarse y analizarse lo suficiente para garantizar que no se logre asociarlos a personas y obtener información personal.

(iii) Debe acatarse los aspectos señalados en el artículo 44 de la **Constitución de la República Dominicana**, sobre el derecho a la intimidad y el honor personal.

(g) Para el ordenamiento de la información reutilizable cada dato debe agruparse en un conjunto de datos relacionado al contexto del mismo, el cual debe contener sus metadatos[13] (ver **directriz 1.05.1.k.vi**.) y disponer de un Identificador Uniforme de Recursos[14] (URI, por sus siglas en inglés).

(i) La estructura de las URI debe contener los siguientes elementos:

- El esquema, el cual identifica el protocolo de acceso al recurso.
- La autoridad, el cual sirve como elemento jerárquico para identificar la autoridad de nombres.
- La ruta, en donde se identifique el recurso de forma organizada y jerárquicamente.
- La consulta, la cual debe empezar con el carácter "?". Este también identifica el recurso consultado, pero con una estructura no jerárquica.
- El fragmento, la cual debe empezar con el carácter "#". Este identifica una parte o vista específica del recurso consultado.

(h) Para la identificación de la información reutilizable cada información debe relacionarse a una o varias de las categorías que definan el contexto de la misma, las cuales se indican a continuación:

[13] Son un conjunto de información que describe las características de otra información. Es "datos sobre datos".
[14] Es una dirección exacta y precisa que permite ubicar un recurso en Internet o en una red de cómputos.

- Ciencia y tecnología.
- Economía.
- Educación.
- Electoral.
- Gestión pública.
- Legislación.
- Medio ambiente.
- Política exterior.
- Salud.
- Sociedad y bienestar.
- Urbanismo.

(i) Para la estructuración de la información reutilizable los formatos[15] a utilizarse deben ser de estándares abiertos[16], sin embargo puede complementarse la información con estándares cerrados[17] para reforzar la publicación.

(i) En los casos que existan particularidades en las que sea necesario utilizar estándares cerrados, estos deben ser justificados con una nota explicativa que acompañe la información, además de indicar el software que permita el procesamiento del formato.

(j) Toda información debe estructurarse de acuerdo a los formatos mínimos requeridos presentados en la **tabla No. 1**. **Formatos para estructura de información**.

[15] Hace referencia al tipo de codificación de la información en un archivo.
[16] Hace referencia a formatos que permiten su uso y manipulación libremente.
[17] Hace referencia a formatos que permiten su uso para consulta, pero sin permisos de manipulación.

Tabla No. 1. Formatos para estructura de información

TIPO DE INFORMACIÓN	FORMATOS	
Hojas de Cálculo	CSV	
	ODS	
	XLSX	
Información reutilizable de texto	TXT	
	ODT	
	DOCX	
Imágenes geográficas Procesadas mediante un Sistema de Información Geográfica (SIG)	Formatos Raster	JPG
		PNG
		MrSID
	Formatos Vectoriales	SVG
		KML
		GML
Imágenes	JPG	
	PNG	
	Formato WebP	
Audio	Audio general	Ogg Vorbis
	Audio sin pérdida de calidad	FLAC
	Audio de voz o reproducción en tiempo real	Opus
Video	Video en general	Ogg Theora
	Video de alta calidad en archivos de tamaño reducido	XviD
	Video en HTML5	WebM
Formatos o lenguajes de marcado Para el intercambio de datos	XML	
	JSON	
Acceso a base de datos relacionales	SQL	
	TSV	

Consulta de grafos RDF	SPARQL
Catalogación de los documentos	RDF serializado bajo el formato de notación Turtle.
Formato de fuente web para compartir contenido en Internet	RSS
Almacenamiento de imágenes en discos ópticos	Formato ISO
Compresión sin pérdida	ZIP
	BZIP
	GZIP
Almacenamiento de documentos digitales	PDF
	DjVu
	ePub
Consulta y actualización de información	ODATA

(k) Los catálogos de información reutilizable elaborados como iniciativa particulares de un organismo, deben cumplir con las siguientes especificaciones:

(i) Presentar los metadatos de las informaciones publicadas, un listado de los conjuntos de datos de cada organismo, así como enlaces a otros datos relacionados a cierta información reutilizable[18] siempre que sea posible.

(ii) Alinearse y enlazarse al catálogo central del Gobierno.

(iii) Poseer una herramienta de búsqueda[19].

(iv) Proveer guías y sugerencias para el usuario.

(v) Organizar, clasificar y relacionar la información reutilizable, en función de metadatos. La estructura de estos se definirá mediante el Vocabulario para Catálogo de Datos[20] (DCAT, por sus siglas en

[18] Conjunto de datos bajo los cuales se publica la información en formato abierto.
[19] Es una herramienta de consulta que arroja resultados basados en los criterios de búsqueda del usuario.
[20] 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.

inglés).

(vi) Ofrecer los metadatos siguientes para cada conjunto de datos: Título, descripción, organismo, licencia, categoría, sub-categoría, fecha de publicación, fecha de actualización, palabras claves, cobertura geográfica y recursos. Este último debe ofrecer los metadatos siguientes: Título, descripción, enlace, formato, fecha de publicación.

(vii) Indicar como metadato el tipo de licenciamiento para cada conjunto de datos que se desee publicar, y presentarse, en la parte anterior al pie de página de las iniciativas de los organismos sobre medios web para la publicación de información reutilizable, todas las insignias de licencias que rigen el uso y permiso de la información publicada. Los tipos de licencias a utilizar serán los siguientes:

- La Licencia Pública General de GNU[21] (GNU/GPL, por sus siglas en inglés).
- La Licencia de Bienes de Creación Común de Atribución-CompartirIgual[22] (CC BY-SA, por sus siglas en inglés).
- La Licencia de Base de Datos Abierta[23] (ODBL, por sus siglas en inglés).

(l) Para la información reutilizable los organismos deben disponer de un correo electrónico personalizado con su nombre de dominio y con un usuario denominado "datosabiertos", el cual debe estar bajo la responsabilidad del CAMWEB o las personas quienes los miembros de este comité designen. El uso de este correo será únicamente para los fines siguientes:

- Registro en el portal web www.datos.gob.do.
- Como medio de comunicación entre los organismos y la DIGEIG, en los casos de que esta última remita información relacionada al

[21] Es una licencia que permite al usuario, compañía u organismo, dar uso público a un contenido o código fuente de manera libre y sin restricción.
[22] Es una licencia de derecho de autor que permite al beneficiario manipular en todos los sentidos el contenido o producto, manteniendo los principios de esta licencia.
[23] Es un contrato de licencia en donde se permite la libre manipulación de una base de datos.

tema de Gobierno Abierto o alguna comunicación importante para la apertura de los datos de los organismos.

(m) Cada organismo tiene la responsabilidad de cargar en el portal de datos abiertos su conjunto de datos.

(n) Todo software desarrollado para o por los organismos del Estado Dominicano debe ser colocado en el repositorio de software gubernamental ubicado en el portal web www.datos.gob.do.

(o) La fecha de actualización es variable para cada conjunto de datos, debido a la naturaleza de la información reutilizable que contiene dicho conjunto, por lo tanto cada uno debe tener una fecha de actualización determinada por los mismos organismos. Una vez la frecuencia de publicación esté definida, se utilizará el periodo indicado para el monitoreo del cumplimiento de los tiempos propuestos.

(p) Para los conjuntos de datos que su frecuencia de actualización es igual o superior a los doce meses, debe indicarse un metadato que indique la última revisión realizada al mismo, la cual debe hacerse cada 6 meses mínimo para estos casos.

Sub-sección 1.05.2. Licenciamiento

(a) Todo organismo gubernamental debe aplicar las directrices establecidas a continuación, permitiendo así el cumplimiento de la ley 65-00 sobre derecho de autor.

(b) Cada software utilizado por los organismos debe incluirse en el inventario general de TIC, siguiendo la periodicidad y las directrices especificadas en la **sección 2.04. Inventario general de TIC**.

(c) Cada software propietario utilizado en los organismos debe contar con la licencia respectiva.

(d) Debe eliminarse aquel software propietario que, requiriendo licencia para su uso, no cuente con la misma, o debe regularizarse la situación con el titular del mismo.

(e) Solo debe instalarse la cantidad de copias del software propietario permitidas por las licencias que poseen los organismos para este fin.

(f) No debe reproducirse ni distribuirse copias no autorizadas de software propietario por Internet u otros medios electrónicos.

(g) Ningún personal de los organismos debe descargar, cargar o transmitir copias no autorizadas de software propietario por Internet u otros medios electrónicos.

CAPÍTULO II

GESTIÓN DEL DEPARTAMENTO DE TIC

En este capítulo se establecen las directrices para la gestión del departamento de TIC, especificando cómo este debe estar estructurado organizacionalmente, las políticas departamentales para una gestión efectiva, cómo deben gestionar los servicios de TIC y cómo llevar el control de los activos que están bajo la responsabilidad del departamento.

SECCIÓN 2.01.

Estructura del departamento de TIC

Se ha dispuesto una estructura organizacional que consta de 5 áreas básicas, las cuales deben cumplir con los roles establecidos para cada una de estas áreas, así como 3 modelos de estructura organizacional y dos formas para la selección de uno de estos modelos basado en una serie de criterios y tablas de ponderaciones.

Sub-sección 2.01.1. Estructura organizacional

(a) Todo organismo gubernamental debe organizar la estructura departamental de TIC, de acuerdo con todas las directrices especificadas en la resolución 51-2013 elaborada entre la OPTIC y el MAP.

(b) La gestión del departamento de TIC debe agruparse en 6 grandes áreas básicas y cumplir con los roles asignados a cada una:

(i) **Unidad TIC**: Tiene bajo su cargo las responsabilidades indicadas en la **sección 2.02. Políticas generales del departamento TIC**.

a) **Administración de los procesos de TIC**: Responsable de

planificar y coordinar todas las actividades de evaluación de procesos. Brinda apoyo a las partes involucradas en la gestión y mejoramiento de los procesos, especialmente a los propietarios del mismo. Este rol también coordina los cambios a procesos, y por tanto, se asegura de que estos interactúen perfectamente entre sí. También es responsable de determinar y velar por el cumplimiento de las estrategias de tecnología verde en el organismo.

b) **Administración del portafolio de servicios**: Determina la estrategia del servicio al cliente y desarrolla las ofertas y capacidades del proveedor de servicios.

c) **Administración del perfeccionamiento continúo del servicio**: A cargo de gestionar mejoras a los procesos de administración sobre servicios de TIC. Tomará medidas continuamente del rendimiento del proveedor de servicios y diseñará mejoras a los procesos, servicios e infraestructura, de manera que se aumente la efectividad y la rentabilidad.

d) **Administración del cumplimiento y calidad de TIC**: A cargo de gestionar todas las actividades relacionadas con el aseguramiento de la calidad de los servicios de TIC para que estos cumplan con los niveles de satisfacción acordados con las áreas que requieran servicios del departamento de TIC.

(ii) **Desarrollo e implementación de sistemas**: Debe responsabilizarse de todas las actividades relacionadas con el diseño, desarrollo, implementación y soporte de los programas y sistemas que apoyan los procesos esenciales de los organismos.

a) **Análisis de sistemas**: Responsable de la administración de todo el ciclo de vida del desarrollo de sistemas para las aplicaciones que den soporte a los procesos del organismo gubernamental. Se encarga de recibir e interpretar las necesidades de los usuarios en torno a la funcionalidad requerida de los sistemas. Es responsable del diseño de las aplicaciones necesarias para la prestación de un servicio y sirve de enlace entre las áreas que requieran servicios y el área de desarrollo de sistemas. Se asegura de que las versiones implementadas y los servicios

resultantes cumplan las expectativas del cliente, y verifica que las operaciones de TIC puedan brindar apoyo a los servicios nuevos.

b) **Programación**: Se ocupa de que las aplicaciones y los sistemas provean la funcionalidad necesaria para que los servicios de TIC estén disponibles. Esto incluye el desarrollo y el mantenimiento de aplicaciones internas. Es responsable de planificar, programar y controlar el movimiento de ediciones en ambientes reales y de prueba. Su objetivo principal es salvaguardar la integridad en el ambiente real y que se utilicen los componentes correctos.

(iii) **Operaciones de TIC**: Debe responsabilizarse de todas las actividades relacionadas con la operación y administración de la infraestructura tecnológica (servidores, bases de datos[1], redes, entre otros), así como el aseguramiento de la continuidad de las operaciones.

a) **Administración de servidores**: Responsable de mantener la integridad y seguridad de los servidores y sistemas que soportan las operaciones del organismo gubernamental.

b) **Administración de bases de datos**: Responsable de la administración de las bases de datos, así como la programación, resolución de problemas y otros servicios técnicos relacionados con las mismas.

c) **Administración de la configuración**: Responsable de dar mantenimiento a la información requerida sobre elementos de configuración de la infraestructura de TIC y gestionar dicha información a través de la Base de Datos de la Gestión de Configuración[2] (CMDB, por sus siglas en inglés). Debe monitorear periódicamente la configuración de los sistemas en el ambiente de producción[3] y compararla con la

[1] Son un conjunto de datos almacenados de manera ordenada y que guardan relación entre ellos para su uso posterior.
[2] Es una base de datos central de todos los elementos de configuración de un sistema de información, ya sea hardware, software, documentación o cualquier otro elemento.
[3] Es el ambiente real en donde los usuarios finales utilizan los sistemas de información y manejan datos concretos. Además, en este entorno las fallas ocurridas pueden afectar al usuario u organismo.

información almacenada en la CMDB para subsanar posibles discrepancias. Además, es responsable del levantamiento, actualización y control del inventario de los bienes bajo responsabilidad del departamento de TIC.

d) **Administración de redes y comunicaciones**: Responsable de mantener en funcionamiento, así como dar mantenimiento a los elementos de red y comunicación que soportan las operaciones del organismo gubernamental. También es responsable de la generación de reportes y mantenimiento al sistema de IVR.

e) **Administración de la continuidad de TIC**: Responsable de gestionar aquellos riesgos que podrían afectar severamente la prestación de los servicios de TIC. Se asegura de que el desempeño del proveedor de servicios de TIC cumpla los requisitos mínimos del nivel de servicio, en caso de desastres, mediante reducción del riesgo a un nivel aceptable y la planificación de la restauración de los servicios de TIC.

(iv) **Administración del servicio de TIC**: Debe responsabilizarse de todas las actividades de soporte técnico a la infraestructura tecnológica, incluyendo el soporte funcional y mesa de ayuda a los usuarios de los servicios de TIC.

a) **Mesa de ayuda**: Responsable de registrar y clasificar los incidentes[4] reportados y llevar a cabo esfuerzos inmediatos para restaurar lo antes posible un servicio de TIC que ha fallado. Cuando no se encuentre una solución adecuada a estos fines, la mesa de ayuda refiere el incidente a los grupos de apoyo técnico especializados (soporte técnico).

La mesa de ayuda también mantiene informados a los usuarios acerca del estatus de los incidentes cada cierto tiempo.

b) **Soporte técnico**: A cargo de los incidentes que no pueden ser resueltos con los recursos de la mesa de ayuda. De ser necesario, requerirá apoyo externo de proveedores de programas y de hardware[5], así como de otras unidades del

[4] Es cualquier funcionamiento incorrecto de cualquiera de los servicios tecnológicos.
[5] Se refiere a todas las partes físicas o tangibles de un sistema de información.

departamento de TIC.

La meta del soporte técnico es restaurar un servicio de TIC fallido en el menor tiempo posible, de modo que si esta unidad no encuentra la solución, el incidente debe ser referido a administración de incidentes y problemas.

El soporte técnico es el responsable de realizar todas las instalaciones, reinstalaciones y desinstalaciones de software en los equipos de los usuarios.

c) **Administración de incidentes y problemas**: Responsable de la implementación efectiva del proceso de administración de incidentes y problemas, y preparar los informes correspondientes. Ofrece representación durante la primera fase de escalado de incidentes, cuando no se pueden solucionar en el marco de los niveles de servicio acordados.

Es responsable de gestionar el ciclo de vida de todos los problemas. Su objetivo principal es la prevención de incidentes y la minimización del impacto de aquellos que no se pueden evitar.

(v) **Seguridad y monitoreo**: Debe responsabilizarse de todas las actividades relacionadas con la definición e implementación de políticas de seguridad de la información, control y monitoreo de los accesos a los sistemas de información.

a) **Administración y monitoreo de la seguridad de TIC**: A cargo de salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TIC del organismo gubernamental, así como de la recuperación de estos en caso de pérdida. También se ocupa de llevar a cabo el borrado seguro de la información.

Se encarga de definir e implementar los sistemas de detección y respuesta a incidentes relacionados con la seguridad de TIC.

b) **Administración de accesos**: Concede el derecho a usar un servicio a usuarios autorizados, mientras previene el acceso de usuarios no autorizados. Ejecuta políticas definidas por el

personal de administración y monitoreo de la Seguridad de TIC.

(vi) **Administración de proyectos de TIC**: Debe responsabilizarse de todas las actividades relacionadas con la administración y coordinación de la implementación de proyectos de TIC.

a) **Oficina de administración de proyectos de TIC**: Responsable de la planificación, coordinación, administración y seguimiento de los proyectos de TIC, asimismo, debe identificar posibles riesgos que puedan afectar los proyectos e identificar acciones de mitigación de los riesgos.

Sub-sección 2.01.2. Modelos de la estructura de TIC

Cada organismo debe adoptar uno de los tres modelos establecidos para la organización de las unidades institucionales de TIC, de acuerdo a los siete criterios especificados en la **tabla No. 2. Modelos de estructuras de TIC**.

Tabla No. 2. Modelos de estructuras de TIC

CRITERIO	DEFINICIÓN	CATEGORÍA		
		A	B	C
Número de empleados	Cantidad de empleados en la nómina del organismo.	Más de 2,000	De 501 a 2,000	De 1 a 500
Localidades	Cantidad de edificaciones que sirven de lugar de trabajo para el personal del organismo.	Más de 14	De 6 a 14	De 1 a 5

Complejidad de aplicaciones desarrollo interno	Nivel de complejidad de las aplicaciones que brindan soporte de desarrollo en el organismo.	**Alta** Más de 50 usuarios, frecuencia de cambios al menos bimensual, arquitectura de desarrollo multi-capa.	**Media** Hasta 50 usuarios, frecuencia de cambios al menos semestral, arquitectura de desarrollo de dos capas.	**Baja** Hasta 10 usuarios, frecuencia de cambios anual, arquitectura de una capa.
Estaciones de trabajo	Cantidad de estaciones de trabajo (computadoras de escritorio o portátiles) en el organismo.	Más de 750	De 201 a 750	De 1 a 200
Número de Servidores	Cantidad de equipos de computación que fungen como servidores en el organismo.	Más de 40	De 9 a 40	De 1 a 8
Centro de datos de contingencia	Este se refiere a aquellos organismos que cuentan con un centro de procesamiento de datos alterno.	Sí	No	No

Administra sistemas de impacto externo	Los sistemas de impacto externo son aquellos utilizados de forma transversal para más de un organismo.	Sí	No	No

Sub-sección 2.01.3. Selección del modelo de estructura de TIC

(a) Cada organismo debe seleccionar el modelo de estructura de TIC correspondiente, mediante uno de los dos métodos de asignaciones establecidos para este fin:

(i) **Asignación simple**: Debe tomarse directamente un modelo de las tres categorías definidas, en base a una asignación de categoría, según una serie de criterios seleccionados.

a) En la asignación simple, debe determinarse la categoría que más se ajusta a cada organismo, ubicando el organismo en la categoría que corresponda, (“A”, “B” o “C”), según los criterios definidos en la **tabla No. 2. Modelos de estructuras de TIC**.

b) La categoría final que corresponde asignar al organismo, para definir su estructura, es aquella en la cual más criterios le coinciden.

(ii) **Asignación compuesta**: Debe tomarse como base la categoría asignada por el modelo de asignación simple y se modifican las áreas básicas específicas utilizando las ponderaciones que se detallan en el **anexo A. Tabla de ponderación para selección compuesta de la estructura del departamento de TIC**.

SECCIÓN 2.02.

Políticas generales del departamento de TIC

Una buena gestión del departamento de TIC incrementa la efectividad y productividad del departamento, y permite lograr los objetivos establecidos previamente, haciendo un mejor uso de la tecnología y la estructura organizacional. Para lograrlo, todo organismo gubernamental debe cumplir con las siguientes directrices:

(a) La máxima autoridad del departamento de TIC debe cumplir con las siguientes responsabilidades, apoyándose en todos los miembros pertenecientes al departamento:

(i) Evaluar y monitorear el cumplimiento de normas, políticas y leyes por parte de todos los miembros del departamento.

(ii) Dirigir la preparación y la implementación de planes y políticas.

(iii) Gestionar y administrar eficientemente las fuentes y activos de información del organismo, disponiendo de controles la calidad y seguridad de los sistemas.

(iv) Gestionar y administrar las licencias de software y realizar su distribución entre las unidades administrativas que las requieran.

(v) Administrar y coordinar todas las actividades relacionadas con la implementación de proyectos de TIC de impacto interno o externo del organismo.

(vi) Administrar y gestionar los servicios del centro de datos, garantizando la tecnología que soporte las actividades de TIC del organismo, así como el aseguramiento de la redundancia y balanceo de los servicios, monitorear el óptimo estado de los sistemas y plataformas alojadas.

(vii) Desarrollar y administrar aplicaciones de TIC que contribuyan al logro de las metas del organismo, asegurando la calidad de la plataforma y el cumplimiento de los estándares especificados en las NORTIC.

(viii) Disponer de los servicios informáticos y de telecomunicaciones que soliciten las diferentes unidades administrativas del organismo.

(ix) Fomentar la integración a diferentes redes de informaciones nacionales e internacionales mediante Internet, para permitir el acceso a distintas bases de datos en línea.

(x) Implantar y mantener actualizado un sistema de información integral que automatice las operaciones y procesos del organismo fomentando la comunicación interna, mediante el uso intensivo de las TIC.

(xi) Implementar y mantener la infraestructura de TIC que permita al organismo alcanzar sus metas estratégicas y promover el Gobierno Electrónico, mediante el intercambio, acceso y uso de la información por los usuarios internos y externos.

(xii) Participar en la elaboración, ejecución y seguimiento, de acuerdos y protocolos de intercambios de información por medios electrónicos que realice el organismo con otras instituciones públicas y privadas.

(xiii) Proveer soporte técnico a los usuarios de las aplicaciones, así como a la información y la infraestructura del organismo.

(xiv) Realizar la planificación estratégica y presupuestaria de las soluciones de TIC del organismo.

(xv) Revisar periódicamente el funcionamiento de la red, el desempeño de los sistemas en operación y el de las bases de datos del organismo para identificar desviaciones respecto a los objetivos y formular recomendaciones que optimicen los recursos y procesos operativos, propiciando el incremento de la productividad y la eficiencia.

(b) De acuerdo con la naturaleza de cada organismo gubernamental, debe crearse políticas de documentación para cada procedimiento, resolución de incidentes, software desarrollado internamente, y cualquier otra información relevante que manipule el departamento.

(i) La documentación debe realizarse de manera minuciosa, explicando todos los detalles de la información a documentar.

(ii) En caso de prescindir de un recurso, debe utilizarse la documentación realizada previamente, de manera que se pueda continuar brindando los servicios que se ofrecen.

SECCIÓN 2.03.

Servicios de TIC

En esta sección se establece el procedimiento a seguir en la prestación de servicios y la gestión de incidentes. Así como las especificaciones para la estructuración del catálogo de servicio y la elaboración de los Acuerdos de Nivel de Servicio[6] (SLA, por sus siglas en inglés).

(a) La disponibilidad de los servicios debe contemplarse en el plan de disponibilidad y continuidad de cada organismo. Ver **sección 6.05. Plan de disponibilidad y continuidad**.

(b) Cualquier tarea que implique una degradación o interrupción del servicio debe realizarse en las horas de inactividad o de menor demanda de este, siempre que sea posible.

(c) Si el servicio debe estar disponible las 24 horas del día y la interrupción es necesaria:

(i) Debe consultarse con el cliente acerca de las horas en la que la interrupción del servicio afectará menos a sus actividades.

(ii) Debe informarse con antelación suficiente a todos los involucrados.

(iii) Debe incorporarse dicha información a los SLA.

(iv) Debe monitorizarse la disponibilidad del servicio y elaborarse informes con los resultados.

(v) Debe especificarse el tiempo de detección.

(vi) Debe especificarse el tiempo de respuesta.

(vii) Debe especificarse el tiempo de reparación/recuperación.

[6] Es un documento que plasma los acuerdos entre un proveedor de servicio y el cliente, en donde se estipulan los requisitos y parámetros que el proveedor se compromete a cumplir para mantener unos niveles de calidad de servicio.

Sub-sección 2.03.1. Catálogo de servicios

(a) Todo organismo debe elaborar un catálogo de servicios[7] cumpliendo las siguientes directrices:

(i) Los servicios deben agruparse en líneas, categorías o familias principales de servicio.

(ii) El catálogo de servicio debe estar escrito en un lenguaje simple, evitando los tecnicismos siempre que sea posible.

(iii) Debe contener solo los servicios que estén activos e interesen al cliente, evitando incluir en el catálogo de servicios aquellos que no se ofrezcan o que se ofrecerán en un futuro.

(iv) Cada servicio incluido debe contener los siguientes datos:

- Nombre y descripción del servicio.
- Propietario del servicio.
- Cliente.
- Otras partes implicadas (proveedores, organismos, entre otros), cuando aplique.
- Fechas de versión y revisión.
- Niveles de servicios acordados en los SLA.
- Condiciones de prestación del servicio: Requisitos para que se pueda brindar el servicio.
- Precio (en caso que aplique).
- Cambios y excepciones. Exclusiones para la prestación del servicio.

(v) El catálogo de servicio debe estar disponible para todos los miembros de la mesa de servicio y a quienes el organismo considere necesario.

[7] Es un listado de todos los servicios activos de un organismo. Este catálogo contiene todas las informaciones necesarias para el cliente sobre dichos servicios.

(vi) Debe elaborarse un plan para el mantenimiento y actualización del catálogo de servicio. Este programa debe incluir:

a) **Las planificaciones de actualizaciones para el catálogo**: Preparar un plan que contenga el cómo, y cuándo se realizarán las actualizaciones.

b) **Planificación de revisiones periódicas**: Cada qué tiempo se realizarán las revisiones al catálogo de servicios.

c) **Protocolos para aprobación de cambios**: Quién y cómo se aprobarán los cambios realizados al catálogo.

d) **Políticas para la medición y monitoreo del catálogo de servicio**: Con el objetivo de medir el rendimiento de este, la calidad en los servicios ofertados y la eficiencia de los procesos establecidos.

i) La unidad de administración del servicio de TIC debe tener un personal que asuma la función de ejecución del plan para el mantenimiento y actualización del catálogo de servicio.

Sub-sección 2.03.2. Niveles de servicio

(a) Cada organismo gubernamental debe establecer los SLA necesarios con los clientes y proveedores para ofrecer los servicios requeridos.

(i) Los niveles de servicios deben contener las siguientes informaciones mínimas:

a) **Descripción del servicio**: Donde se especifique de manera detallada todo los aspectos del servicio brindado.

b) **Revisión y vigencia**: Donde se estable el tiempo durante el cual es válido el SLA y el procedimiento de revisión establecido.

c) **Objetivo del servicio**: Finalidad que se desea alcanzar con el servicio brindado.

d) **Políticas**: Especificación de las políticas que regulan el servicio brindado.

e) **Monitoreo del SLA**: Especificación de cada qué tiempo se estará monitoreando el servicio.

f) **Contactos**: Informaciones de contactos del cliente y del representante del departamento de TIC.

g) **Quejas y reclamaciones**: Informaciones de contactos en donde el cliente pueda comunicarse en caso de incumplimiento del SLA.

h) **Reporte de incidentes**: Informaciones de contactos en donde el usuario se comunique en caso de averías en el servicio.

i) **Tiempo de respuesta**: Especificación del tiempo de respuesta según la prioridad del incidente.

Para más información sobre el establecimiento de prioridades en la gestión de incidentes, ver anexo B. Diagrama de prioridades, según el impacto y la urgencia del incidente.

(ii) Debe enviarse al cliente un informe del monitoreo del servicio con la periodicidad establecida en el SLA.

Sub-sección 2.03.3. Gestión de incidentes

(a) Toda incidencia debe registrarse inmediatamente sea recibida en la mesa de servicio o por cualquier otro medio establecido por el organismo para la recepción de estas.

(b) Para el registro de incidencias debe realizarse lo siguiente:

(i) Verificar si el servicio solicitado se incluye en el SLA del cliente.

(ii) Registrar en la plataforma utilizada para estos fines. Como mínimo debe cumplir con los siguientes requisitos para cada registro de incidencia:

a) Asignar una categoría dependiendo el tipo del incidente o del grupo de trabajo involucrado.

b) Establecer la prioridad, la cual puede ser:

- Crítica.
- Alta.

- Media.
- Baja.

c) Asignar el personal que trabajará en la resolución del incidente.

d) Asociar un estado al incidente, el cual puede ser:

- **Registrado**: Cuando el incidente se registra, sin embargo por razones propias del organismo no se inicia su resolución hasta que el área o unidad responsable lo determine.
- **Activo**: Cuando la resolución del incidente se inicia inmediatamente se registra el mismo.
- **Suspendido**: Cuando el estado del incidente estuvo activo y por razones propias del organismo, o el área responsable, la resolución se detuvo.
- **Resuelto**: Cuando el incidente se ha solucionado y especificado el procedimiento llevado a cabo para su resolución, pero no se ha confirmado con el cliente.
- **Cerrado**: Cuando se haya completado el proceso de resolución, incluyendo la confirmación con el cliente de la correcta resolución.

e) Establecer un tiempo de respuesta de acuerdo a lo acordado en el SLA.

(iii) Luego del registro debe informarse al cliente como mínimo el número de caso, el tiempo de respuesta para que sea resuelto su caso, así como el soporte técnico asignado para dar resolución al incidente.

(iv) Debe existir un proceso de escalamiento para los incidentes que no puedan ser resueltos por el técnico asignado. En estos casos deberá seguirse el protocolo establecido por el organismo. Ver **anexo C. Matriz de escalamiento para la gestión de incidentes**.

(v) Cuando se haya resuelto el incidente debe:

a) Confirmar y notificar con el cliente la correcta resolución del incidente.

b) Registrar el procedimiento que se llevó a cabo para la resolución del incidente.

c) Cerrar la solicitud.

SECCIÓN 2.04.

Inventario general de TIC

Se establece el procedimiento para el levantamiento, actualización y control de inventario que todos los organismos deben seguir para la gestión de los activos físicos y de información que se encuentren bajo la responsabilidad del departamento de TIC.

(a) Todo organismo debe realizar un inventario ordenado, completo y actualizado de todos los activos que estén bajo la responsabilidad del departamento de TIC.

(i) El inventario general de TIC debe estar organizado en dos secciones principales:

- **Activos físicos**: Donde se registrarán todos los equipos de la infraestructura TI, estaciones de trabajo, portátiles y demás.
- **Activos de información**: Donde se registrará todo el software utilizado, sistemas operativos y demás.

(ii) La unidad de operaciones de TIC debe tener un personal que asuma la función de llevar a cabo todo el proceso de inventario. Este tendrá a la responsabilidad de coordinar las tareas que deben desarrollarse:

a) **Levantamiento de inventario**: Registrar todos los bienes que forman el equipamiento tecnológico bajo el control del departamento de TIC. Esta fase se realizará en caso de que el organismo no haya realizado un inventario anteriormente.

b) **Actualizaciones de inventario**: Agregar al inventario nuevos bienes adquiridos por el departamento de TIC, igualmente eliminar los bienes que han salido de la responsabilidad del organismo.

c) **Control de inventario**: Revisar físicamente los bienes que se encuentran en el inventario.

Sub-sección 2.04.1. Levantamiento de inventario

(a) Para el levantamiento de inventario debe seguirse los siguientes pasos:

(i) Definir los tipos de activos a ser considerados para el registro en el inventario.

(ii) Identificar todas las dependencias del organismo con equipamiento tecnológico y demás activos considerados.

(iii) Planificar el horario, que no interfiera con la prestación de los servicios brindados, en caso contrario, elegir el horario que menos impacto cause.

(iv) Para los activos físicos debe registrarse los siguientes datos:

- **Código**: Código generado para individualizar cada bien inventariado.
- **Artículo**: Tipo de artículo a inventariar.
- **Marca/modelo**: Marca y modelo del artículo.
- **Número de serie**: Número de serie del activo a inventariar.
- **Estado**: El bien a inventariar puede estar en uno de estos tres estados:
  - **Operativo**: Funciona correctamente y está siendo utilizado o puede utilizarse.
  - **No operativo**: Requiere alguna reparación.
  - **De baja**: Bien que no puede ser utilizado.
- **Responsable**: Nombre o cargo del encargado del bien.

- **Ubicación**: Lugar en donde se encuentra ubicado el bien.
- **Fecha de baja**: Fecha en que es dado de baja el bien (en caso de que aplique).
- **Observaciones**: Comentarios relacionados con el estado del bien.
- Cualquier otro dato que sea de relevancia para el organismo.

(v) En los activos de información debe registrarse los siguientes datos:

- **Código**: Código generado para individualizar cada bien inventariado.
- **Nombre**: Nombre del software a inventariar.
- **Versión**: Versión del software (si aplica).
- **Tipo de software**: Clasifica el software en aquellos que son de desarrollo interno y aquellos que son adquiridos.
- **Proveedor**: Organización distribuidora del software (para software adquirido).
- **Tipo de licencia**: Licencia bajo la cual fue desarrollado el software.
- **Número de licencia:** En caso que el software utilice un número de licencia.
- **Número de instalaciones**: Cantidad de veces que se ha instalado el software en el organismo.
- **Equipo**: Donde se encuentra instalado/ubicado el activo de información.
- **Fecha de adquisición**: Fecha en que se adquirió la licencia.
- **Caducidad de licencia**: Fecha en que vence la licencia (cuando aplique).
- **Observaciones**: Comentarios relacionados con el software.

- Cualquier otro dato que sea de relevancia para el organismo.

(vi) En caso de que la información sea levantada en papel, esta debe digitalizarse[8].

a) Para la digitalización de esta información debe utilizarse uno de los siguientes medios:

- Planilla de cálculo.
- Base de datos.
- Sistema de inventario[9].

b) Debe seguirse las instrucciones de digitalización especificadas en la **sección 7.01. Digitalización de documentos**.

Sub-sección 2.04.2. Actualización de inventario

(a) Debe realizarse una actualización al inventario cada vez que ocurra uno o más de los siguientes eventos a los activos del organismo:

- En caso de adquisición de un nuevo bien que esté bajo la responsabilidad del departamento de TIC.
- Movimiento de ubicación.
- Salida del organismo cuando sea para activos físicos.
- Asignación a otro responsable.
- En los casos de activos físicos, cuando este es dado de baja, mientras que para los casos de activos de información, cuando este se elimina o descontinúa su uso en el equipo.
- Cuando se realice el control de inventario.

Sub-sección 2.04.3. Control de inventario

(a) El control del inventario debe planificarse, dentro de lo posible, en un horario que no interfiera con la prestación de los servicios brindados,

[8] Hace referencia a la transformación de un documento físico a una imagen o medio digital para su visualización y manipulación en un dispositivo electrónico.
[9] Software que permite realizar y controlar todo el proceso de inventario.

en caso contrario, elegir el horario que menos impacto cause.

(b) El control de inventario para los activos de información debe realizarse cada 12 meses.

(c) El control de inventario para los activos físicos debe realizarse cada 6 meses.

(d) El proceso de control debe realizarse a partir de la última versión del inventario.

(e) Debe verificarse la información registrada en el inventario con los bienes existentes.

(f) Al final de la revisión debe actualizarse el inventario con la información que aún no esté registrada obtenida en la verificación.

SECCIÓN 2.05.

Recomendaciones para las políticas del departamento de TIC

- Establecer responsabilidades claramente entendidas y aceptadas por todos los miembros del departamento de TIC.
- Para cumplir con los objetivos departamentales, antes de elaborar las estrategias de trabajo, es necesario tomar en cuenta las capacidades y recursos técnicos que posee el departamento de TIC.
- Que la estructura del departamento de TIC esté distribuida, tanto en recursos tecnológicos como en recursos humanos, de manera que pueda darse soporte al organismo y brindar los servicios con la calidad exigida.

CAPÍTULO III

IMPLEMENTACIÓN DE TIC

En el siguiente capítulo se establecen las directrices y los procesos que deben realizarse para la planificación de un proyecto TIC, así como también las directrices necesarias que un organismo debe cumplir al momento de adquirir bienes o contratar servicios.

SECCIÓN 3.01.

Planificación de proyectos de TIC

Los organismos gubernamentales deben contar con procesos, documentaciones y controles que permitan la correcta ejecución de un proyecto de TIC, de manera que el resultado final cumpla con la expectativa y el objetivo esperado. Por lo que deben seguirse las directrices que se describen a continuación:

(a) Los proyectos TIC en su fase de inicial deben contar con el acta de constitución, donde se demuestre la existencia del proyecto a realizar.

(i) El acta de constitución debe tener como mínimo las siguientes informaciones:

- Nombre del proyecto.
- Código del proyecto.
- Partes involucradas en el proyecto.
- Director del proyecto y su nivel de autoridad dentro del proyecto.

- Descripción del proyecto.
- Requisitos del proyecto.
- Criterios de aceptación del proyecto.
- Riesgos del proyecto.
- Objetivo general y específico del proyecto.
- Resumen de hitos del proyecto.
- Presupuesto estimado para la realización del proyecto.
- Método de escalamiento de comunicación, el cual se define por los siguientes niveles:
    - **Nivel 1**: Persona designada por el director del proyecto.
    - **Nivel 2**: Persona encargada de la dirección del proyecto.
    - **Nivel 3**: Director general del organismo.

(ii) El acta de constitución debe estar aprobada y firmada por la persona encarda de la dirección del proyecto, por las partes interesadas y cualquier otra firma que se considere necesaria.

(b) Durante la planificación de los proyectos de TIC, debe elaborarse el enunciado del alcance del proyecto, donde se describe el trabajo a realizar, así como el producto o resultado final, acompañado la Estructura de Desglose del Trabajo (EDT). Los documentos mencionados anteriormente se detallan a continuación:

(i) El enunciado del alcance del proyecto, debe presentar como mínimo los siguientes elementos:

- Nombre del proyecto.
- Código del proyecto.
- Partes involucradas en el proyecto.
- Director del proyecto y su nivel de autoridad dentro del proyecto.

- Objetivo del entregable.
- Requisitos y características del entregable.
- Criterios de aceptación del entregable.

(ii) El enunciado del alcance del proyecto debe estar aprobado y firmado por la persona encarda de la dirección del proyecto, por las partes interesadas y cualquier otra firma que se considere necesaria.

(iii) El EDT, debe estructurarse como se muestra en el **anexo D. Diagrama de planificación de proyectos de TIC**, y contener los siguientes componentes:

- Una escala inicial, en donde se especifique el nombre del proyecto y el código.
- Una escala intermedia, en la cual se muestren las principales partes o componentes del proyecto.
- Una escala inferior, en donde se establecen los paquetes de trabajo, en los cuales se especifiquen los recursos, el tiempo y las estimaciones de los costos, de cada uno de los componentes o partes del proyecto.
- Estos paquetes de trabajo deben ser asignados a los diferentes miembros del equipo o unidades organizativas para la realización de las actividades.

(c) Todo cambio durante la ejecución del proyecto debe ser solicitado, aprobado y documentado, como se muestra en el **anexo E. Proceso de solicitud de cambio**, cumpliendo con los siguientes criterios:

(i) Elaboración de una solicitud del cambio por parte de la persona que hace el requerimiento, en la cual se especifique como mínimo las siguientes informaciones:

- Los datos del proyecto:
  - Nombre del proyecto.
  - Código del proyecto.

- Número de solicitud del cambio.
- Nombre de la persona encargada de la dirección del proyecto.
- Fecha del cambio, especificada en DD/MM/AA.

- Datos del cambio:
  - Nombre de la persona que solicita el cambio.
  - Lugar, fase o capa en donde se realizará el cambio.
  - Descripción del cambio.
  - Justificación del cambio.
  - Impacto del cambio.
  - Duración aproximada que tomará aplicar el cambio.
  - Nombre y firma de la persona encarga de la aprobación del cambio.
  - Resultado de la solicitud del cambio: aprobada, cancelada o pendiente.
  - Descripción del cambio.
  - Justificación del cambio.

(ii) La documentación de la solicitud debe detallar como mínimo:

- Datos del proyecto:
  - Nombre del proyecto.
  - Código del proyecto.
  - Nombre de la persona encargada de la dirección del proyecto.
  - Fecha de registro de la solicitud del cambio.

- Datos del cambio:
  - Número del cambio.
  - Nombre de la persona que solicitó el cambio.
  - Fecha de la solicitud del cambio.
  - Descripción del cambio.
  - Estado del cambio: aprobado, en proceso, cancelado.
  - Fecha en que se implementará el cambio.
  - Duración de la implementación del cambio.

(d) Debe establecerse procesos que verifiquen que el entregable ha sido completado, cumpliendo con lo requerido en el enunciado del alcance del proyecto.

(e) Una vez finalizado el proyecto debe elaborarse una documentación de cierre del proyecto, la cual muestre que el proyecto se completó satisfactoriamente y cumplió con las expectativas de las partes interesadas.

SECCIÓN 3.02.

Compra y contratación de TIC

Las compras y contrataciones efectuadas por los organismos gubernamentales deben cumplir con la ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones.

(a) Para realizar una compra dentro del departamento de TIC, debe elaborarse un documento de Solicitud de Propuesta (RFP, por sus siglas en inglés) que incluya como mínimo:

- Objetivo de la solicitud.
- Fecha de aprobación de la solicitud.
- Fecha de revisión (si aplica).

- Una definición de los términos utilizados en la solicitud.
- Alcance y los requisitos de la compra.
- Copia de los términos y condiciones que serán incluidos en el contrato.
- Anexos (si aplica).

(b) Si los equipos o software son rentados por un periodo de tiempo, debe exigirse un SLA como se especifica en la **sub-sección 2.03.2. Niveles de Servicio**.

(c) Para realizar una solitud de servicio o asesoría el departamento de TIC debe elaborarse un RFP que incluya como mínimo:

- Una definición de los términos utilizados en la solicitud y un resumen de los requisitos administrativos.
- Una breve descripción del servicio o asesoría.
- El alcance del servicio o asesoría.
- Los requisitos del servicio o asesoría.
- Una copia de los términos y condiciones que serán incluidos en el contrato.
- Anexos (si aplica).

(d) Todo RFP elaborado por el departamento de TIC, debe estar aprobado por el departamento de compras del organismo.

CAPÍTULO IV

INFRAESTRUCTURA TECNOLÓGICA

En el siguiente capítulo se establecen las directrices que todo organismo gubernamental debe aplicar para una correcta disposición de su infraestructura a nivel de conectividad, servicios de la Voz sobre IP[1] (VoIP, por sus siglas en inglés) y la documentación de la red, así como para la computación en la nube.

SECCIÓN 4.01.

Conectividad

Para una conectividad efectiva a nivel de datos, todos los organismos gubernamentales deben hacer una buena administración de su Red de Área Local[2], la Red Privada Virtual[3] y la Red de Área Local Inalámbrica[4] (LAN, VPN y WLAN, respectivamente, por sus siglas en inglés), evitando la infiltración de intrusos y pérdida de información.

Sub-sección 4.01.1. Administración de la red de área local

Toda LAN debe poseer un esquema de su topología de datos y direccionamiento, permitiendo así una mejor configuración y conexión física de sus equipos, tales como: enrutadores[5] y conmutadores[6]; por lo que estos deben cumplir con los

[1] Son recursos que permiten que una señal de voz sea transmitida, a través de Internet, mediante el protocolo IP.
[2] Es una red de datos con un alcance geográficamente limitado.
[3] Es una red virtual privada que permite de forma segura la interacción de datos sobre redes compartidas utilizando como vínculo el Internet.
[4] Es un sistema de comunicación inalámbrico, utilizado como otra opción a las redes locales, usando la tecnología de radiofrecuencia para llevar información de un punto a otro, permitiendo mayor movilidad y disminución en las conexiones cableadas.
[5] También conocido como router, son dispositivos utilizados para crear e intercomunicar sud-redes de datos.
[6] También conocido como switch, son dispositivos utilizados para conectar dos o más segmentos de redes.

requerimientos necesarios para operar en la red de datos[7].

Para más información sobre la estructura gráfica de las diferentes topologías, consultar el anexo F. Diseño de la topología de la red LAN.

Apartado 4.01.1.1. Topología y direccionamiento

(a) La LAN de cada organismo gubernamental debe estructurarse en base a una de las siguientes topologías de red:

- **Topología estrella**: Es aquella en la cual todos los puntos deben conectarse a un dispositivo central en la red.
- **Malla completa**: Es aquella en la cual todos los dispositivos deben tener conexión redundante entre sí.
- **Malla parcial**: Es aquella en la cual algunos dispositivos deben tener conexión redundante con otros dispositivos en la red.

(b) Todo direccionamiento de la red debe estructurarse en base a una de estas clases de direcciones IP privadas[8]:

- Direcciones de Clase A, las cuales comprenden un rango desde la 10.0.0.0 hasta la 10.255.255.255 para 16,777,214 dispositivos por red.
- Direcciones de Clase B, las cuales comprenden un rango desde la 172.16.0.0 hasta la 172.31.255.255 para 65,534 dispositivos por red.
- Direcciones de Clase C, las cuales comprenden un rango desde la 192.168.0.0 hasta la 192.168.255.255 para 254 dispositivos por red.

(c) Debe implementarse procesos para mejorar la segmentación de la red, tales como:

(i) División de sub-redes[9] como técnica de direccionamiento de la red.

[7] Hace referencia a un conjunto de dispositivos o computadores interconectados entre sí para el intercambio de información.
[8] Son direcciones IP utilizadas únicamente para la comunicación dentro de una red datos, por lo que estas direcciones IP no son utilizadas para el servicio de Internet.
[9] Es una técnica utilizada para la división de redes de datos en redes más pequeñas, bajo una misma mascara de red.

(ii) Máscaras de sud-red de tamaño Variable[10] (VLSM, por sus siglas en inglés) como solución de direccionamiento y reducir el desperdicio de direcciones IP[11].

(iii) Sumarización de direcciones IP[12], para la optimización recursos en los cálculos de las rutas IP.

(iv) Cualquier otro que se considere necesario.

Apartado 4.01.1.2. Enrutadores y conmutadores

(a) El enrutador debe contar con las siguientes características:

(i) Soportar mínimamente los siguientes protocolos:

- Protocolo de Información de Enrutamiento[13] (RIP, por sus siglas en inglés).
- Protocolo del Primer Camino Más Corto[14] (OSPF, por sus siglas en inglés).

(ii) Soporte para direccionamiento IPV4[15] e IPV6[16].

(iii) Herramientas para realizar el respaldo de las configuraciones.

(iv) Soporte o garantía por parte del proveedor, en caso de averías o daños.

(v) El enrutador debe ser interoperable con cualquier otro equipo de la red.

(vi) Acceso vía línea de comando y gráfica.

(vii) Controles de autenticación para el acceso.

[10] Es una técnica para brindar una mayor flexibilidad en uso de sub-redes, permitiendo al organismo dividir un sistema independiente utilizando más de una máscara de sub-red.
[11] Es una numeración que se le asigna de manera manual o automática a un dispositivo para identificarlo dentro de una red de datos.
[12] Es un método para reducir el número de entradas de direcciones IP al enrutador, teniendo como resultado una automatización en el cálculo de rutas.
[13] Es un protocolo de tipo vector-distancia empleado para intercambiar información sobre redes IP, el cual utiliza la cantidad de enrutadores presentes en una ruta.
[14] Es un protocolo de enrutamiento de tipo estado-enlace que utiliza el algoritmo Dijkstra para calcular la ruta más corta hacia un destino en específico.
[15] Es la cuarta versión del protocolo IP de 32 bits de longitud y fue la primera versión en ser implementada.
[16] Es la sexta versión del protocolo IP de 64 bit de longitud, con el fin de cubrir el agotamiento de las direcciones IPV4.

(b) El conmutador debe contar con las siguientes características:

(i) Compatibilidad con los estándares del IEEE:

- IEEE 802.1[17], para evitar el acceso no autorizado a la red de datos por medio de la capa 2[18].
- IEEE 802.3u[19] y superiores, como estándar para los medios Ethernet[20].

(ii) Soporte para los siguientes protocolos de gestión remota:

- Protocolo para la Transferencia Simple de Correo Electrónico (SNMP, por sus siglas en inglés).
- Protocolo de Red de Telecomunicación[21] (Telnet, por sus siglas en inglés).
- Protocolo de Transferencia de Hipertexto[22] (HTTP, por sus siglas en inglés).

(iii) Luces que indiquen el estado del equipo, tales como:

- Encendido.
- Actividad de conexión.
- Conexión estable.
- Cualquier otro estado necesario.

(iv) Debe tener herramientas para realizar respaldo de las configuraciones.

(v) Debe tener soporte o garantía por parte del proveedor, en caso de averías o daños.

[17] Es una norma de la IEEE para el control de acceso a la red mediante el uso de puertos de comunicación.
[18] Referente al modelo OSI, es la capa que se encarga de la transmisión fiable de datos y direccionamiento del control de acceso a los medios.
[19] Es un estándar de la IEEE para medios de transmisión Ethernet con velocidades de 100 Mbps.
[20] Son los diferentes tipos de vías por la cual se puede establecer una conexión entre dos o más dispositivos o computadores dentro del estándar Ethernet.
[21] Es un protocolo que nos permite acceder remotamente a otro equipo mediante una terminal, es decir sin gráficos.
[22] Es un protocolo utilizado para realizar la transferencia de texto o hipervínculos, a través de la web.

(vi) Debe ser interoperable con cualquier otro equipo de la red.

(vii) Debe permitir la implementación de Red de Área Local Virtuales[23] (VLAN, por sus siglas en inglés).

(viii) Debe permitir configuraciones para la segmentación de la red[24].

Apartado 4.01.1.3. Conexión física entre dispositivos

(a) Si la longitud del segmento de red de dato es igual o menor a 100 metros, debe utilizarse la configuración en base a:

- 100BASE-T[25], para Fast Ethernet[26] sobre Par Trenzado sin Blindaje[27] (UTP, por sus siglas en inglés).
- 1000BASE-T[28], para Gigabite Ethernet sobre Par Trenzado sin Blindaje (UTP, por sus siglas en inglés).

(b) Si la longitud máxima del segmento es de 550 metros, debe utilizarse Gigabit Ethernet[29] 1000BASE-LX[30].

(c) Si la longitud máxima del segmento es de 220 metros, debe utilizarse Gigabit Ethernet 1000BASE- SX[31] 62.5 de micrones[32].

(d) Todo el cableado de la red debe estar etiquetado e identificado.

(e) Las categorías de cable UTP permitidas son las siguientes:

- Categoría 5e, para soportar velocidades de transmisión de datos hasta los 100 Mbps.

[23] Es una red interna virtual, que permite crear redes lógicas dentro de una misma red física.
[24] Es la conexión que existe entre un dispositivo o computador y un equipo de la red datos como un switch o un router.
[25] Es estándar para cables de par trenzado sin blindaje, utilizado para recorrer distancias no mayor a 100 metros a una velocidad de transmisión de 100 Mbps.
[26] También conocido como Ethernet de alta velocidad, es un conjunto de estándares de la IEEE para redes Ethernet con velocidades de 100 Mbps.
[27] Es un tipo de cable de par trenzado utilizado para las telecomunicaciones. El trenzado de estos cables anula las interferencias de fuentes externas.
[28] Es un estándar para cables de par trenzado sin blindaje, donde se utilizan los cuatro pares del cableado simultáneamente para transmitir datos a 1,000 Mbps.
[29] Es un estándar para los tipos de cables cuya velocidad de transmisión de datos es de 1,000 Mbps.
[30] Es un estándar para cables de fibra óptica que recorren una distancia menor a los 10 kilómetros.
[31] Es un estándar para cables de fibra óptica que recorren una distancia menor a los 550 kilómetros.
[32] Es la millonésima parte de un metro, y corresponde a una unidad de medida de longitud en el cableado de fibra óptica.

- Categoría 6, para soportar velocidades de transmisión de datos hasta los 1,000 Mbps.
- Categoría 7, para soportar velocidades de transmisión de datos hasta los 10 Gigabit Ethernet.

(f) La configuración del medio de transmisión de datos debe ser en bidireccional simultánea.

(g) El conector terminal para el cableado debe ser:

- Para UTP:
  - Conector Registrado 45[33] (RJ-45, por sus siglas en inglés) para UTP.
- Para fibra óptica[34]:
  - Conector Cuadrado y el Conector Cuadrado Dúplex[35] (SC, por sus siglas en inglés).
  - Conector de Punta Recta (ST, por sus siglas en inglés).
  - Conector Lucent[36] (LC, por sus siglas en inglés).
  - Conector de Canal de Fibra[37] (FC, por sus siglas en inglés).
  - Conector de Interfaz de Datos Distribuida por Fibra[38] (FDDI, por sus siglas en inglés).

Sub-sección 4.01.2. Administración de la red privada virtual y la red de área local inalámbrica

(a) Los protocolos de seguridad en las conexiones en una VPN que los organismos deben utilizar son los siguientes:

- Seguridad del protocolo IP[39] (IPsec, por sus siglas en inglés).

[33] Es un conector utilizado en el cable UTP para establecer conexiones con los dispositivos de una red de datos.
[34] Es un hilo de vidrio o plástico, por el cual se transmiten datos en forma de pulsos de luz.
[35] Son conectores para cables de fibra óptica de forma cuadrada, su diseño permite el fácil manejo y la reducción de daños en la fibra óptica durante su instalación.
[36] Es un conector para cable de fibra óptica utilizado para transmisiones de datos de alta densidad.
[37] Es un tipo de conector para cables de fibra óptica utilizados en ambientes con altas vibraciones.
[38] Es un tipo de conector utilizado en redes de fibra óptica.
[39] Es un conjunto de protocolos que proporcionan seguridad al protocolo IP en cuanto a la autenticación y cifrado de los datos.

- Capa de Conexión Segura[40] (SSL, por sus siglas en inglés).
- Intérprete Órdenes Seguras (SSH, por sus siglas en inglés).

(b) Las conexiones VPN deben utilizar algoritmos y protocolos que aseguren la integridad de los datos, tales como:

- Algoritmo de Resumen del Mensaje[41] (MD5, por sus siglas en inglés).
- Algoritmo de Hash[42] Seguro (SHA1, por sus siglas en inglés).

(c) Debe implementarse algoritmos de cifrado de datos[43], tales como:

- El Estándar Triple de Cifrado de Datos[44] (TDES, por sus siglas en inglés).
- El Estándar de Cifrado Avanzado[45] (AES, por sus siglas en inglés).

(d) Los estándares que deben utilizarse para la conexión en la WLAN tienen que estar bajo criterios de la IEEE.

(e) La WLAN debe tener métodos de cifrado como el Acceso WIFI Protegido[46] (WPA, por sus siglas en inglés), el Acceso WIFI Protegido 2 (WPA2, por sus siglas en inglés) y cualquier otro superior.

(f) Debe proveer funcionalidad para las Zonas Desmilitarizadas[47] (DMZ, por sus siglas en inglés), el protocolo de Autenticación Remota para Servicios de Marcado a Usuarios[48] (RADIUS, por sus siglas en inglés) y el Protocolo de configuración Dinámica de Host[49] (DHCP, por sus

[40] Es un protocolo de seguridad para conexiones de transmisión información, el cual emplea autenticación y cifrado de datos.
[41] Es un algoritmo de cifrado que utiliza una codificación de 128 bits.
[42] Es una función que utilizada un algoritmo de computación para realizar, a partir de cualquier dato de entrada, la conversión del mismo a una cadena que solo es posible volver a crear con dicha entrada.
[43] Es un proceso que utiliza algoritmos matemáticos para la protección de datos.
[44] Encriptación de triple cifrado con una longitud de la clave de 112 bits.
[45] Es un algoritmo de cifrado publicado por el Instituto Nacional de Normas y Tecnologías (NIST, por sus siglas en inglés) del gobierno de Estados Unidos. Se conoce popularmente como Rijndael y es utilizado para la criptografía simétrica.
[46] Protocolo utilizado para la protección de las redes inalámbricas, adoptando la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.
[47] Es una red de datos localizada entre la red de datos del organismo y la red externa, esta funciona como una zona de seguridad en donde las conexiones externas tienen restringido el acceso a la red de datos del organismo, evitando así, comprometer la seguridad del mismo.
[48] Es un protocolo de autentificación para acceso a redes.
[49] Es un protocolo de red, el cual permite a los ordenadores obtener una dirección IP de manera automática,

siglas en inglés).

(g) Debe estar en una sub-red diferente a las demás redes.

Sub-sección 4.01.3. Estructura del centro de datos y administración de servidores

Los organismos gubernamentales deben disponer de una topología de red[50] del centro de datos, la cual permita identificar las diferentes áreas de operación, disposición de equipos y cableados. Del mismo modo, debe contar con un sistema de ventilación y espacios físicos adecuados. Los servidores de datos deben estar administrados contando con políticas de seguridad y herramientas de respaldo de información, así como también con los requerimientos mínimos de hardware para su operación.

Apartado 4.01.3.1. Topología del centro de datos

(a) Debe crearse un diseño de la topología como se muestra en el **anexo G. Diseño para la topología del centro de datos**.

(b) Debe contar con un Cuarto de Entrada[51] (ER, por sus siglas en inglés) para la conexión del proveedor del servicio.

(c) Debe contar con un Área Central de Distribución[52] (MDA, por sus siglas en inglés) para la conexión del cableado Cruzado Principal[53] (MC, por sus siglas en inglés).

(d) Debe contar con un Área Horizontal de Distribución[54] (HDA, por sus siglas en inglés) para la conexión del cableado Cruzado Horizontal (HC, por sus siglas en inglés).

(e) Debe contar con un Área de Distribución Zonal[55] (ZDA, por sus siglas en inglés) para el punto de consolidación[56].

así como otros parámetros de configuración.

[50] Es la arquitectura física y lógica de una red. En esta se representan todos los enlaces y dispositivos que se relacionan entre sí.

[51] Es un área dentro del centro de datos en la cual se encuentran los cables, dispositivos o equipos provistos por el proveedor servicio.

[52] Es donde se encuentra localizado el cableado cruzado principal.

[53] También conocido como backbone, es el cableado que conecta el MDA con el HDA.

[54] Es el área donde se localiza el cableado cruzado horizontal.

[55] Es donde se aloja el cableado horizontal, el cual conecta el HDA con los equipos y armarios en el EDA.

[56] Son los puntos de interconexión entre cableados horizontales.

(f) Debe contar con un Área de Distribución de Equipos[57] (EDA, por sus siglas en inglés) para la localización de los equipos y armarios.

(g) Debe contar con un área para el centro de operaciones y soporte.

Apartado 4.01.3.2. Cableado del centro de datos

(a) El cableado entre las diferentes áreas debe tener las siguientes especificaciones:

(i) Contar con un cableado horizontal desde HDA a una entrada en el EDA o ZDA.

(ii) El tipo de cable a utilizar debe tener las siguientes especificaciones:

a) Cable de par trenzado de 100 ohm de categoría 6, certificado bajo el estándar ANSI/TIA/EIA-568B.2-1[58].

b) Cable de fibra óptica multimodo[59] 62.5/125 micrones, 50/125 micrones, o algún otro superior, aprobado por el estándar ANSI/TIA/EIA-568-B.3.

c) Cable de fibra óptica monomodo, certificado bajo el estándar ANSI/TIA/EIA-568-B.3[60].

d) Cable coaxial de 75 ohm tipo 734[61] y 735[62].

(iii) La distribución del cableado debe ser mediante bandejas o canaletas que posean las diferentes divisiones, tanto para cableado UTP, coaxial, fibra óptica y el cableado eléctrico.

(iv) Debe elaborarse y aplicarse un esquema de etiquetado para los armarios, cables, paneles de conexión y los cables de conexión entre los paneles.

[57] Es un área dentro de un centro de datos donde se encuentran los dispositivos de almacenamiento y los servidores de aplicaciones del organismo.
[58] Es un estándar que define las características físicas de debe poseer un cable de par trenzado sin blindaje de categoría 6.
[59] Es un tipo de fibra óptica, en el cual los pulsos de luz toman diferentes modos o vías para ser transmitidos dentro de la fibra óptica.
[60] Es un estándar de cable que describe los componentes físicos que debe poseer un cable de fibra óptica.
[61] Es un cable de cobre de calibre 26, usado para recorrer distancias menores a los 225 pies.
[62] Es un cable de cobre de calibre 20, usado para recorrer distancias menores a los 450 pies.

Apartado 4.01.3.3. Condiciones físicas y ambientales del centro de datos

(a) La altura mínima del centro de datos debe ser de 2.6 metros.

(b) El tamaño de la puerta debe ser igual o superior a 1 metro de ancho y 2.13 metros de alto.

(c) La temperatura debe estar entre 20 y 25 grados *Celsius*.

(d) Debe contar con una alarma contra incendios.

Apartado 4.01.3.4. Administración de servidores del centro de datos

(a) El servidor debe contar con las siguientes especificaciones mínimas:

- Una herramienta de respaldo y un sistema de restauración en caso de fallas.
- Tarjeta de red[63] redundante.
- Reporte o informe de fallas en el hardware y sistema del equipo.
- Utilizar técnicas para el balanceo de cargas[64] cuando exista una saturación en el tráfico de información.

(b) Debe utilizarse servidores de prueba, antes de realizar cambios en la red en un ambiente de producción.

(c) Debe aplicarse políticas de control y manteamiento, tales como:

(i) Establecer políticas y controles para la aplicación de actualizaciones, tomando en cuenta las directrices mencionadas en la **sub-sección 5.01.2. Actualización del software adquirido**.

(ii) Elaborar políticas de usuario para la asignación de los privilegios de acceso físico al centro de datos, según lo establecido en el **apartado 6.03.5.2. Controles de acceso a la infraestructura**.

[63] Es una tarjeta o adaptador que permite la comunicación entre dos dispositivos en una red datos, a través de un medio físico o inalámbrico.

[64] Es un tipo de técnica utilizado en informática, en la cual las operaciones realizadas en un servidor son compartidas con otros servidores o recursos en la red, con el objetivo de evitar la saturación información.

(iii) Establecer políticas para la generación de copias de respaldo[65] del sistema de acuerdo a lo establecido en la **sub-sección 6.02.4. Respaldo de la información**.

(iv) Elaborar políticas de seguridad basadas en el uso de sistemas de protección contra intrusos.

(d) Los servidores deben contar mínimamente con los siguientes sistemas de protección:

- Antivirus[66].
- Cortafuegos[67].

(e) Debe utilizarse una o más de las siguientes tecnologías de almacenamiento que soporten Entradas y/o Salidas[68] (I/O, por sus siglas en inglés) o un Conjunto Redundante de Discos Independientes[69] (RAID, por sus siglas en inglés) tales como:

- Acoplamiento de Serie de Tecnología Avanzada[70] (SATA, por sus siglas en inglés).
- Interfaz de Sistema para Pequeñas Computadoras versión 3[71] (SCSI 3, por sus siglas en inglés).
- Acoplamiento Serial SCSI[72] (SAS, por sus siglas en inglés).
- Unidad de Estado Sólido (SSD, por sus siglas en inglés).
- Cualquier otro medio compatible con esas tecnologías.

[65] Son copias de los datos almacenados de un sistema, con el objetivo de tenerlos disponibles en caso de fallas.
[66] Es un programa desarrollado con el fin de proteger un computador o servidor contra virus informáticos.
[67] También conocido como firewall, es un sistema que brinda protección contra la infiltración de intrusos a los recursos de una red, equipo o servicio.
[68] Para fines de esta norma, es la forma de comunicación que se da entre un sistema de información con un medio de almacenamiento externo.
[69] Es un sistema de almacenamiento de datos que utiliza varios medios de almacenamiento para distribuir o replicar información.
[70] Es una interfaz de datos para transferir información entre una placa base y dispositivos de almacenamiento.
[71] Es una interfaz de datos para transferir información en serie, con una velocidad trasmisión de 20MB/s a 80MB/s dependiendo de su implementación, con soporte para 15 dispositivos.
[72] Es una interfaz de datos para transferir información en serie, con una velocidad de trasmisión de 3.0 Gbit/s a 6.0 Gbit/s, con soporte para 65,535 dispositivos.

Sub-sección 4.01.4. Administración del servicio de voz sobre IP

(a) El cableado de la red debe estar basado en UTP categoría 5e o superior.

(b) Debe separarse el direccionamiento de la VOIP de la red de datos.

(c) Los conmutadores utilizados para la implementación de la VOIP deben soportar:

- Arquitectura de conmutación en base a VLAN, para una mejor segmentación del tráfico de la red generado por el VoIP.
- Calidad de servicio[73] (QoS, por sus siglas en inglés), para obtener un mejor rendimiento en el tráfico de llamadas en la red.

SECCIÓN 4.02.

Documentación de la red de datos

(a) Debe elaborarse un diagrama de la LAN, en el cual se presenten como mínimo los siguientes elementos:

- **Dispositivos de la red**: Enrutador, conmutador, servidores y cualquier otro equipo de relevancia que contenga la topología.
- Líneas de conexión entre los diferentes dispositivos.
- Nombre de la interfaz física[74] de los dispositivos.

(b) Debe realizarse una documentación del direccionamiento IP de la red que contenga como mínimo los siguientes requerimientos:

- Sub-redes.
- Las VLAN.
- Direcciones IP asignadas y su máscara de red[75].
- Cantidad de equipos en el segmento de red.

[73] Hace referencia al rendimiento de una red telefónica o de computadoras.
[74] Para fines de esta norma, es el medio que utilizan los dispositivos o computadores para conectarse a la red de datos.
[75] Permite a los dispositivos identificar cuál es la sud-red a la que pertenecen.

- Código de los equipos.
- Paquete de direcciones IP públicas[76] provistas por los Proveedores de Servicio de Internet[77] (ISP, por sus siglas en inglés).

(c) Debe elaborarse un plan de distribución del cableado especificando la siguiente información:

- **Lugar de conexión**: Este incluye la conexión de los Puntos de Distribución Central (MDF, por sus siglas en inglés) a los Puntos de Distribución Intermedios[78] (IDF, por sus siglas en inglés) o algún otro lugar de conexión en la topología.
- Código de cable que conecta ambos puntos.
- Tipo de conexión cruzada vertical[79] o conexión cruzada horizontal[80], y el número de puerto de conexión[81] en el dispositivo.
- Tipo de cable utilizado.
- Estado de la conexión, si es habilitado o deshabilitado.

(d) Si toda la documentación es realizada a través de un software o una CMDB, este debe proveer toda la información antes descrita y cualquier otra de interés para el organismo gubernamental.

SECCIÓN 4.03.

Computación en la nube

Con el objetivo de mejorar los servicios utilizados y ofrecidos por los organismos gubernamentales mediante el uso de la nube computacional, se describen las siguientes pautas que deben implementarse para una efectiva administración y configuración de esos servicios e infraestructura.

[76] Son un tipo de direcciones IP que se utilizan para establecer comunicación a través del Internet, por lo que su uso no aplica a lo interno de una red de datos.
[77] Son todas aquellas empresas que ofrecen el servicio de conexión a Internet.
[78] Es el área dentro de una LAN donde se distribuye todo el cableado de datos correspondiente a los usuarios. Comúnmente también se alojan equipos de redes, tales como, conmutadores, enrutadores o servidores de respaldos.
[79] Es el cableado que conecta el/los IDF con el MDF en una LAN.
[80] Es el cableado que conecta un IDF con los equipos de las diferentes áreas de trabajos en una LAN.
[81] Hace referencia a una interfaz física para transferencia de datos.

(a) Todo servicio computacional en la nube utilizado o implementado por los organismos gubernamentales debe cumplir con las siguientes características:

- Auto-servicio bajo demanda[82], en el cual los organismos puedan solicitar recursos sin interacción con el proveedor.
- Acceso a través de diferentes medios, permitiendo a los organismos acceder mediante cualquier dispositivo.
- Agrupación de recursos, en el cual los recursos se encuentren agrupados en un lugar común para diferentes organismos.
- Elasticidad[83], en la cual los organismos puedan aumentar la capacidad de sus recursos de acuerdo a las necesidades.
- Medición del servicio, en donde el organismo pueda monitorear y controlar el uso de sus recursos.

(b) Todo modelo de servicio computacional en la nube utilizado o implementado por los organismos gubernamentales debe estar bajo los siguientes criterios:

(i) Para una Infraestructura como Servicio[84] (IaaS, por sus siglas en inglés):

a) Debe proveerse al organismo de procesamiento, almacenamiento, redes y cualquier otra característica de hardware necesitado, en la cual el organismo pueda implementar sus sistemas o aplicaciones.

b) El organismo, debe administrar sus aplicaciones y sistemas dispuestos sobre la infraestructura de la nube computacional.

c) La infraestructura física de la nube computacional debe estar administrada por el proveedor del servicio.

[82] Referente al servicio en la nube computacional, es donde el usuario pueda gestionar los servicios en tiempo real, sin interacción directa con el proveedor del mismo.

[83] Es la capacidad que tienen los servicios ofrecidos, a través de la nube computacional, para aumentar o reducir sus recursos en tiempo real, de acuerdo a la necesidad del usuario.

[84] Es un servicio de computación en la nube, en el cual el cliente tiene a su disposición una infraestructura de datos virtual.

(ii) Para una Plataforma como Servicio[85] (PaaS, por sus siglas en inglés):

a) Debe permitírsele al organismo, desarrollar y ejecutar sistemas codificados en base a diferentes lenguajes de programación y tecnologías que el proveedor del servicio brinde soporte.

b) El organismo debe tener control de las aplicaciones y sistemas desarrollados.

c) La infraestructura física de la nube computacional debe estar administrada por el proveedor del servicio.

(iii) Para un Software como Servicio[86] (SaaS, por sus siglas en inglés):

a) El organismo debe hacer uso de todas las aplicaciones que se ejecutan en la infraestructura de la nube computacional.

b) Las aplicaciones ejecutan en la infraestructura de la nube computacional deben ser accesibles por el organismo desde cualquier dispositivo, a través de un navegador web[87].

c) El proveedor del servicio debe administrar y controlar toda la infraestructura de la nube computacional, así como aplicaciones y sistemas.

(c) Todo servicio computacional en la nube utilizado o implementado por los organismos gubernamentales debe tener al menos una 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

[85] Es un servicio de computación en la nube, en el cual el cliente tiene a disponible una plataforma para desarrollar y ejecutar diferentes tipos de software, siempre y cuando estos sean compatibles con dicha plataforma de información.

[86] Hace referencia a un modelo de distribución de software donde los datos y el soporte del mismo están alojados en una compañía que da servicios de TIC donde este es accedido desde el navegador.

[87] Es un tipo de software utilizado para acceder de forma gráfica a los recursos disponibles en una red o Internet.

Compromisos 340 (SSAE 16/ISAE, por sus siglas en inglés), para medir el control de las informaciones financieras de una organización o presa de servicios.

- Matriz de Control en la Nube[88] (CCM, por sus siglas en inglés), creada por la CSA para controles de seguridad en plataformas de clientes y proveedores de servicios computaciones en la nube.

[88] Es una matriz de control desarrolla por la CSA para ayudar a los clientes a evaluar los niveles de riesgos de seguridad de los proveedores de servicio en la nube computacional.

CAPÍTULO V

ADMINISTRACIÓN Y DESARROLLO DE SOFTWARE

En este capítulo se presentan las directrices que deben aplicar los organismos gubernamentales para lograr una mejor administración y uso del software, así como el desarrollo del software gubernamental, estableciendo una vía de control y estandarización en cada uno de sus procesos.

SECCIÓN 5.01.

Administración del software

En la siguiente sección de establecen las pautas y lineamientos que los organismos gubernamentales deben implementar al momento de instalar, reinstalar o actualizar un software, así como también las políticas de uso.

Sub-sección 5.01.1. Instalación y reinstalación del software

(a) Todo requerimiento o solicitud de instalación, reinstalación o reparación del software por parte de un usuario, debe ser realizado mediante correo electrónico o algún otro medio de comunicación usado por el organismo, detallando como mínimo:

- Nombre de usuario.
- Cargo de usuario.
- Razones de la instalación/reinstalación.
- Programas, aplicaciones o utilitarios a instalar o reinstalar.

(b) Todo requerimiento o solicitud de instalación, reinstalación o reparación de software perteneciente a la plataforma de TIC[1], debe ser aprobado por el personal autorizado del área de Operaciones TIC.

(c) Para la instalación del software adquirido debe cumplirse con los requerimientos mínimos de hardware especificados por el fabricante como:

- Tipo de procesador.
- Cantidad de memoria.
- Cantidad de espacio en disco.
- Sistema operativo o plataforma compatible.
- Cualquier otro requerimiento especificado por el fabricante.

(d) La unidad de administración del servicio TIC debe contar con un personal que asuma la función de las instalaciones, reinstalaciones o reparaciones del software en los equipos de los usuarios. Para las instalaciones, reinstalaciones o reparaciones en equipos, tales como servidores, base de datos, equipos de redes y comunicaciones entre otros, la unidad de operaciones TIC debe contar con el personal necesario para realizar estas funciones.

(e) El personal designado debe tener conocimientos técnicos de los sistemas operativos y aplicaciones utilizadas en las áreas de operación y administración TIC antes mencionadas.

(f) Antes de realizarse la desinstalación del software adquirido en la infraestructura TIC, debe hacerse un respaldo de los archivos o informaciones como se establece en la **sub-sección 6.02.4. Respaldo de la información**.

(g) Toda instalación, reinstalación o reparación del software adquirido en la plataforma TIC o en los equipos de usuario debe ser documentada.

[1] Para fines de esta norma, se refiere al tipo de arquitectura, sistema operativo, lenguaje de programación o interfaz de usuario, que en conjunto establecerán el sistema base para hacer operar determinados hardware o software dentro de un organismo.

(i) La documentación debe contener como mínimo:

- Nombre del software adquirido y tipo de software adquirido.
- Justificación de la instalación, reinstalación o reparación.
- Equipo donde se realizó la instalación, reinstalación o reparación.
- Responsable de la instalación, reinstalación o reparación.

Sub-sección 5.01.2. Actualización del software adquirido

(a) Para la actualización del software[2] adquirido con carácter crítico, debe cumplirse con las siguientes directrices:

(i) Autorización del personal responsable dentro del área de operaciones TIC.

(ii) Tener una copia de seguridad del sistema en caso de fallas.

(iii) Realizar las actualizaciones del software adquirido luego de la jornada laboral o en horas donde se experimente menos uso del ancho de banda[3] de la red.

(iv) Descargar las actualizaciones directamente desde el proveedor.

(b) Los departamentos de TIC deben elaborar políticas para la implementación de aquellas actualizaciones que no sean consideradas como críticas.

(c) Las políticas de actualizaciones automáticas realizadas mediante un servidor de aplicaciones, repositorio o algún otro medio, deben ser elaboradas por el departamento de TIC, tomando las siguientes medidas:

(i) Las actualizaciones del software adquirido deben ser programadas en horas no laborales o en horas donde se experimente menos uso del ancho de banda de la red.

[2] Hace referencia a un consolidado de cambios para ser aplicados a un programa o plataforma para corregir errores y agregar funcionalidades.

[3] Es la cantidad de bits que se pueden transmitir en un tiempo determinado entre dos dispositivos digitales o en un sistema de transmisión.

(ii) El proceso de actualización no debe interrumpir los servicios del organismo gubernamental.

(iii) El proceso de actualización entre el servidor o repositorio de aplicaciones o y el proveedor, no debe afectar el ancho de banda de la red.

Sub-sección 5.01.3. Políticas de uso del software adquirido

(a) Debe elaborarse políticas para el uso del software adquirido, en donde se establezcan los derechos y restricciones que tienen los usuarios respecto al software adquirido instalado en el equipo.

(b) Las políticas de uso del software adquirido deben ser dadas a los usuarios, mediante correo electrónico, Intranet o cualquier medio de comunicación que el organismo considere.

(c) Los departamentos de TIC deben implementar controles que eviten la instalación y desinstalación del software adquirido.

(d) El software utilizado por el organismo debe estar provisto con el soporte necesario por parte del proveedor.

SECCIÓN 5.02.

Desarrollo del software gubernamental

Todo software gubernamental desarrollado por los organismos debe mantener un marco de usabilidad[4] y accesibilidad[5] para seguir una metodología que permita la buena gestión de los requerimientos, diseño, codificación y prueba del software gubernamental, cumpliendo así con la calidad y el tiempo a la hora de la entrega del producto final.

Sub-sección 5.02.1. Usabilidad del software gubernamental

(a) El software gubernamental debe estar diseñado para ofrecer la mejor experiencia al usuario tomando como referencia los siguientes criterios:

[4] Es la facilidad con la que el usuario puede interactuar con un software para la realización de una tarea en específica. Este término fue definido por primera vez por Jakob Nielsen considerado el padre la usabilidad.
[5] Es el grado en que las personas, sin importar su capacidad, puedan acceder y manipular un software.

(i) Evitar el uso de ventanas emergentes[6] cuando estas no sean solicitadas por el usuario.

(ii) Mantener la homogeneidad del software gubernamental permitiendo que los usuarios realicen las tareas en el mismo orden lógico y en las mismas condiciones en todas las pantallas.

(iii) Si la pantalla en la que se encuentra el usuario tiene un límite de tiempo, informar al usuario antes de que este expire.

(iv) Retroalimentar al usuario mientras este espera por la finalización de un proceso o tarea:

a) Si el proceso o la tarea dura más de 10 segundos, debe hacerse uso de un reloj de arena, barra de progreso o algún otro indicativo.

(v) Tener una opción de ayuda, en caso de que el usuario lo necesite.

(vi) Tener una resolución de pantalla[7] mínima para visualización de las pantallas de 1024 x 768 pixeles.

(b) Poseer una pantalla de inicio:

(i) El usuario debe poder acceder a la pantalla de inicio en todo momento.

(ii) Todos los elementos y opciones principales deben estar presentes en la pantalla de inicio.

(c) Utilizar un diseño adecuado cuando se necesite visualizar una información en pantalla, evitando que los usuarios tengan que desplazarse horizontalmente.

(d) Informar al usuario en qué pantalla se encuentra:

(i) Debe destacarse el menú[8] en donde se encuentra el usuario.

(ii) Cuando el usuario hace clic sobre un botón dentro de la pantalla

[6] Las ventanas emergentes, también conocidas como pop-up, son ventanas o navegadores que abren automáticamente para presentar un contenido específico, los cuales, en su mayoría, abren sin el permiso o consentimiento del usuario.

[7] Es la cantidad máxima de pixeles que pueden ser mostrados en un monitor.

[8] Son una serie de opciones dispuestas para el usuario para poder acceder a diferentes secciones o páginas internas de un portal web.

este debe cambiar de color o forma.

(iii) Cuando se utilicen formularios, los campos requeridos deben diferenciarse de los campos opcionales.

(iv) El formulario debe validar los datos antes hacer el envío.

(v) No debe existir faltas ortográficas.

Sub-sección 5.02.2. Accesibilidad del software gubernamental

(a) El software gubernamental debe permitir la navegación, a través del menú principal, y seleccionar todos los elementos del menú, incluyendo el menú del sistema por medio del teclado.

(b) Cada función de la barra de herramientas[9] debe ser seleccionable desde el teclado.

(c) Todas las funciones básicas del teclado y atajos deben estar disponibles.

(d) El usuario debe navegar por el área de texto o contenido por medio del teclado.

(e) El usuario debe acceder a cualquier interfaz de la aplicación utilizando el teclado.

(f) Cuando se utilice elementos de multimedia[10] en la aplicación, estos deben incorporar:

- Una indicación de la señal del sonido y audio.
- Gráficos descriptivos para la señalización del audio.
- Textos descriptivos para la señalización del video.
- Una opción donde el usuario pueda habilitar o deshabilitar el sonido o ajustar el volumen.

(g) No debe utilizarse objetos que provoquen parpadeos o movimientos continuos en el contenido.

[9] Es un elemento que contiene las funciones principales de una aplicación en forma de íconos o hipervínculos.
[10] Se refiere al conjunto de elementos de audio, video, textos, imágenes o animaciones usados para comunicar una información.

(h) La información o contenido no debe depender de los colores.

(i) No debe haber elementos escondidos u ocultos.

(j) Todos los controles deben estar con una etiqueta que describa su utilidad.

(k) Debe evitarse que los controles no disponibles puedan ser marcados con el cursor.

(l) Todos los elementos de una ventana deben tener una tabulación y orden lógico.

(m) Todo tipo de fuente[11] debe ser legible y entendible por el usuario.

(n) Las imágenes e íconos deben ser descriptivos y objetivos a su función.

Sub-sección 5.02.3. Metodología para el desarrollo del software gubernamental

La metodología para el desarrollo del software gubernamental, debe seguir un conjunto de procesos, los cuales se describen en el **anexo H. Metodología de desarrollo del software gubernamental**.

Apartado 5.02.3.1. Proceso de gestión de los requerimientos

(a) Debe elaborarse una lista ordenada con todos los requerimientos del software gubernamental suministrados por los interesados, especificando como mínimo:

- Prioridad de cada requerimiento.
- Validación y aceptación de cada requerimiento por los interesados.
- Características, funcionalidades, requisitos, mejoras y correcciones que se vayan realizando sobre cada entrega del prototipo[12] del software gubernamental.

[11] Es la forma en la cual se representa o visualiza una letra, número o símbolo.
[12] Es la representación inicial de un producto entregable, con el objetivo de aplicarle mejoras o correcciones.

(b) La lista de requerimientos del software gubernamental debe contar con los siguientes atributos:

- Descripción del requerimiento.
- Número de orden del requerimiento.
- Tiempo estimado para desarrollo del requerimiento.
- Valor del requerimiento dado por la parte interesada.

(c) La prioridad y los detalles de cada requerimiento solo deben ser actualizados o modificados a solicitud del departamento de TIC con aprobación de las partes interesadas.

(d) El software gubernamental debe dividirse en prototipos, los cuales serán mostrados y entregados a los interesados.

Apartado 5.02.3.2. Proceso de planificación del desarrollo

(a) Debe realizarse un plan de desarrollo en base a un periodo de tiempo no mayor de un mes.

(b) El plan de desarrollo debe contener como mínimo los siguientes elementos:

- Lista de requerimientos seleccionados para la entrega del prototipo.
- Objetivo que se alcanzará en la entrega de cada prototipo.
- Detalles que contendrá la entrega de cada prototipo.
- Capacidad de desarrollo para la ejecución del desarrollo.

(c) Debe decidirse y evaluarse cuáles son los requerimientos que se tomarán en cuenta de la lista para la entrega de cada prototipo.

(d) Una vez seleccionados los requerimientos para la entrega del prototipo y estos sean aprobados por las partes interesadas, debe elaborarse:

(i) Un diseño general de la arquitectura del software gubernamental, utilizando uno de los siguientes patrones arquitectónicos:

- Arquitectura en base a modelos y vistas, y cualquier otro que

se adapte a este patrón, con el objetivo de separar los datos, las funcionalidades del software gubernamental y la interfaz del usuario[13].

- Arquitectura por n-capas[14], donde el software gubernamental sea segregado en el número de capas necesarias.

(ii) Un diseño preliminar de las interfaces de usuario, pantallas y cualquier otro elemento o componente del software gubernamental.

(iii) Un diseño inicial de la base datos, tomando en cuenta los siguientes criterios:

a) Las base de datos, tanto relacional como orientadas a objetos, debe soportar los siguientes formatos para el intercambio de información:

- Notación de Objetos de JavaScript (JSON, por sus siglas en inglés) y sus variantes.
- Lenguaje de Marcas Extensible (XML, por sus siglas en inglés) y sus variantes.
- Valores Separados por Coma (CSV, por sus siglas en inglés).
- Valores Separados por Delimitadores (TSV, por sus siglas en inglés).

(e) Los diseños elaborados deben ser incluidos dentro del plan de desarrollo y actualizados cada vez que se genere algún cambio.

(f) Debe especificarse el tiempo que se tomará para entregar cada prototipo.

(g) Debe informarse a las partes interesadas mediante una documentación o comunicación cómo será ejecutado el desarrollo para cumplir con la entrega del prototipo.

Apartado 5.02.3.3. Proceso de organización del desarrollo

(a) Una vez seleccionados los requerimientos para la entrega del prototipo

[13] Es el medio por el cual el usuario puede interactuar con un dispositivo o computador.
[14] Es utilizado para referirse al número de niveles que componen la arquitectura de un software.

debe listarse, dividir y seleccionar los requerimientos con los cuales se trabajará diariamente.

(b) La lista de requerimientos diarios debe ser actualizada constantemente durante la realización del desarrollo, mostrando lo siguiente:

- Requerimiento completado.
- Requerimiento pendiente.
- Requerimiento actualizado.
- Requerimiento eliminado.

(c) Cuando uno de los requerimientos de la lista de desarrollo diario pasa a ser innecesario este debe ser eliminado.

Apartado 5.02.3.4. Proceso de desarrollo diario

(a) Durante el desarrollo diario cada participante en el desarrollo debe informar:

- Desarrollo realizado el día anterior.
- Desarrollo que realizará.
- Impedimentos que puedan atrasar la ejecución del desarrollo diario.

(b) El prototipo debe desarrollarse cumpliendo con los requerimientos obtenidos en la lista de requerimientos del software gubernamental y con el diseño general de la arquitectura del software gubernamental.

(c) El código fuente[15] debe estar comentado.

(d) Las variables deben ser nombradas de acuerdo a su función en el código fuente.

(e) Todo el código fuente debe estar claramente tabulado.

(f) Debe implementarse herramientas para el control de versiones del código fuente.

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

(g) Debe realizarse pruebas de unidad en cada uno de los módulos[16], verificando que estos cumplan con los requerimientos del software gubernamental. Ver **apartado 5.02.3.1. Proceso de gestión de los requerimientos**.

(h) Debe realizarse pruebas de integración, verificando que los módulos sean interoperables entre sí.

Apartado 5.02.3.5. Proceso de revisión del desarrollo

(a) Para la revisión del desarrollo debe realizarse una prueba general del prototipo del software gubernamental, donde se compruebe su funcionamiento y estabilidad.

(b) Debe verificarse cuáles funcionalidades de la lista de requerimientos del software gubernamental se han completados y cuáles están pendientes.

(c) Si la parte interesada añade nuevos requerimientos después de presentar el prototipo, la lista de requerimientos del software gubernamental debe ser actualizada.

(d) Los resultados de la prueba general del prototipo del software gubernamental deben incluirse dentro del plan de desarrollo.

Apartado 5.02.3.6. Proceso de recapitulación del desarrollo

(a) Debe identificarse y ordenarse las actividades más importantes que salieron de forma efectiva y las posibles mejoras a realizarse.

(b) Estas informaciones deben estar contenidas dentro del plan de desarrollo.

SECCIÓN 5.03.

Software libre en la administración pública

(a) Los organismos gubernamentales deben desarrollar sus aplicaciones en base a código fuente y licencias abiertas.

[16] Los módulos son funciones extras que extienden la funcionalidad de una plataforma; estos pueden brindar funcionalidades sin depender de una plataforma.

(b) Los organismos que contraten servicios de desarrollo de aplicaciones, deben exigir a los desarrolladores propiedad exclusiva de las aplicaciones y códigos fuentes, y estos deben colocarse en el Repositorio del Software Gubernamental del Estado; cumpliendo con todo lo especificado en la NORTIC A3, sobre publicación de datos abiertos en el gobierno dominicano.

SECCIÓN 5.04.

Recomendaciones sobre la administración y desarrollo del software

Para la usabilidad del software gubernamental

- Permitir que el usuario pueda cambiar el tamaño de las ventanas así como su posición.

Para el uso de software libre en la administración pública

- Se sugiere a los organismos gubernamentales que hagan uso de software desarrollado en base a estándares y licencias abiertas en la plataforma TIC.

CAPÍTULO VI

SEGURIDAD DE LAS TIC

En este capítulo se indican las directrices para establecer la correcta administración de la información y el debido tratamiento de la misma, aplicando controles de seguridad que salvaguarden los activos de información de los organismos gubernamentales, y de igual manera se establecen las directrices para la correcta implementación de la continuidad, tanto para la prestación de servicios al ciudadano como de las operaciones dentro de los organismos.

SECCIÓN 6.01.

Administración de la información

La gestión de la información se basa en la protección del activo de información de los organismos gubernamentales, de manera que las directrices en esta sección están dirigidas al fortalecimiento de la confidencialidad, integridad y disponibilidad de la información, así como a la protección de la infraestructura que alberga los datos.

Sub-sección 6.01.1. Sistema para la administración de la seguridad de la información

(a) Los organismos gubernamentales deben implementar un Sistema para la Administración de la Seguridad de la Información (SASI).

(i) El SASI debe contemplar las siguientes informaciones dentro de su elaboración:

- **Documento de definición y alcance del SASI**: Este debe establecer el alcance, objetivos y las responsabilidades del

SASI.

- **Manual de procedimientos**: Este debe establecer los documentos operativos que aseguran el debido funcionamiento del SASI.
- **Manual de instrucciones, lista de tareas y formularios**: Estos documentos deben establecer las actividades del nivel operativo para la correcta realización de las actividades del SASI.
- **Registros**: Estos documentos deben mantener evidencias de las acciones realizadas, según el SASI.

La implementación de un SASI debe asegurar:

- *Que los activos de información estén dentro de un marco de seguridad.*
- *Que las informaciones estén disponibles.*
- *Que los datos estén íntegros.*
- *Que la infraestructura tecnológica que alberga el activo de información esté segura.*
- *Que estén establecidas las medidas y controles necesarios para mitigar riesgos que expongan los activos de información.*

Para ver las fases de implementación del SASI, ver anexo I. Implementación del Sistema para la Administración de la Seguridad de la Información (SASI).

(ii) El SASI debe estar orientado a procesos, y el mismo debe tener la estructura de entradas, procesos y salidas como se muestra en el **anexo J. Procesos para la implementación de un SASI**:

a) El SASI debe contemplar las siguientes actividades para la elaboración e implementación del sistema:

i) Implicación de la Alta Gerencia en el proceso de elaboración.

ii) Definición del alcance del SASI y políticas de seguridad.

iii) Identificación de amenazas[1], vulnerabilidades[2] e impactos.

iv) Definición y selección de controles para el tratamiento de riesgos.

v) Aprobación por parte de la Alta Gerencia del riesgo residual[3].

[1] Es una posible causa de riesgo o perjuicio hacia una persona o algo.
[2] Hace referencia a la incapacidad de defensa frente a una amenaza.
[3] Hace referencia al riesgo que queda luego de haber tomado todas las medidas preventivas de reducción de

vi) Elaboración del documento de declaración de aplicabilidad[4].

vii) Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo del SASI.

viii) Definición de los indicadores para la medición de la efectividad de los controles.

ix) Formación y concienciación, en lo relativo a seguridad de la información, a todo el personal del organismo gubernamental.

x) Monitoreo y registro de todas las incidencias.

xi) Monitoreo del SASI y mejora continua.

xii) Evaluación periódica de los riesgos, revisión de los niveles de riesgos residuales identificados para el SASI, así como su alcance.

xiii) Mejora continua del SASI.

b) Los organismos gubernamentales deben hacer una revisión del SASI una (1) vez al año.

Sub-sección 6.01.2. Responsabilidad del empleado público

(a) Los empleados de los organismos gubernamentales deben cumplir con las siguientes responsabilidades:

(i) El empleado público debe velar porque otras personas no accedan a su estación de trabajo.

(ii) El empleado público no debe dejar su estación de trabajo desatendida sin antes bloquearla. Ver **directriz 6.03.3.h**.

riesgos.

[4] Hace referencia al documento que establece que controles se aplicaran al organismo gubernamental en la implementación del SASI.

(iii) El empleado público debe velar por la integridad de sus equipos asignados y reportar al departamento de TIC cualquier irregularidad con los mismos.

(iv) El empleado público no debe divulgar las credenciales que utiliza dentro del organismo gubernamental.

(v) El empleado público no debe divulgar información confidencial a otro personal no autorizado para circular con dicha información.

(b) El organismo gubernamental debe asegurar que cada uno de los empleados tenga total conocimiento de las directrices establecidas en esta sección.

SECCIÓN 6.02.

Tratamiento seguro de la información

Esta sección indica las directrices necesarias para lograr el correcto tratamiento de la información basada en políticas para la administración del activo de información, su correcto almacenamiento dependiendo el tipo de información y los procedimientos que deben ejecutarse cuando exista inconvenientes con el activo de información.

Sub-sección 6.02.1. Administración de la información

(a) Toda información de los organismos gubernamentales debe estar debidamente categorizada dentro de los parámetros siguientes:

- **Información pública**: Esta información debe estar al alcance, tanto de los empleados del organismo gubernamental como del público externo.
- **Información valiosa**: Esta información se utiliza para las operaciones del organismo gubernamental y debe estar solo al alcance de los sus empleados.
- **Información sensitiva**: Esta información debe estar solo al alcance de personas autorizadas. Esta puede afectar un personal o departamento dentro del organismo gubernamental.

- **Información confidencial**: Esta información debe estar permitida para un personal autorizado. Este personal debe estar designado por la máxima autoridad del organismo gubernamental o áreas designadas para otorgar dichos permisos. Esta puede afectar los intereses del organismo gubernamental.

(b) Los organismos gubernamentales deben tener un sitio de almacenamiento[5] especial para las informaciones sensitivas o confidenciales (en lo adelante, informaciones clasificadas).

(i) El sitio de almacenamiento debe disponer de una ruta, la cual pueda ser accedida única y exclusivamente por el personal autorizado.

(c) Los medios de almacenamiento que albergan información clasificada deben estar cifrados.

(d) Los organismos gubernamentales no deben permitir la divulgación ni replicación de informaciones clasificadas a terceros o personas no autorizadas, ya sea por vía electrónica o física.

(e) Los organismos gubernamentales deben tener los medios adecuados para poner a disposición su información pública y valiosa.

(i) Los medios mínimos requeridos son:

a) **Portal web**: Para informaciones públicas dirigidas al ciudadano sobre el organismo gubernamental. Ver **sub-sección 7.04.1 Medios web**.

b) **Intranet**: Para información exclusiva de los empleados del organismo gubernamental. Ver **Sección 7.02 Intranet**.

c) **Correo electrónico**: Para informaciones con carácter importante o urgente a los empleados del organismo. Ver **sub-sección 7.04.3 Correo institucional**.

(f) Las áreas o departamentos que manipulen información clasificada, deben tener independencia de recursos como impresoras, escáner, trituradoras de papel y archiveros.

[5] Hace referencia a un lugar específico dentro de un medio de almacenamiento. Esto puede ser una carpeta determinada dentro de un repositorio de documentos o carpetas.

(g) Toda información clasificada debe tener una frecuencia de respaldo superior a las informaciones no clasificadas.

Sub-sección 6.02.2. Políticas para la administración de la información

(a) Los organismos gubernamentales deben tener políticas definidas para la conservación de documentos o informaciones.

(i) Los organismos gubernamentales deben tener todas sus informaciones digitalizadas y almacenadas por categoría, según se establece en la Ver **sub-sección 6.02.1 Administración de la información**.

a) Toda información digitalizada debe perdurar en el tiempo y no debe ser eliminada.

b) Los organismos gubernamentales deben tener un sistema de respaldo para estas informaciones.

(ii) Los documentos alojados en el repositorio de archivos muertos[6] deben ser eliminados luego de un tiempo de conservación de cinco (5) años.

a) Para proceder con la eliminación de los archivos muertos, deben seguirse las siguientes directrices:

i) Debe llenarse un formulario de solicitud para la eliminación de los archivos muertos, el cual debe ser aprobado y autorizado por la unidad, departamento o personal dueño de la información.

ii) Este formulario debe tener los siguientes datos:

- Nombre y apellido de quien elimina.
- Fecha.
- Departamento dueño de la información.
- Nombre del documento que elimina.
- Firma del empleado que elimina.

[6] Son los documentos sin interés inmediato para el organismo gubernamental.

- Firma de autorización por parte de la máxima autoridad del departamento o entidad.

iii) Luego de la aprobación para la eliminación de los archivos muertos, estos deben ser digitalizados y categorizados como se establece en la **sub-sección 6.02.1 Administración de la información**.

(iii) Los organismos gubernamentales deben tener políticas para la conservación y eliminación de documentos físicos (ver **directriz 6.02.2.a)**. Las informaciones que tengan que ser eliminadas, deben ser digitalizadas y categorizadas debidamente antes de su eliminación.

a) La memoria institucional y las noticias de los organismos son consideradas informaciones históricas y esta debe permanecer en el tiempo y no ser eliminadas.

b) Toda información física que no agregue valor estratégico para decisiones de la Alta Gerencia con una antigüedad de 10 años, debe ser eliminada.

c) Toda información clasificada que pierda su utilidad y tenga una antigüedad de 5 años debe ser eliminada.

d) Toda información de empleados no activos en los organismos gubernamentales por un periodo de antigüedad de 2 años, debe ser eliminada, incluyendo:

- Toda información de los empleados fallecidos.
- Toda información almacenada de un empleado por causa de renuncia.
- Toda información de un empleado inactivo por causa de cancelación.
- Toda información judicial, historial médico, historial de sanciones e historial de méritos de empleados no activos, también aplican para ser eliminadas.

Para ver una referencia de los documentos a borrar con su tiempo correspondiente, ver el anexo K. Referencia para eliminación de documentos por antigüedad.

e) Toda información de accidentes de trabajo de los empleados con más de 2 años de antigüedad debe ser eliminada, a partir de la fecha de prescindir del recurso.

f) Toda información de solicitud de empleo al organismo gubernamental con una antigüedad de 6 meses, debe ser eliminada.

g) Cualquier otra documentación no mencionada que no agregue valor con una antigüedad de 12 años, debe ser eliminada.

(iv) Para la correcta eliminación de los documentos físicos o digitales, Ver **sub-sección 6.02.6 Borrado seguro de la información**.

(b) Las informaciones sensitivas de los empleados deben tener el siguiente tratamiento:

(i) Informaciones personales como contactos, cuentas de banco, cédula, tarjetas de crédito, pasaportes, y demás, que sean administradas por el organismo gubernamental, no pueden ser divulgadas al público y deben estar a disponibilidad del empleado dueño de la información.

a) Debe agregarse una marca de agua a los documentos digitalizados para garantizar la integridad del mismo.

b) En caso de un personal, entidad o departamento del organismo gubernamental solicitar información sensitiva, el departamento que custodia la información debe ocultar las informaciones que no son necesarias suministrar al solicitante.

(ii) El organismo gubernamental es responsable de la custodia de la información sensitiva, la cual debe estar en ambientes controlados de seguridad. Ver **directriz 6.02.1.b**.

(c) Las informaciones clasificadas que estén impresas deben ser retiradas inmediatamente de los medios utilizados para la impresión o escaneo.

Sub-sección 6.02.3. Almacenamiento de la información

(a) Los organismos gubernamentales deben definir políticas para los siguientes tipos de almacenamiento de la información:

(i) Almacenamiento local: Esto se lleva a cabo en las estaciones de trabajo de cada empleado del organismo gubernamental.

a) Debe estar definido qué clase de información estará almacenada, según su clasificación. Ver **directriz 6.02.1.a**.

i) Las informaciones de relevancia o alto impacto que residan en el almacenamiento local con un permiso temporal, deben ser eliminadas de forma segura al terminar con su utilización.

ii) En caso de que la información sea de relevancia o alto impacto, la información debe estar cifrada.

b) Debe estar definido en qué ubicación del árbol de directorios del sistema operativo estará residiendo la información.

(ii) Servidores de almacenamiento en red: Este es el almacenamiento común localizado en un servidor especial para los fines de almacenamiento.

a) Deben estar configurados para poner a disponibilidad del empleado cualquier documento o información del organismo gubernamental.

i) Toda información alojada en los servidores, debe estar regida por las políticas definidas en la Ver **sub-sección 6.02.2 Políticas para la administración de la información**.

b) Deben permitir al empleado disponer de carpetas personales para el desarrollo de sus funciones.

c) Deben permitir compartir los contenidos creados por el propio empleado.

d) Deben tener los accesos definidos para cada empleado.

e) Deben ser utilizados para el almacenamiento de contenido personal.

i) No deben contener archivos de audio o video sin relación con el organismo.

ii) No deben contener archivos de información personal del empleado.

iii) No deben contener software no licenciados. Ver **directriz 1.05.2.c**.

f) Los servidores de almacenamiento en red deben tener cuotas de almacenamiento por empleado.

(iii) Dispositivos de almacenamiento externo: Estos son dispositivos generalmente personales como Discos Compactos (CD, por sus siglas en inglés), Discos Versátiles Digitales (DVD, por sus siglas en inglés), memorias bus universal en serie (USB, por sus siglas en inglés), entre otros.

a) Los dispositivos de almacenamiento externo deben ser utilizados para transportar información del organismo gubernamental temporalmente.

i) La información debe ser borrada cuando deje de ser necesaria en este medio de almacenamiento. Ver **sub-sección 6.02.4 Respaldo de la información**.

b) Los dispositivos de almacenamiento externo no deben ser utilizados para transportar información clasificada.

i) Esta directriz no aplicará para personas con la autorización de circular con la información como ministros, directores generales, gerentes, directores de área, encargados o personas asignadas por los antes mencionados; dicho dispositivo de almacenamiento externo debe estar cifrado para el transporte de la información.

Sub-sección 6.02.4. Respaldo de la información

(a) Los organismos gubernamentales deben tener políticas para los sistemas de respaldo de la información.

(i) Los organismos gubernamentales deben definir qué informaciones serán incluidas en el respaldo.

a) Las informaciones vitales para el correcto funcionamiento de los organismos deben ser incluidas dentro del programa de respaldo.

(ii) Los organismos gubernamentales deben definir la frecuencia en la que se realizarán los respaldos.

(iii) Los organismos gubernamentales deben disponer de un espacio físico para el almacenamiento de los respaldos.

a) Solo el personal autorizado podrá acceder y manipular los respaldos.

(iv) Los organismos gubernamentales deben asegurar que los datos respaldados están íntegros y libres de errores para su posterior uso.

a) Debe probarse periódicamente y aleatoriamente los respaldos realizados para garantizar su integridad.

(v) Los organismos gubernamentales deben definir la vigencia que tendrá cada respaldo realizado.

Sub-sección 6.02.5. Recuperación de la información

(a) En caso de pérdida o destrucción de la información clasificada de manera accidental, los organismos deben:

(i) Proceder a utilizar los medios de respaldo establecidos anteriormente en la Ver **sub-sección 6.02.4 Respaldo de la información**.

(b) La unidad de Seguridad y Monitoreo debe tener un personal que asuma la función de recuperación de pérdida de datos.

Sub-sección 6.02.6. Borrado seguro de la información

(a) Los organismos gubernamentales deben tener los siguientes métodos disponibles para la eliminación de la información en caso de desechar medios de almacenamiento, avería permanente o borrado seguro de la información en un medio de almacenamiento no necesario.

- **Desmagnetización**: Este proceso de borrado consiste en exponer el medio de almacenamiento a un potente campo magnético, con el cual se eliminan los datos almacenados.
- **Destrucción física**: Este proceso consiste en inutilizar permanentemente el medio de almacenamiento, a través de diferentes métodos, como pueden ser:
  - Desintegración, pulverización, fusión o incineración: Estos métodos destruyen el medio de almacenamiento por completo, utilizando una trituradora de metal o proceso de incineración.
    - En caso de utilizar el método anterior, debe tomarse en cuenta las medidas de seguridad pertinentes para áreas no seguras[7], como lo especifica el **apartado 6.03.5.2 Controles de acceso a la infraestructura**.
  - Trituración: Ese método puede ser utilizado para la destrucción de los medios de almacenamiento de información flexible como el papel.
- **Sobreescritura o formato**: Este proceso consiste en sobrescribir la superficie que contiene la información con datos nuevos o también con un proceso de formateo de bajo nivel al dispositivo de almacenamiento.

(b) En caso del organismo gubernamental optar por utilizar el método de formateo para la eliminación de datos, debe utilizar el formateo de bajo nivel para asegurar el correcto borrado de la información.

(c) La unidad de Seguridad y Monitoreo debe tener un personal que asuma la función de borrado seguro de la información. Ver **directriz 2.01.1.b.v.a**.

[7] Hace referencia a los lugares no seguros dentro del organismo permitiéndole solo a el personal autorizado transitar por dichos lugares tomando precauciones para evitar lesiones.

(d) El organismo gubernamental debe tener registros de los borrados solicitados y autorizados por la entidad que los solicita.

(e) Debe tomarse en cuenta el **anexo L. Métodos de borrado adecuado en función del dispositivo** para el borrado seguro de la información, según el medio de almacenamiento y el método a utilizar.

SECCIÓN 6.03.

Administración de los controles de acceso

En esta sección se establecen las directrices que deben implementar los organismos gubernamentales para la correcta administración de los controles de acceso, por medio de políticas que apoyan los marcos de acceso a la información, acceso a la red del organismo gubernamental, acceso a los sistemas que soportan las operaciones del organismo, y las políticas para la regulación de los accesos de los usuarios.

Sub-sección 6.03.1. Políticas de acceso a la información

(a) Los organismos gubernamentales deben definir categorías de protección para la información.

(i) Estas informaciones deben estar categorizadas como lo establece la **directriz 6.02.1.a** y acorde a las directrices citadas en la sección anterior.

(ii) Los grupos de seguridad deben estar definidos como se establece a continuación:

- **Categoría 1**: Es información de poca protección, ya que esta es información pública.
- **Categoría 2**: Es información de carácter personal y privada de los empleados y funcionarios del organismo gubernamental.
  - Información valiosa.
  - Información sensitiva.

- **Categoría 3**: Es información de alto interés organizacional y estratégico; información sustancial y de acceso exclusivo a un personal autorizado.
    - Información confidencial.

(b) Los organismos gubernamentales deben elaborar y establecer un Contrato de Confidencialidad con sus empleados sobre el uso de las informaciones.

(i) El contrato de confidencialidad debe contemplar los siguientes elementos:

- **Consideraciones**: Contiene información relacionada al contrato mismo e información sobre el organismo.
- **Cláusulas**: Contiene las especificaciones del contrato y sus condiciones; esto debe contemplar las definiciones, excepciones, sanciones, plazos y demás.

Sub-sección 6.03.2. Control de acceso en la red

(a) Los organismos gubernamentales deben tener políticas para el uso de los servicios y recursos de la red.

(i) Dentro de los servicios y recursos a tomar en cuenta deben estar:

a) Internet:

i) Este servicio debe tener protección por cortafuegos e intermediario (haciendo referencia a proxy).

ii) Este servicio debe tener filtro de tráfico por categoría.

- Los sitios web con contenido ilícito deben estar bloqueados.
- Los sitios web de juegos en línea deben estar bloqueados.
- Los sitios web de apuestas en línea o actividades ilegales deben estar bloqueados.

- Los sitios web con contenido pornográfico deben estar bloqueados.

b) Intranet:

i) Este servicio debe estar a la disposición del empleado por medio de autentificación.

ii) Este servicio debe ser para uso exclusivo de los empleados del organismo.

c) Impresora:

i) Este recurso debe ser utilizado exclusivamente para impresiones relativas al organismo gubernamental.

ii) Los empleados no deben hacer uso personal de este recurso.

iii) Los documentos impresos deben ser retirados de inmediato por el dueño del documento impreso.

d) Escáner:

i) Los documentos escaneados deben ser retirados de inmediato por el empleado dueño del documento escaneado.

ii) Para el correcto procedimiento de escaneo de documentos, deben seguirse las pautas establecidas en la **sub-sección 7.01.1 Preparación de documentos**.

e) Correo electrónico:

i) Este servicio no debe ser usado para enviar correos masivos.

ii) El correo es para el uso exclusivo de temas pertinentes al organismo gubernamental.

iii) Para la correcta implementación del correo electrónico de los organismos

Para la categorización de usuarios, tomar como referencia el anexo M. Categorías de Usuarios.

gubernamentales, deben seguirse las pautas establecidas en la **sub-sección 7.04.3 Correo institucional**.

f) Servidor de archivos y almacenamiento:

i) Todas las directrices establecidas en la **sub-sección 6.02.3 Almacenamiento de la información** aplican para este mandato.

(b) Los organismos gubernamentales deben tener políticas de autenticación para conexiones externas a los servicios internos del organismo. Ver **sub-sección 4.01.2. Administración de la red privada y la red de área local inalámbrica**.

(c) Cada equipo dentro de la red de los organismos gubernamentales debe estar registrado dentro del inventario de los departamentos de TIC. Ver **sub-sección 2.04.3. Control de inventario**.

(d) El departamento de TIC debe controlar la configuración, y acceso físico o lógico, tanto interno como externo al organismo, a los puertos de diagnóstico de la infraestructura de TIC del organismo.

(e) El departamento de TIC debe tener controles establecidos de enrutamiento de las redes, para asegurar que las conexiones de las aplicaciones y servicios en la red del organismo gubernamental no incumplan las políticas de seguridad.

Sub-sección 6.03.3. Control de acceso al sistema operativo

(a) Las conexiones remotas a las estaciones de trabajo o servidores deben:

(i) Tener un cifrado mínimo de 128 bits.

(ii) Tener un tiempo de bloqueo de la estación de trabajo o servidores tras treinta (30) minutos de inactividad.

(iii) Tener un tiempo de desconexión de acceso a la estación de trabajo o servidores tras treinta (30) minutos de inactividad.

(iv) Este servicio solo debe estar disponible para el personal autorizado por el departamento de TIC.

(v) Todos los servidores deben disponer de conexión segura por medio de SSH.

(vi) Las conexiones remotas para transferencia de archivos deben ser por medio del Protocolo Seguro de Transferencia de Archivos (SFTP, por sus siglas en inglés).

(b) Las estaciones de trabajo que establezcan conexiones a servidores deben estar protegidas por antivirus.

(c) Las conexiones fuera de los organismos gubernamentales a servicios críticos en servidores deben ser por medio de una VPN, seguida por autentificación en el servidor. Ver **directriz 4.01.2.a**.

(d) Las conexiones dentro de los organismos gubernamentales a servicios críticos en servidores deben ser por medio de autentificación en el servidor que aloja los servicios.

(e) Los departamentos de TIC deben tener un sistema de monitoreo para evitar que las medidas de seguridad sean violadas por el empleado.

(f) Solo el personal técnico del departamento de TIC, o a quién este autorice, tendrá permisos a conexiones de terminales de trabajo o servidores.

(g) Todos los usuarios deben estar registrados en la base de datos del departamento de TIC para poder tener acceso a las estaciones de trabajo.

(i) Los departamentos de TIC deben asignar permisos para autentificación en las estaciones de trabajo y permisos para los servicios que estén disponibles en la red.

(h) Todas las estaciones de trabajo de los organismos gubernamentales deben estar protegidas por contraseña que cumplan las siguientes características:

(i) Las contraseñas deben tener un mínimo de ocho (8) caracteres.

(ii) Las contraseñas deben tener al menos una letra mayúscula.

(iii) Las contraseñas deben tener letras minúsculas.

(iv) Las contraseñas deben tener al menos un número.

(v) Las contraseñas deben ser renovadas cada noventa (90) días.

(vi) Las contraseñas personales no deben ser compartidas para no comprometer información sensible que resida en las estaciones de trabajo.

(vii) Las contraseñas definidas por el empleado no deben ser comunes.

(i) En caso de que el empleado tenga inconvenientes para acceder a su estación de trabajo, este debe solicitar soporte al departamento de TIC y bajo ningún término tratar de acceder por mecanismos de fuerza bruta[8].

Sub-sección 6.03.4. Gestión de acceso de usuario

(a) Los organismos gubernamentales deben tener procedimientos establecidos para la gestión de accesos de sus empleados, estos procedimientos deben contemplar:

(i) Accesos de entrada y salida al organismo gubernamental.

a) El sistema de acceso al organismo gubernamental debe cumplir las directrices establecidas en el **apartado 6.03.5.2. Controles de acceso a la infraestructura**.

(ii) Controles de accesos a la información del organismo gubernamental.

a) Estos controles deben contemplar las directrices establecidas en la **sub-sección 6.02.1 Administración de la información**.

(iii) Controles de accesos a estaciones de trabajo.

a) Estos controles deben tomar en cuenta las directrices establecidas en la **directriz 6.03.5.1.b**.

(iv) Controles de accesos a áreas restringidas.

(v) Controles de accesos a áreas de servidores.

[8] Hace referencia al método de recuperar una contraseña probando todas las combinaciones posibles hasta encontrar el acceso.

(vi) Controles de accesos a software del organismo gubernamental.

(b) Los organismos gubernamentales deben hacer una revisión de los accesos de los usuarios anualmente. Esta revisión debe estar documentada.

(c) Los organismos gubernamentales deben hacer una revisión, modificación o eliminación de los accesos de los usuarios al momento en que estos:

- Sean cancelados.
- Sean promovidos.
- Sean degradados.
- Sean transferidos a diferentes localidades.
- En caso de fallecimiento.

(d) La unidad de Seguridad y Monitoreo debe tener un personal que asuma la función de la administración de accesos de los empleados. Ver **directriz 2.01.1.b.v.b**.

Sub-sección 6.03.5. Políticas de gestión de activos físicos

En esta sección se indican las políticas para la correcta implementación sobre controles de entrada y salida de mobiliario y materiales diversos en los organismos gubernamentales, así como las pautas para regular los accesos a las localidades de los organismos estableciendo un marco de seguridad.

Apartado 6.03.5.1. Controles de hardware, mobiliario y materiales diversos

(a) Todos los activos físicos de los departamentos de TIC deben tener un responsable de los mismos.

(b) Los organismos gubernamentales deben tener procedimientos y políticas para los activos físicos que estarán fuera del local. Estas directrices no aplican para empleados con activos portátiles asignados como móviles, computadoras, tabletas y trasmisores-receptores (también conocidos como *Walkie-Talkie*).

(i) Los procedimientos deben ser:

a) El empleado debe llenar una solicitud para los fines, especificando la razón, cantidad de equipos, seriales o códigos de identificación de los equipos y periodo por el cual necesita el activo fuera de la locación.

b) La solicitud debe ser aprobada por el gerente del área y archivada en el registro del departamento de TIC.

c) La solicitud debe ser entregada en la recepción al personal de seguridad, este verificará las especificaciones del permiso con el activo para asegurar que sea la misma cantidad y los seriales o códigos de identificación especificados.

i) El personal de seguridad debe firmar y retener el documento para archivarlo.

ii) El personal de seguridad debe entregar una copia del documento impreso al empleado.

d) Al momento del empleado retornar con el activo, se buscará el documento archivado para ingresar su fecha y día de ingreso, seguido por la firma del personal de seguridad.

e) El activo físico debe ser devuelto al área pertinente y el documento debe ser entregado a la autoridad que inicialmente autorizó la salida del mismo.

(ii) Políticas para la salida y entrada de los activos físicos:

a) Solo el personal autorizado puede sacar un activo físico del organismo gubernamental.

b) El departamento de TIC debe establecer una fecha límite para los activos que sean solicitados fuera del organismo gubernamental.

c) Los activos deben ser entregados en las mismas condiciones en las que fueron retirados del organismo gubernamental.

d) El departamento de TIC debe asegurar que los datos e informaciones que residirán en el activo físico estarán seguros

por medio de políticas y controles establecidos para dichos casos.

(c) Para los empleados con activos físicos asignados, estos deben estar en el inventario del departamento de TIC. El estado físico de los mismos debe estar documentado.

(i) El empleado debe asumir cualquier responsabilidad del activo físico en caso de pérdida o daño del activo.

(ii) El empleado debe mantener el activo físico en perfecto estado y entregar el mismo en las condiciones como lo recibió.

(d) Los organismos gubernamentales deben tener políticas para la reutilización o eliminación de equipos.

(i) Para la aplicación de estos mandatos debe seguirse las directrices establecidas en la **sub-sección 6.02.6 Borrado seguro de la información**.

(ii) Las estaciones de trabajo que sean traspasadas o reasignadas a un nuevo empleado deben pasar por un proceso completo de eliminación de datos de los medios de almacenamiento que el activo físico contenga.

(iii) Para los equipos que estén en proceso de eliminación, sus medios de almacenamiento deben ser retirados y eliminados por separado.

Apartado 6.03.5.2. Controles de acceso a la infraestructura

(a) Los organismos gubernamentales deben contar con un proceso de control de acceso.

(i) Los organismos gubernamentales deben tener un procedimiento de registro de entradas y salidas.

a) El sistema debe contemplar los siguientes datos e informaciones:

- Fecha.
- Nombre del empleado.

- Hora de entrada.
- Firma a la hora de entrada.
- Hora de salida.
- Firma a la hora de salida.

(ii) Para la entrada de un visitante al organismo gubernamental, deben agotarse los pasos a continuación:

a) El visitante debe dejar una identificación en la recepción donde posteriormente se le entregará un carnet de identificación con el nivel de acceso permitido descrito en la **tabla No. 3. Niveles de acceso**.

b) El visitante debe ser acompañado por un personal del organismo gubernamental hasta su lugar de visita o reunión. Del mismo modo, el visitante debe ser acompañado a la salida de la locación, al momento de concluir su visita.

c) Al final de la visita del invitado, este debe entregar el carnet de identificación en la recepción donde se le entregaran sus credenciales.

(iii) La Alta Gerencia del organismo gubernamental debe asignar el departamento o área que administrará la información generada por el sistema.

(iv) Los organismos gubernamentales deben hacer su asignación de niveles de accesos en base a la siguiente **tabla No. 3. Niveles de acceso**:

Tabla No. 3. Niveles de acceso

NIVEL DE ACCESO	DESTINADO A	DESCRIPCIÓN
Nivel 1	Invitados	Acceso de entrada y salida al organismo
		Acceso a áreas básicas del organismo
		Acceso restringido al centro de datos

Nivel 2	Personal del organismo	Acceso restringido a áreas de seguridad específicas y clasificadas por el organismo
		Acceso de entrada y salida al organismo
		Acceso a áreas pertinentes al rol del personal
Nivel 3	Personal del organismo autorizado	Acceso restringido al centro de datos
		Acceso de entrada y salida al organismo
		Acceso a todas las áreas básicas del organismo
Nivel 4	Personal del departamento de TIC	Acceso abierto al centro de datos
		Acceso de entrada y salida al organismo
		Acceso a todas las áreas básicas de la organismo
		Acceso a áreas de seguridad específicas y clasificadas por el organismo

(b) Los organismos deben tener señalizadas las áreas seguras[9] y no seguras para el empleado.

(i) Las áreas no seguras deben estar igualmente señalizadas y solo el personal autorizado tendrá acceso a las mismas.

(ii) Dentro de las áreas no seguras debe incluirse:

- Áreas de carga.
- Áreas eléctricas.
- Áreas con productos derramados.
- Áreas con herramientas cortantes o filosas.
- Áreas con tránsito vehicular dentro del organismo.
- Áreas con desechos del organismo.
- Áreas con combustibles.

[9] Hace referencia a los lugares dentro del organismo seguros para que los empleados y visitantes permitiéndoles transitar sin correr ningún peligro por el organismo.

- Cualquier otra área determinada como no segura por el organismo.

SECCIÓN 6.04.

Plan de disponibilidad y continuidad

A continuación se estarán estableciendo las directrices pertinentes para la implementación y administración de la disponibilidad y continuidad de los servicios y operaciones de los organismos gubernamentales.

Sub-sección 6.04.1. Plan de disponibilidad

(a) Los organismos gubernamentales deben tener un plan de disponibilidad. Este debe tener las siguientes informaciones:

(i) La situación actual de disponibilidad de los servicios TIC. Información que debe ser actualizada periódicamente.

(ii) Herramientas para la monitorización de la disponibilidad.

(iii) Métodos y técnicas de análisis a utilizar.

(iv) Definiciones relevantes y precisas de las métricas a utilizar.

(v) Planes de mejora de la disponibilidad.

(vi) Expectativas futuras de disponibilidad.

Sub-sección 6.04.2. Plan de continuidad del organismo

(a) Los organismos gubernamentales deben tener un Comité de Continuidad (CONTI).

(b) El CONTI debe estar compuesto por la Alta Gerencia, la máxima autoridad del departamento TIC y áreas claves del organismo gubernamental para la prestación de servicios.

(c) Los organismos gubernamentales deben tener un plan de continuidad para asegurar la no interrupción de sus operaciones vitales y sus servicios al ciudadano o demás organismos.

(d) Los organismos gubernamentales deben realizar un Análisis de Impacto del Negocio (BIA, por sus siglas en inglés) y este debe ser de insumo para la implementación del plan de continuidad.

(i) La integración de la Alta Gerencia del organismo gubernamental en este proceso es fundamental para la correcta elaboración y aprobación del BIA.

(ii) En la elaboración de BIA debe tomarse en cuenta los siguientes procesos:

- Verificación del inventario de procesos.
- Identificación de impactos.
- Definición de tiempos y secuencia de recuperación.
- Identificación de interdependencias entre procesos.
- Identificación de los procesos críticos del negocio.
- Análisis de riesgo. Ver **directriz 6.04.2.e.i**.

(iii) En caso de que los organismos gubernamentales no tengan el recurso humano para la elaboración del BIA, debe contratar un consultor para los fines. Ver **directriz 3.02.1.c**.

(e) Los organismos gubernamentales deben tomar en cuenta lo siguiente para la elaboración del plan de continuidad:

(i) Análisis de riesgos, dentro de este proceso debe realizarse lo siguiente:

- Identificar los ambientes operativos que se pueden ver afectados en caso de un siniestro.
- Identificar los principales escenarios de falla y los recursos e infraestructuras críticas.
- Identificar oportunidades de mejora o exposiciones críticas a riesgos de falla.
- Identificar las políticas y mejores prácticas de seguridad existentes.

- Revisión de instalaciones físicas, centros de cómputo e infraestructuras tecnológicas en general.

(ii) Selección de la estrategia de continuidad, dentro de este proceso debe realizarse lo siguiente:

- Definir requerimientos mínimos para cada recurso.
- Identificar configuraciones alternativas de recursos.
- Determinar las redundancias de equipos y de comunicaciones.
- Analizar las diferentes posibilidades en procesamiento y en comunicaciones.
- Determinar las opciones estratégicas de procesamiento internas y externas.

(iii) Plan de recuperación ante desastres (DRP, por sus siglas en ingles), para la implementación del DRP debe tomarse como referencia lo establecido en la siguiente metodología:

- Análisis de impacto sobre los servicios de TIC.
- Evaluación de riesgos de la infraestructura de TIC, ver **sub-sección 6.04.3. Gestión de riesgos**.
- Desarrollo de estrategias para la recuperación.
- Definición de roles y responsabilidades.
- Pruebas del DRP.

El DRP debe tener un Tiempo de Recuperación Objetivo (RTO, por sus siglas en inglés) y un Punto Objetivo de Recuperación (RPO, por sus siglas en inglés) aceptables que no comprometan las operaciones vitales del organismo gubernamental.

(iv) Ejecución y Desarrollo del Plan, dentro de este proceso debe realizarse lo siguiente:

- Definir los planes de continuidad y restauración.
- Elaborar el manual del plan.

- Definir las condiciones que deben cumplirse para que el plan tenga éxito.

(v) Evaluación y Mantenimiento, dentro de este proceso debe realizarse lo siguiente:

- Desarrollar las tareas necesarias para garantizar la operatividad del plan como simulacros y otras actividades relacionadas.
- Concientizar sobre la importancia del plan a todos los empleados del organismo.
- Socializar el plan al CONTI y a todo el organismo.
- Designar un responsable del plan para su actualización y mantenimiento.

(f) Los organismos gubernamentales deben generar periódicamente informes sobre la ejecución y estado de su plan de continuidad.

(i) Los organismos gubernamentales deben tomar en cuenta lo siguiente para sus evaluaciones periódicas del plan de continuidad:

- Análisis sobre nuevos riesgos y los impactos de los mismos.
- Revisión del impacto económico asociado al plan de continuidad.
- Evaluación sobre los simulacros del plan de continuidad.
- Capacitación del personal del departamento de TIC para llevar a cabo el plan de continuidad.

(ii) Los organismos gubernamentales deben hacer una revisión de su plan de continuidad una (1) vez al año.

Sub-sección 6.04.3. Gestión de riesgos

(a) Los organismos gubernamentales deben tener un plan para la gestión de riesgos que trate de manera proactiva las amenazas que afecten la operación del organismo en caso de futuras situaciones.

(i) El plan de gestión de riesgos debe estar hecho a la medida del

organismo gubernamental.

(ii) El plan de gestión de riesgos debe formar parte de la toma de decisiones de la Alta Gerencia del organismo gubernamental.

(iii) El plan de gestión de riesgos debe estar alineado al plan estratégico del organismo gubernamental.

a) El plan de gestión de riesgos debe atender y dar prioridad a los objetivos estratégicos establecidos en el plan del organismo.

(iv) El plan de gestión de riesgos debe tomar en cuenta los recursos humanos dentro de su planificación.

(v) El plan de gestión de riesgos debe facilitar la mejora continua del organismo gubernamental.

(vi) El plan de gestión de riesgos debe ser lo suficientemente flexible al cambio, en caso de que sea requerido por la Alta Gerencia del organismo gubernamental.

(b) Los organismos gubernamentales deben tomar en cuenta la siguiente estructura para la elaboración del plan de gestión de riesgo:

- Diseño de los procesos y flujos de soporte del plan de gestión de riesgos.
- Implantación de la gestión del riesgo.
- Seguimiento y revisión del plan de gestión de riesgos.
- Mejora continua del plan de gestión de riesgos.

(c) El plan de gestión de riesgos debe tomar en cuenta las siguientes fases con sus respectivas acciones para la elaboración del plan.

- **Análisis de probabilidad**:
  - Oportunidad de que se materialice la amenaza.
  - Tendencia de las probabilidades.
- **Análisis de consecuencias**:

- Impacto económico, material o humano.
- Análisis del entorno de las consecuencias (visión holística).

- **Valor del riesgo**:
  - Costo económico al asumir un riesgo.
- **Creación de defensas**:
  - Plan de acción preventiva para mitigar los riesgos.
- **Investigación de amenazas**:
  - Amenazas a los procesos.
  - Fallas activas y condiciones actuales.
  - Causa raíz.

Para la determinación del riesgo debe usarse la fórmula riesgo (R) = impacto (I) x probabilidad (P), siendo R = I x P donde:
Impacto: Indica qué tan crítico es el activo o servicio a tomar en cuenta y qué tan grave es la vulnerabilidad encontrada.
Probabilidad: Indica la posibilidad de que pueda ocurrir una amenaza, así como la posibilidad de que esta afecte la disponibilidad del activo o servicio.
Los posibles valores, tanto del impacto como de la probabilidad en un orden del número 1 hasta el 4, siendo:

- *Uno (1) equivalente a un riesgo insignificante.*
- *Dos (2) equivalente a un riesgo bajo.*
- *Tres (3) equivalente a un riesgo medio.*
- *Cuatro (4) equivalente a un riesgo alto.*

Ver anexo N. Referencia para determinar el nivel del riesgo identificado.

(d) Deben tomarse en cuenta los diferentes tipos de análisis de riesgo los cuales se detallan en el **anexo O. Tipos de análisis de riesgo**.

(e) Los organismos gubernamentales deben tomar en cuenta las siguientes directrices para la elaboración de los riesgos identificados, tomando acciones dependiendo del impacto y la probabilidad del mismo.

(f) Los organismos gubernamentales tienen varias opciones frente a los riesgos encontrados, de los cuales deben escoger una de las citadas para cada riesgo identificado:

(i) **Aceptación del riesgo**: El organismo conoce el riesgo y sabe las consecuencias del mismo y decide asumirlos en caso de que este se materialice; ya sea porque tiene la capacidad de mitigarlo, o porque no tiene la capacidad de lidiar con el mismo por su magnitud.

(ii) **Transferencia del riesgo**: El organismo transfiere a otra entidad la responsabilidad de la mitigación del riesgo, por medio de la contratación de servicios o seguros de cobertura.

(iii) **Reducción de los riesgos a niveles aceptables**: El organismo reduce los impactos del riesgo, por medio de políticas y medidas.

(iv) **Evitar el riesgo**: El organismo elimina el riesgo, por medio de la reingeniería de los procesos o eliminando el factor que produce el riesgo sin afectar la actividad principal del organismo.

(g) Los organismos deben soportar el plan de gestión de riesgo con el BIA establecido en la **directriz 6.04.2.d**.

SECCIÓN 6.05.

Recomendaciones sobre seguridad de las TIC

Esta sección contiene todas las recomendaciones referentes al capítulo de Seguridad de las TIC.

Para el borrado seguro de la información:

- Cortar a la mitad los CD o DVD, en caso de prescindir de la información que resida en estos medios.

Para las políticas de control de acceso:

- Implementar un sistema de control de acceso que tenga las siguientes funcionalidades:

  - Registro de entrada y salida del personal.
  - Cancelación de accesos de entrada y salida con efecto inmediato.
  - Permitir accesos por medio de:
    - Huella dactilar.
    - Tarjeta codificada.
  - Permitir la impresión de reportes.

Para ver las ventajas y desventajas de los diferentes métodos de borrado de información, ver en anexo P. Comparativa de los métodos de borrado seguro.

- Tener cifrado de datos.
- Administrar áreas de acceso como se describe en la **directriz 6.03.5.2.b**.

- Que el Departamento de Recursos Humanos sea quien administre la información generada por el sistema.

Para el control de acceso en la red:

- Verificar que la autentificación de la Intranet esté ligada a la autentificación de la estación de trabajo.

Para el control de acceso al Sistema Operativo:

- Agregar a la contraseña caracteres especiales como los que se muestran a continuación: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; “ ‘ < > , . ? /.

CAPÍTULO VII

ADMINISTRACIÓN EFICIENTE

Con el objetivo de hacer más eficiente la administración pública mediante las TIC, se dan a conocer las directrices necesarias para alcanzar el mismo, adoptando medidas que permitan la reducción de los consumos y mejora de los servicios brindados por el organismo.

SECCIÓN 7.01.

Digitalización de documentos

En esta sección se establecen las directrices para la preparación, inspección, conservación y puesta a disposición de las imágenes digitales generadas de un documento físico.

Sub-sección 7.01.1. Preparación de documentos

(a) Toda entidad de intermediación financiera del Gobierno Dominicano debe regirse bajo el Instructivo sobre digitalización, truncamiento y compensación de cheques, elaborado por el Banco Central de la República Dominicana.

(b) Todo organismo que haya elaborado sus políticas para la digitalización de documentos deben estandarizar las mismas, según lo establecido en esta sección. Sin embargo, aquellos puntos o elementos particulares para cada organismo, y que no se haga mención en esta norma, pueden seguir como lo establece las políticas de digitalización propias de cada organismo.

(c) Debe verificarse que los documentos a digitalizar no contengan duplicados, borradores o algún otro documento que carezca de valor.

(i) En caso de haber documentos duplicados o que los organismos lo consideren carentes de valor informativo, debe enviarse el documento físico a un repositorio de archivos muertos preestablecido en cada organismo.

a) El repositorio de archivos muertos debe estar clasificado por cada una de las áreas que componen la estructura del organismo.

(ii) Los documentos guardados en el repositorio de archivos muertos deben tener un límite de tiempo para poder proceder a su eliminación, como se establece en la **directriz 6.02.2.a.ii.**

(d) Para los documentos con informaciones sensitivas, tales como cédulas, tarjetas de crédito, pasaportes y aquellos que los organismos consideren sensibles, debe cumplirse como mínimo las directrices establecidas en la **directriz 6.02.1.b.**

(e) Debe separarse en repositorios[1] diferentes los documentos de textos y los documentos gráficos cuando se proceda a digitalizar.

Sub-sección 7.01.2. Requerimientos técnicos de los documentos para la digitalización

(a) Para la digitalización de documentos de textos debe seguirse las directrices a continuación:

(i) Para aquellos documentos bien contrastados, debe realizarse una captura en blanco y negro de 300 puntos por pulgadas (ppp).

a) Estos documentos deben estar en Formato de Archivo de Imagen Etiquetado[2] (TIFF, por sus siglas en inglés) sin compresión[3].

b) En caso de utilizar compresión, esta debe ser sin pérdida de

[1] Es un sitio en la red donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.
[2] 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.
[3] Refiriéndose a los datos, es reducir el volumen de los mismos con el objetivo de ganar más espacio libre.

calidad.

(ii) Para aquellos documentos que estén mal contrastados, debe realizarse una captura en escala de grises de 300 ppp.

a) Los documentos de textos mal contrastados deben estar en formato TIFF sin compresión.

(b) Para los documentos gráficos debe seguirse las directrices a continuación:

(i) Cuando el documento sea de fotografías, debe realizarse una captura a color de 300 ppp.

a) Estos documentos deben estar en formato TIFF sin compresión o en el formato de Grupo Conjunto de Expertos en Fotografía[4] (JPEG, por sus siglas en inglés) con mínima compresión.

(ii) Los documentos de planos, que estén bien contrastados o en buena conservación, deben tener una captura en blanco y negro de 300 ppp.

a) Estos documentos deben estar en formato TIFF sin compresión o compresión sin pérdida de calidad de la imagen.

(iii) Los documentos de planos a color deben tener una captura de 300 ppp.

a) Estos documentos deben estar en formato TIFF sin compresión o JPEG mínima compresión.

Puede ver la tabla de requerimientos técnicos para digitalización de documentos en el **anexo Q. Requerimientos técnicos para digitalización de documentos.**

(c) Los documentos de planos mal contrastados o con mala conservación, debe tener una captura en escala de grises de 300 ppp.

(i) Estos documentos deben estar en formato TIFF sin compresión.

[4] Es un formato orientado a la captura de imágenes digitales de compresión con pérdida. Aunque su uso es muy común en la web, este no permite transparencia y se puede lograr un tamaño de imagen superior a los 65 mil pixeles, tanto de anchura como de altura.

(d) Para la consulta de los documentos digitalizados, tanto textos como gráficos, debe utilizarse en Formato de Documento Portátil[5] (PDF, por sus siglas en inglés).

(e) Debe utilizarse un dispositivo de captura de imágenes[6] que garantice la integridad de los documentos.

(i) Una vez digitalizadas las imágenes debe verificarse que:

- Estén correctamente alineadas.
- No tengan márgenes añadidos.
- Sean una representación fiel e integra del documento físico.
- Sean legibles.

(f) Debe crearse un repositorio seguro de almacenamiento para conservar los documentos después de su verificación.

SECCIÓN 7.02.

Intranet

En esta sección se establecen las directrices para la creación de la Intranet con una estructura homogénea y usable que permita al usuario localizar y visualizar las informaciones rápidamente.

(a) Para la correcta implementación de la Intranet todo organismo gubernamental, debe contar con una estructura de red interna que cumpla con los requerimientos de conexión establecidos en la **sección 4.01. Conectividad.**

(b) La Intranet debe contar con el siguiente mapa de sitio:

- Institución.
  - ¿Quiénes somos?
    - Historia.

[5] 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.

[6] Es un dispositivo que permite convertir un documento o imagen física en una imagen digital.

- Estructura orgánica.
- Despacho del [Título la máxima autoridad del organismo].
- Marco legal del organismo.
- Plan estratégico.

- Foro de discusión.
- Librería.
- Compartir documentos.
- Directorio de empleados.
- Marco legal del empleado.
- Términos de uso.
- Políticas de privacidad.

(c) La Intranet debe disponer de los siguientes módulos:

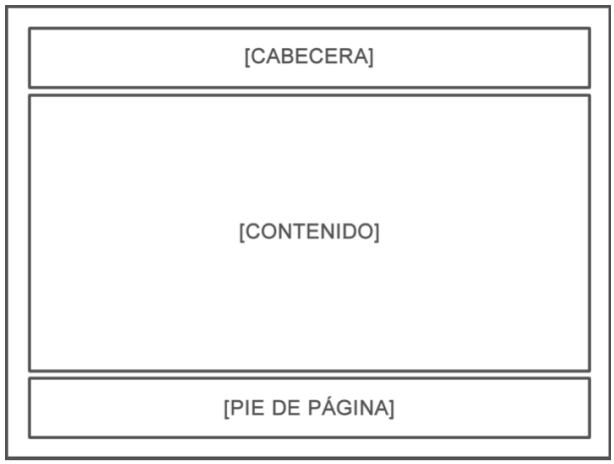
- Noticias.
- Tareas.
- Agenda:
  - Eventos.
  - Calendario.
- Mensajería electrónica.

Sub-sección 7.02.1. Disposición de elementos de la Intranet

(a) Toda Intranet debe cumplir con siguientes elementos generales:

(i) La estructura de la Intranet debe estar formada por tres divisiones: la cabecera, el panel central y el pie de página como se muestra en la **figura No. 1 Elementos generales de la Intranet.**

Figura No. 1. Elementos generales de la Intranet



(ii) La estructura de la Intranet debe diseñarse para una resolución de pantalla igual o superior a los 1024px. de anchura por 768px. de altura.

(iii) Debe tener una alineación al centro de la pantalla.

(iv) Cuando se utilice un menú desplegable, este debe presentar las opciones inmediatamente se pase el cursor por encima.

(v) Este tipo de menú debe tener un tiempo de presentación superior a los 50 milisegundos, al momento de que el cursor deje de estar por encima de alguno de sus elementos.

(vi) Debe indicarse gráficamente en el menú, la existencia de sub-menús de nivel I y de nivel II.

(b) La división de cabecera debe mostrarse de la siguiente manera:

(i) En la cabecera debe mostrarse solo 6 elementos, los cuales son:

- Fotografía del empleado.
- Detalles del empleado, donde se muestre el nombre del usuario, cargo que ocupa y el departamento al que pertenece.
- Logo o identidad del organismo.
- El escudo de la República Dominicana.
- La herramienta de búsqueda.
- "Editar perfil" del usuario.

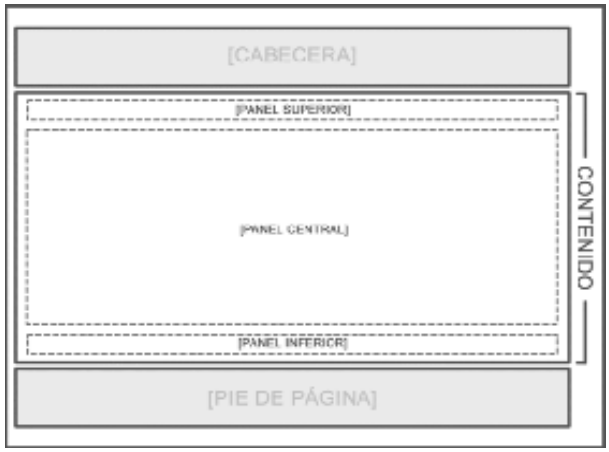
(ii) La cabecera debe diagramarse como lo muestra la **figura No. 2 Diagramación de la cabecera de la Intranet.**

Figura No. 2. Diagramación de la cabecera de la Intranet

(c) La división de contenido debe mostrarse de la siguiente manera:

(i) La división de contenido debe tener la suficiente flexibilidad para soportar tres paneles (panel superior, central e inferior) como muestra la **figura No. 3. Paneles de la división de contenido**.

Figura No. 3. Paneles de la división de contenido



(ii) El panel superior debe utilizarse para mostrar los siguientes elementos:

- Declaración del año, donde se define el objetivo o meta del Gobierno en el año en curso. Para el año 2014, será: **"Año de la Superación del Analfabetismo"**.
- Un menú principal horizontal.
- El rastro de navegación[7].
- Cualquier otro elemento que se considere de relevancia para el usuario.

(iii) El panel central debe mostrar los siguientes módulos:

- Tareas.
- Mensajes.

[7] Muestra la profundidad en la que estamos navegando en un portal, este comúnmente se encuentra en la parte superior donde esta fácilmente visible al usuario.

- Agenda.
- Noticias.
- Cualquier otro elemento que se considere de relevancia para el usuario.

(iv) El panel inferior debe utilizarse para mostrar cualquier elemento que se considere de relevancia para el usuario.

(v) Las secciones internas deben presentar los siguientes elementos:

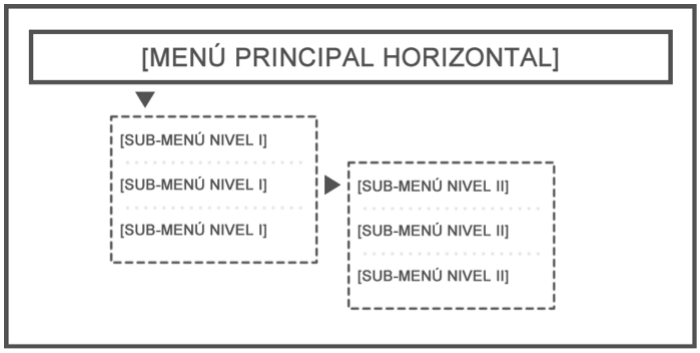
- La información de la sección.
- El rastro de navegación.
- Cualquier otro elemento que se considere de relevancia para el usuario.

(vi) Debe mostrarse en el menú principal las siguientes secciones:

- Inicio.
- ¿Quiénes somos?
  - Visión, misión y valores.
  - Organigrama.
  - Nuestro director.
  - Departamentos.
  - Plan estratégico.
  - Marco legal del organismo.
- Marco legal para el empleado.
- Foro.
- Librerías.
- Directorios de empleados.

(vii) El menú principal debe desplegarse como se muestra en la **figura No. 4. Niveles de profundidad de sub-menús.**

Figura No. 4. Niveles de profundidad de sub-menús



(viii) La estructura del menú principal debe presentarse en el panel superior y mostrar las secciones que componen cada opción del menú.

a) Solo debe mostrarse con un tipo de menú desplegable, los sub-menús desde el nivel I hasta el nivel II, de ser necesario.

b) El menú principal horizontal debe mantenerse igual en todas las secciones de la Intranet, es decir, tanto para la portada como para las secciones internas.

(d) La división del pie de página debe mostrar los siguientes elementos como lo muestra la **Figura No. 5. Diagramación de pie de página de la Intranet**:

- Nombre detallado del organismo y la sigla de ser necesario.
- Dirección física y contactos telefónicos del organismo.
- Términos de uso.
- Políticas de privacidad.
- Mapa de sitio.
- Año actual.

- Aviso de derecho de autor.

Figura No. 5. Diagramación de pie de página de la Intranet

Sub-sección 7.02.2. Estructura de contenido para la Intranet

(a) La Intranet debe poseer mínimamente las siguientes secciones obligatorias.

(b) Debe existir la sección "Inicio", la cual es la portada de la Intranet.

(c) Debe existir una sección "Institución", la cual contenga las siguientes sub-secciones:

(i) "¿Quiénes somos?", donde se exponga la definición, descripción y funciones del organismo, además de presentar la visión, misión y valores del mismo.

(ii) "Historia", donde se presente cronológicamente el origen y las razones de la creación del organismo, además de presentar los hechos, proyectos y programas más transcendentales que se han logrado.

(iii) "Estructura orgánica", donde se presente gráficamente el organigrama o esquema en el que se despliegue con claridad todos los departamentos, unidades o dependencias que componen el organismo.

a) Debe proveerse al usuario la posibilidad de descargar el documento.

(iv) Debe existir la sección "Despacho del [Título la máxima autoridad del organismo]", en la cual se presenta una semblanza o bosquejo biográfico de su persona.

(v) Debe existir la sección "Marco legal", presentando las leyes, decretos, resoluciones, reglamentos, normas, políticas, acuerdos y

convenios relacionados con el organismo.

a) Debe proveerse al usuario la posibilidad de descargar los documentos.

(vi) Debe existir una descripción del "Plan estratégico" con el listado completo de los objetivos, estrategias y tácticas que ejecutará el organismo en el plazo de tiempo determinado.

(d) Debe existir la sección "Marco legal para el empleado", indicando las leyes, decretos, resoluciones, reglamentos, normas, políticas, acuerdos y convenios relacionados con el empleado.

(e) Debe existir la sección "Librería", donde se le permita al usuario descargar cualquier documentación de interés al usuario.

(i) Esta documentación debe estar categorizada por área.

(f) Debe existir la sección "Términos de uso", donde se establece al usuario los términos de uso que regulan la Intranet.

(g) Debe existir la sección "Política de privacidad", donde se informa al usuario sobre los métodos de rastreo de información que se utilizan en la Intranet.

(h) Debe existir la sección "Mapa de sitio", donde se liste todas las secciones que componen la Intranet.

(i) Debe existir la sección "Foro", donde distintas personas puedan sostener una conversación en torno a un tema de interés común.

(j) Debe existir la sección "Compartir", donde el usuario pueda cargar documentos o archivos para que otros usuarios puedan utilizarlos.

(k) Debe existir la sección "Directorio de empleados", donde el usuario pueda obtener rápidamente las informaciones de contacto de otros empleados y este debe contener las siguientes informaciones:

- Nombre del empleado.
- Cargo.
- Departamento.

- Número telefónico y extensión.
- Correo electrónico.
- Cualquier otra información que se considere relevante.

(l) Debe existir un módulo "Noticias", el cual ha de presentar, ordenados cronológicamente, los hechos más novedosos del organismo o relacionados con su ámbito de acción o misión.

(i) Cada noticia debe tener un título, fecha, lugar e imágenes o videos relacionados a la misma.

(m) Debe existir un módulo "Agenda", donde el usuario pueda visualizar de forma rápida las reuniones, eventos, calendario, entre otras informaciones que el organismo considere relevante.

(n) Debe existir un módulo "Mensajería electrónica", el cual servirá al usuario como un buzón de los mensajes recibidos por otros usuarios.

(o) Debe existir un módulo "Tareas", donde el usuario pueda visualizar un listado de sus asignaciones o proyectos pendientes.

(p) Debe existir la sección "Perfil del usuario", donde se le permita al usuario modificar su cuenta.

(i) Esta sección debe contener los siguientes campos:

- Cambiar imagen.
- Modificar contactos:
  - Teléfono.
  - Celular.
  - Flota.
- Cualquier otro elemento que se considere de relevancia para el usuario.

SECCIÓN 7.03.

Tecnologías verdes

Para el uso sostenible e implementación de tecnología verde en el Estado Dominicano, se establecen directrices para reducir el consumo de la energía y sus emisiones de carbono asociados a una mala gestión del uso descontrolado de los equipos electrónicos.

(a) Todo organismo gubernamental debe formular políticas de tecnologías verdes y estas deben estar plasmadas en un documento visible para todo el personal. El documento debe ser difundido por los medios internos que el organismo considere pertinentes.

(b) Todo organismo gubernamental debe realizar un diagnóstico, para saber su estado con relación a las implementaciones de tecnología verde en la que se encuentra el organismo, y este debe abarcar los siguientes elementos:

- Estrategias de tecnología verdes realizadas.
- Metodologías de ahorro.
- Equipos electrónicos certificados bajo el programa de *Energy Star*.
- Metodología de reciclaje.
- Otros puntos que el organismo considere relevantes o hayan implementado.

(c) Todo organismo gubernamental debe clasificar los desechos tecnológicos en tóxicos y no tóxicos.

(i) Todo organismo gubernamental debe reciclar la basura por separado.

(ii) Todo organismo gubernamental debe recolectar las baterías gastadas o dañadas, con el fin de evitar ácidos o gases perjudiciales al medio ambiente.

(iii) Debe descartarse de forma adecuada las baterías gastadas o dañadas, enviando dichos componentes a los organismos correspondientes

o desecharlas en un ambiente controlado para su eliminación o reutilización.

(d) Las impresoras adquiridas por los organismos gubernamentales deben cumplir con las siguientes funcionalidades:

- Permitir la impresión doble cara.
- Permitir el control de impresiones por usuario.
- Permitir la generación de registro de impresiones por usuario o departamentos.
- Tener la funcionalidad de entrar en modo hibernación cuando no esté en servicio.

(e) La máxima autoridad del departamento de TIC debe ser el responsable del diseño y puesta en marcha de las estrategias de tecnologías verdes en los organismos gubernamentales, o quien la alta gerencia del organismo designe.

(i) La alta gerencia debe comprometerse en la implantación de tecnologías verdes en los organismos.

(ii) La máxima autoridad del departamento de TIC es la encarga de proporcionar una plataforma segura para la formulación e implementación de tecnologías verdes en el organismo.

(f) Las estrategias de tecnologías verdes del organismo deben ser revisadas y actualizadas una vez al año.

SECCIÓN 7.04.

Canales de acceso

En esta sección se establecen directrices para mejorar las vías de comunicación de los ciudadanos con el Estado Dominicano, a través de medios presenciales, telefónicos y web.

Sub-sección 7.04.1. Medios web

(a) Todos los organismos deben cumplir con las directrices establecidas en la NORTIC A2, orientado en los siguientes criterios:

- Usabilidad.
- Disposición de elementos.
- Contenido.
- Administración y seguridad.
- Accesibilidad.

(b) Para lograr una estructuración de contenido estándar basado en la normativa NORTIC A2 debe cumplirse las siguientes directrices:

(i) El portal web debe tener una estructura mínima de contenido establecida de la siguiente manera:

- Inicio.
- Sobre nosotros.
- ¿Quiénes somos?
  - Historia.
  - Organigrama.
  - Dependencias (Si aplica).
  - Despacho del [Título de la máxima autoridad del organismo].

- Marco legal.
- Memorias.
- Plan estratégico.

- Servicios.
- Proyectos.
- Transparencia.
- Noticias.
- Contactos.
- Mapa de sitio.
- Términos de uso.
- Política de privacidad.
- Preguntas más frecuentes.

(c) El portal móvil del organismo debe tener una estructura mínima de contenido establecida de la siguiente manera:

- Inicio.
- Sobre nosotros.
- Dependencias (Si aplica).
- Despacho del [Título de la máxima autoridad del organismo].
- Marco legal.
- Plan estratégico.
- Servicios.
- Proyectos.
- Transparencia.
- Contactos.

- Términos de uso.
- Política de privacidad.
- Preguntas más frecuentes.

(d) El sub-portal de transparencia del organismo debe tener una estructura de contenido cumpliendo con lo establecido por la DIGEIG de la siguiente manera:

- Inicio.
- Portal institucional.
- Base legal.
- Marco legal de transparencia.
- Organigrama.
- Derechos de los ciudadanos.
- Oficina de Libre Acceso a la Información (OAI).
- Plan estratégico.
- Publicaciones.
- Estadísticas.
- Servicios.
- Acceso al 311.
- Declaraciones juradas.
- Presupuesto.
- Recursos humanos.
    - Nómina.
    - Jubilaciones, pensiones y retiros.
    - Vacantes.

- Beneficiarios.
- Compras y contrataciones.
  - Lista de proveedores.
  - ¿Cómo ser proveedor?
  - Plan anual de compras.
  - Licitaciones públicas.
  - Licitaciones restringidas.
  - Sorteos sobre obras.
  - Comparaciones de precios.
  - Compras menores.
  - Casos de emergencia.
  - Estado de cuentas de suplidores.
- Proyectos y programas.
- Finanzas.
  - Balance general.
  - Ingresos y egresos.
  - Informes de auditorías.
  - Activos fijos.
  - Inventario en almacén.

Sub-sección 7.04.2. Disposición de elementos para el portal web

(a) La división de cabecera debe cumplir con los siguientes requerimientos:

(i) En la cabecera debe mostrarse solo 5 elementos, los cuales son:

- Logo o identidad del organismo.

- Nombre detallado del organismo y la sigla de ser necesario.
- El escudo y mención de la República Dominicana.
- La herramienta de búsqueda.
- Las herramientas de soporte de navegación, tales como: Inicio, mapa de sitio y contactos.

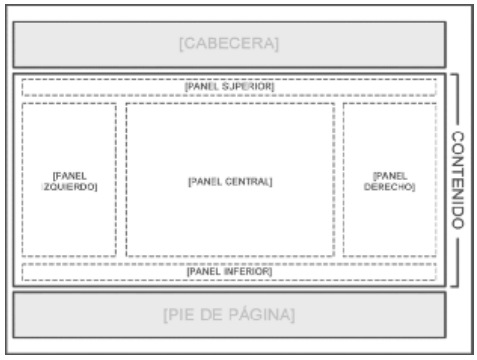
Para obtener una orientación sobre qué elementos insertar en estos paneles referirse al capítulo de disposición de elementos de la NORTIC A2.

(ii) La cabecera debe diagramarse como lo muestra la **figura No. 6. Diagramación de la cabecera:**

Figura No. 6. Diagramación de la cabecera

(b) La división de contenido debe tener la suficiente flexibilidad para soportar 5 paneles (panel superior, panel izquierdo, panel central, panel derecho y panel inferior) como muestra la **figura No. 7 Paneles de la división de contenido:**

Figura No. 7. Paneles de la división de contenido



(i) La portada debe presentar los siguientes elementos:

- Servicios que ofrece el organismo.
- Proyectos en ejecución.
- Noticias o información de alto impacto para el usuario sobre el organismo o relacionado al mismo.
- Cualquier otro elemento que se considere de relevancia para el usuario.

(ii) Las páginas web internas deben presentar los siguientes elementos:

- Información de la sección.
- El rastro de navegación.

(iii) Solo es permitido utilizar el menú horizontal y el menú vertical, como lo establece la NORTIC A2 en el **capítulo III. Disposición de Elementos**.

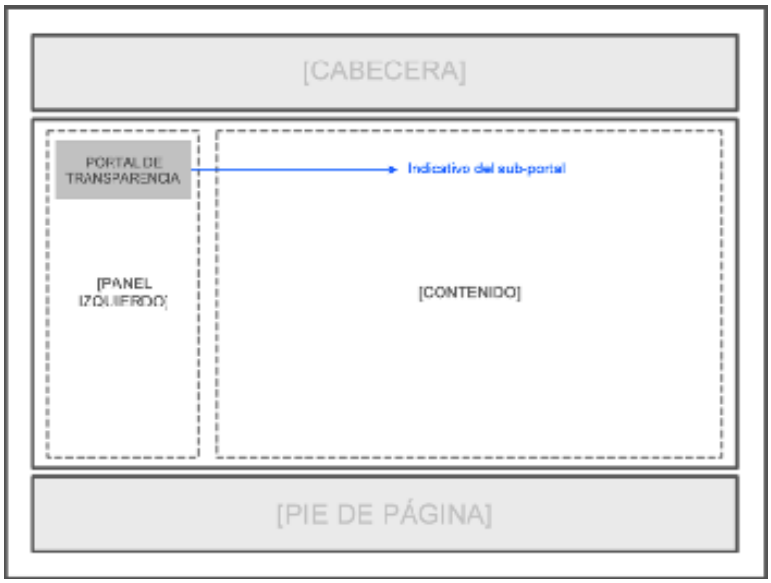
a) Cuando se utiliza el menú principal horizontal, este debe presentarse en el panel superior y mostrar las secciones que componen cada opción del menú.

b) Cuando se utiliza el menú principal vertical, este debe presentarse en el panel izquierdo y mostrar las secciones que componen cada opción del menú.

c) Los menús principales de los medios web deben mantenerse igual, tanto en la portada como en las secciones internas.

d) Para el sub-portal de transparencia, la estructura que debe utilizarse es como se muestra en la **figura No. 8 Estructura para el sub-portal de transparencia.**

Figura No. 8. Estructura para el sub-portal de transparencia



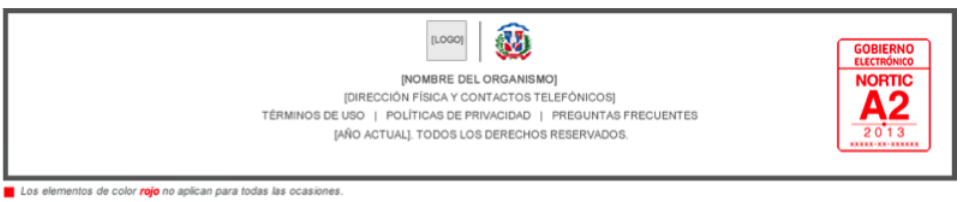
(c) La división de pie de página debe cumplir con los siguientes requerimientos:

(i) En el pie de página debe mostrarse los puntos citados a continuación y diagramados como se muestra en la **figura No. 9. Diagramación del pie de página**.

- Logo o identidad del organismo.
- Escudo de la República Dominicana.
- Nombre detallado del organismo y la sigla de ser necesario.
- Contactos del organismo:
  - Dirección.
  - Teléfono.
  - Fax.
- Términos de uso.

- Políticas de privacidad.
- Preguntas más frecuentes.
- Año actual.
- Correo electrónico.
- Aviso sobre los derechos de autor.

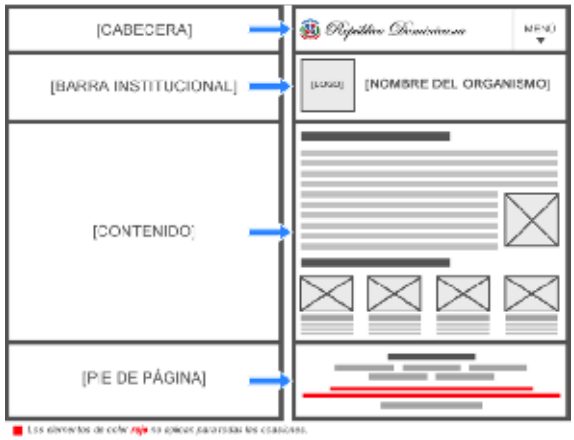
Figura No. 9. Diagramación del pie de página



(d) La versión móvil debe cumplir con los siguientes requerimientos:

(i) La estructura de la versión móvil para el portal del organismo estará conformada por cuatro grandes divisiones: la cabecera, la barra institucional, el contenido y el pie de página, como se muestra en la **figura No. 10. Diagramación de la versión móvil.**

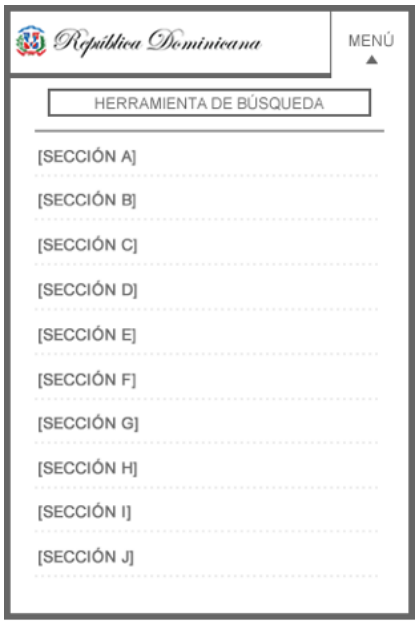
Figura No. 10. Diagramación de la versión móvil



(ii) En la cabecera solo debe mostrarse 2 elementos, los cuales son:

- El escudo y la mención de la República Dominicana.
- El menú desplegable, el cual debe contener la herramienta de búsqueda seguida de toda la estructura de páginas web para la versión móvil, como se muestra en la **figura No. 11. Herramienta de búsqueda y menú de la versión móvil**.

Figura No. 11. Herramienta de búsqueda y menú de la versión móvil



(iii) La disposición de elementos para la División de la barra institucional de la versión móvil debe tener:

- Logo o identidad del organismo.
- Nombre detallado del organismo y la sigla de ser necesario.

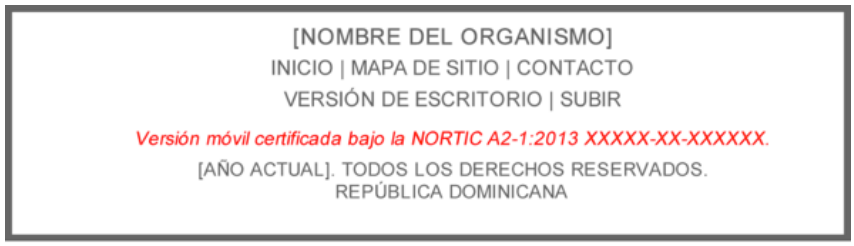
(iv) La división de contenido para la versión móvil debe cumplir los requerimientos de la NORTIC A2.

(v) La división del pie de página debe cumplir con los siguientes requerimientos:

a) En el pie de página debe mostrarse los puntos citados a continuación y diagramados como se muestra en la **figura No. 12. Diagramación y elementos del pie de página para la versión móvil.**

- Nombre detallado del organismo y la sigla de ser necesario.
- Las herramientas de soporte de navegación, tales como: Inicio, mapa de sitio y contactos.
- Indicaciones de accesibilidad.
- Año actual.
- Aviso de derecho de autor.
- Mención de la República Dominicana.

Figura No. 12. Diagramación y elementos del pie de página para la versión móvil



*Los elementos de color **rojo** no aplican para todas las ocasiones.*

Sub-sección 7.04.3. Correo institucional

(a) Todo correo perteneciente al organismo debe estar bajo la jerarquía .GOB, .MIL o .EDU, según la naturaleza del mismo.

(b) Todo organismo debe utilizar para el correo electrónico, únicamente nombres de dominios relacionados al nombre del organismo.

(c) Todo organismo debe contar con los siguientes correos electrónicos:

- oai@nombre-organismo.[gob/mil/edu].do, para comunicación directa con la oficina de libre acceso a la información pública.

- sugerencias@nombre-organismo.[gob/mil/edu].do, para quejas y sugerencias.
- contacto@nombre-organismo.[gob/mil/edu].do, para información adicional que el ciudadano necesite.

(d) Los protocolos de mensajería que deben utilizarse para el envío y recepción de correos deben ser:

- Protocolo para la Transferencia Simple de Correo Electrónico (SMTP, por sus siglas en inglés).
- Protocolo de Oficina de Correo 3 (POP3, por sus siglas en inglés).
- Protocolo de Mensaje de Acceso a Internet (IMAP, por sus siglas en inglés).

(e) La firma del empleado, dentro del correo electrónico, no debe contener imágenes.

Sub-sección 7.04.4. Canales de acceso presenciales

(a) Todo organismo debe tener una Oficina de Libre Acceso a la Información, como lo establece la ley 200-04.

Sub-sección 7.04.5. Canales de acceso de medios telefónicos

(a) Debe incluirse en el portal de los organismos un banner o enlace al sistema de Atención Ciudadana, Denuncias, Quejas y Reclamaciones (311), como lo establece el Decreto No. 694-09.

(b) Todo organismo que ofrezca servicios de cara al ciudadano debe tener presencia en el Centro de Contacto Gubernamental (*462), ofrecido por la OPTIC.

Apartado 7.04.5.1. Sistema de respuesta de voz interactiva

(a) Todo organismo gubernamental debe disponer de un IVR estandarizado bajo las directrices establecidas en esta sección.

(b) El IVR debe estar disponible las 24 horas del día.

(c) El IVR debe transferir a la operadora cuando el usuario durante un

tiempo razonable no marque ninguna opción.

(d) No deben existir extensiones inválidas.

(e) Cuando el usuario marque una extensión (o es transferido) y no se comunique, el IVR debe mencionarle las siguientes opciones:

- **No.1**: Grabar un mensaje de voz, donde se le permita al usuario dejar un mensaje grabado.
- **No.2**: Retornar al menú principal, donde se le permita al usuario volver al inicio del menú.

(f) El IVR debe tener la opción "Repetir opciones", donde se le permita al usuario escuchar nuevamente las opciones del menú.

(g) El IVR debe informar al usuario el horario laboral cuando este llame en horarios no laborables para el organismo.

(h) El mensaje de bienvenida del IVR debe mencionar:

- Saludo cordial.
- Nombre del organismo.

(i) Cuando el usuario ingrese datos, ya sean generales como personales, el IVR debe estar configurado para finalizar la función con la tecla almohadilla (#).

(j) El IVR debe indicar el número de la opción antes del nombre o descripción de la misma.

(k) El IVR debe estar configurado para soportar como mínimo 3 niveles de profundidad, los cuales se identificarán como primer nivel, segundo nivel y tercer nivel.

(i) Para el primer nivel deben reservarse las siguientes opciones:

- **No.0**: Operadora, donde el usuario se comunique rápidamente con un representante del organismo.
- Desde la opción No.1 hasta la No.6 son opciones abiertas para el organismo, donde podrá hacer eso de estas bajo su consideración.

- **No.7:** Extensiones de los departamentos, donde se le facilite al usuario todos los departamentos del organismo.
- **No.8:** Información del organismo gubernamental, donde debe reservarse las siguientes opciones para ofrecer las informaciones siguientes:
  - **No.1:** Horario laboral.
  - **No.2:** Localidades (Si aplica).
  - **No.3:** Servicios (Si aplica).
  - **No.4:** Canales de acceso, donde se le facilite al usuario otras vías por las que se puede comunicar con el organismo.
  - **No.7:** Retornar al menú anterior.
  - **No.9:** Repetir opciones.
  - **No.0:** Operadora.
  - Cualquier otra información que el organismo considere de relevancia para el usuario.
- **No.9:** Repetir opciones

(ii) Para el segundo nivel debe reservarse las opciones siguientes:

- **No.7:** Retornar al menú anterior.
- **No.9:** Repetir opciones.
- **No.0:** Operadora.

(iii) Para el tercer nivel debe reservarse las opciones siguientes:

- **No.7**: Retornar al menú anterior.
- **No.8:** Retornar al menú principal.
- **No.9:** Repetir opciones.
- **No.0:** Operadora.

(l) Las grabaciones de los menús o notificaciones emitidas por el IVR deben ser definidas por el organismo y debe cumplirse con los siguientes requerimientos:

(i) El tipo de voz utilizado para el IVR debe ser el mismo en todas las opciones.

(ii) No es permitido usar ningún tipo de aplicación que emule a la voz humana.

(iii) Debe permitirse al usuario interrumpir cualquiera de los mensajes del IVR, sin importar el nivel, para que este pueda acceder a la opción deseada del menú.

(iv) Debe procurarse ordenar las opciones, desde las más demandas hasta las menos.

(v) Debe informarse al usuario los días no laborables.

(vi) Debe informarse al usuario cuando su llamada pueda estar siendo grabada.

(m) El IVR debe generar reportes de cantidad de llamadas atendidas, opciones más usadas y tiempo de atención.

(n) El personal de administración de redes y comunicaciones, será el responsable de la generación de reportes y mantenimiento del IVR.

(o) El IVR debe informarle al usuario con anticipación sobre cualquier mantenimiento que se vaya a realizar a la plataforma del IVR que interrumpa el sistema.

(p) Debe informársele al usuario cualquier cambio de programación del menú del IVR.

(q) Todo organismo debe tener disponibilidad de las partes físicas utilizadas por el IVR, con el fin de minimizar el impacto en caso de fallas en el sistema y dar una solución rápida y efectiva.

(r) Todo organismo gubernamental debe contar con respaldos de información que permitan garantizar que no haya pérdidas de informaciones registradas. Ver **sub-sección 4.02.4. Respaldo de información**.

SECCIÓN 7.05.

Recomendaciones para la administración eficiente

Para la reducción del uso de papel se recomienda lo siguiente:

- Imprimir o fotocopiar a doble cara, con el fin de reducir el consumo de papel.
- Reducir el tamaño de los documentos al imprimir o fotocopiar.
- Elegir tamaño y fuentes pequeños.
- Corregir en pantalla antes de imprimir cualquier documento.
- Evitar copias e impresiones innecesarias.
- Reutilizar el papel usado por una cara.

Para la implementación de tecnologías verdes se recomienda lo siguiente:

- Implementar la virtualización[8] de servidores.
- Implementar la fórmula 3R (Reducir, Reutilizar y Reciclar.)
- Automatizar los procesos que considere necesarios.
- Realizar actividades sobre concientización del uso y apoyo de las estrategias implementadas de tecnologías verdes.
- Adquirir equipos electrónicos que estén certificados bajo el programa de *Energy Star*.
- Adquirir impresoras que el proveedor garantice la recolección de los cartuchos vacíos.

Para canales de acceso se recomienda:

- Tener presencia en las redes sociales[9] para aquellos organismos que ofrezcan servicios para el ciudadano.

[8] Es el uso de un software para crear máquinas virtuales (VM) para emular un computador físico.
[9] Son medios virtuales de comunicación que funcionan como una plataforma para que los usuarios puedan interactuar con otras personas que tienen intereses en común.

Para la Intranet se recomienda:

- Habilitar la función de chat[10], permitiéndole al usuario una herramienta para interactuar internamente con los demás integrantes del organismo.
- Habilitar las herramientas de encuestas, para obtener una aplicación que permita tener estadísticas que arroje las necesidades y la forma de pensar de los empleados de algún tema determinado por el organismo.

Para administración eficiente se recomienda:

- Para automatizar y tener una mayor eficiencia en los procesos de los organismos gubernamentales se recomienda implementar los siguientes software:
    - Sistemas de Planificación de Recursos Empresariales (ERP, por sus siglas en inglés) para optimización de los procesos de logística, distribución, inventario, envíos, facturas y contabilidad de la compañía de forma modular.
    - Mesa de ayuda, para gestionar y solucionar todas las posibles incidencias de manera integral en los organismo.
    - Sistema de Gestión de Relaciones con Clientes (CRM, por sus siglas en inglés) para organizar, automatizar y sincronizar las ventas, el marketing, atención al cliente y soporte técnico, entre otros.
    - Sistema de gestión de proyectos, para la toma de decisiones asociadas a todas las etapas del ciclo de un proyecto.

[10] Es una aplicación utilizada como canal de comunicación entre una persona y otra.

GLOSARIO DE TÉRMINOS

1000BASE-LX

Es un estándar para cables de fibra óptica que recorren una distancia menor a los 10 kilómetros.

1000BASE-SX

Es un estándar para cables de fibra óptica que recorren una distancia menor a los 550 kilómetros

1000BASE-T

Es un estándar para cables de par trenzado sin blindaje, donde se utilizan los cuatro pares del cableado simultáneamente para transmitir datos a 1,000 Mbps.

100BASE-T

Es estándar para cables de par trenzado sin blindaje, utilizado para recorrer distancias no mayor a 100 metros a una velocidad de transmisión de 100 Mbps.

Accesibilidad

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

Acceso WIFI Protegido (WPA)

Protocolo utilizado para la protección de las redes inalámbricas, adoptando la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.

Acceso WIFI Protegido 2 (WPA2)

Es un protocolo para la protección de las redes inalámbricas que utiliza la encriptación de datos.

Acoplamiento de Serie de Tecnología Avanzada (SATA)

Es una interfaz de datos para transferir información entre una placa base y dispositivos de almacenamiento.

Acoplamiento Serial SCSI (SAS)

Es una interfaz de datos para transferir información en serie, con una velocidad de trasmisión de 3.0 Gbit/s a 6.0 Gbit/s, con soporte para 65,535 dispositivos.

Actualización del software

Hace referencia a un consolidado de cambios para ser aplicados a un programa o plataforma para corregir errores y agregar funcionalidades.

Acuerdo de Nivel servicio (SLA)

Es un documento que plasma los acuerdos entre un proveedor de servicio y el cliente, en donde se estipulan los requisitos y parámetros que el proveedor se compromete a cumplir para mantener unos niveles de calidad de servicio.

Algoritmo de Resumen del Mensaje (MD5)

Es un algoritmo de cifrado que utiliza una codificación de 128 bits.

Amenaza

Es un evento que puede provocar un daño o perjuicio al organismo.

Ancho de banda

Es la cantidad de bits que se pueden transmitir en un tiempo determinado entre dos dispositivos digitales o en un sistema de transmisión.

ANSI/TIA/EIA-568-B.2-1

Es un estándar que define las características físicas de debe poseer un cable de par trenzado sin blindaje de categoría 6.

ANSI/TIA/EIA-568-B.3

Es un estándar de cable que describe los componentes físicos que debe poseer un cable de fibra óptica.

Antivirus

Es un programa desarrollado con el fin de proteger un computador o servidor contra virus informáticos.

Archivos muertos

Son los documentos físicos sin interés inmediato para el organismo gubernamental.

Área Central de Distribución (MDA)

Es donde se encuentra localizado el cableado cruzado principal.

Área de Distribución de Equipos (EDA)

Es un área dentro de un centro de datos donde se encuentran los dispositivos de almacenamiento y los servidores de aplicaciones del organismo.

Área de Distribución Horizontal (HDA)

Es el área donde se localiza el cableado cruzado horizontal.

Área de Zona de Distribución (ZDA)

Es un área donde se distribuye el cableado proveniente de la MDA.

Áreas no seguras

Hace referencia a los lugares no seguros dentro del organismo que solo el personal autorizado puede transitar, tomando precauciones para evitar lesiones.

Áreas seguras

Hace referencia a los lugares seguros dentro del organismo que los empleados y visitantes pueden transitar sin correr ningún peligro.

Auto-servicio bajo demanda

Referente al servicio en la nube computacional, es donde el usuario pueda gestionar los servicios en tiempo real, sin interacción directa con el proveedor del mismo.

Balanceo de cargas

Es un tipo de técnica utilizado en informática, en la cual las operaciones realizadas en un servidor son compartidas con otros servidores o recursos en la red, con el objetivo de evitar la saturación información.

Barra de herramientas

Es un elemento que contiene las funciones principales de una aplicación en forma de íconos o hipervínculos.

Base de Datos de Imagen con Multi-Resolución Constante (MRSID)

Es un estándar abierto para compresión de imágenes raster.

Base de Datos de la Gestión de Configuración (CMDB)

Es una base de datos central de todos los elementos de configuración de un sistema de información, ya sea hardware, software, documentación o cualquier otro elemento.

Bases de datos

Son un conjunto de datos almacenados de manera ordenada y que guardan relación entre ellos para su uso posterior.

bzip2

Es un programa de compresión con licencia BSD, en donde el porciento de compresión depende del tamaño del archivo.

Cable coaxial tipo 734

Es un cable de cobre de calibre 26, usado para recorrer distancias menores a los 225 pies.

Cable coaxial tipo 735

Es un cable de cobre de calibre 20, usado para recorrer distancias menores a los 450 pies.

Cableado Cruzado Horizontal (HC)

Es donde se aloja el cableado horizontal, el cual conecta el HDA con los equipos y armarios en el EDA.

Cableado Cruzado Principal (MC)

También conocido como backbone, es el cableado que conecta el MDA con el HDA.

Calidad de servicio (QoS)

Hace referencia al rendimiento de una red telefónica o de computadoras.

Capa 2

Referente al modelo OSI, es la capa que se encarga de la transmisión fiable de datos y direccionamiento del control de acceso a los medios.

Capa de Conexión Segura (SSL)

Es un protocolo de seguridad para conexiones de transmisión de información, el cual emplea autenticación y cifrado de datos.

Catálogo de información reutilizable

Conjunto de datos bajo los cuales se publica la información en formato abierto.

Catálogo de servicios

Es un listado de todos los servicios activos de un organismo. Este catálogo contiene todas las informaciones necesarias para el cliente sobre dichos servicios.

Centro de datos

Es un área donde se concentran y operan los equipos que conforman la infraestructura TIC que utilizan los organismos para administrar sus actividades y servicios.

Certificado digital

Es un documento digital que permite garantizar la identidad de una persona en la red, a través de una firma electrónica. Se utiliza como una forma segura de garantizar la autentificación, integridad y confidencialidad de la información.

Chat

Es una aplicación utilizada como canal de comunicación entre una persona y otra.

Cifrado de datos

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

Códec libre de compresión de audio sin pérdida (FLAC)

Es un formato abierto de audio que permite la compresión sin pérdida.

Código fuente

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

Componentes

Referido a la web, son aplicaciones que agregan funcionalidades específicas a un manejador de contenidos.

Compresión

Refiriéndose a los datos, es reducir el volumen de los mismos con el objetivo de ganar más espacio libre.

Computación en la nube

También llamada nube computacional, es una tecnología que permite la utilización de servicios de cómputos por medio de Internet.

Conector Cuadrado y el Conector Cuadrado Dúplex (SC)

Son conectores para cables de fibra óptica de forma cuadrada, su diseño permite el fácil manejo y la reducción de daños en la fibra óptica durante su instalación.

Conector de Canal de Fibra (FC)

Es un tipo de conector para cables de fibra óptica utilizados en ambientes con altas vibraciones.

Conector de Interfaz de Datos Distribuida por Fibra (FDDI)

Es un tipo de conector utilizado en redes de fibra óptica.

Conector Lucent (LC)

Es un conector para cable de fibra óptica utilizado para transmisiones de datos de alta densidad.

Conector Registrado 45 (RJ-45)

Es un conector utilizado en el cable UTP para establecer conexiones con los dispositivos de una red de datos.

Conexión cruzada horizontal

Es el cableado que conecta un IDF con los equipos de las diferentes áreas de trabajos en una LAN.

Conexión cruzada vertical

Es el cableado que conecta el/los IDF con el MDF en una LAN.

Conjunto Redundante de Discos Independientes (RAID)

Es un sistema de almacenamiento de datos que utiliza varios medios de almacenamiento para distribuir o replicar información.

Conmutadores

También conocido como switch, son dispositivos utilizados para conectar dos o más segmentos de redes.

Copias de respaldo

Son copias de los datos almacenados de un sistema, con el objetivo de tenerlos disponibles en caso de fallas.

Correo electrónico

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

Cortafuegos

También conocido como firewall, es un sistema que brinda protección contra la infiltración de intrusos a los recursos de una red, equipo o servicio.

Cuarto de Entrada (ER)

Es un área dentro del centro de datos en la cual se encuentran los cables, dispositivos o equipos provistos por el proveedor servicio.

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.

Datos abiertos

Son datos que están disponibles para cualquier persona sin restricciones, los cuales pueden ser utilizados, reutilizados y redistribuidos libremente.

Derecho de autor

Es el conjunto de leyes y principios que provee protección a los autores, artistas y demás creadores para sus creaciones.

Digitalizar

Hace referencia a la transformación de un documento físico a una imagen o medio digital para su visualización y manipulación en un dispositivo electrónico.

Dirección IP

Es una numeración que se le asigna de manera manual o automática a un dispositivo para identificarlo dentro de una red de datos.

Direcciones IP privadas

Son direcciones IP utilizadas únicamente para la comunicación dentro de una red datos, por lo que estas direcciones IP no son utilizadas para el servicio de Internet.

Direcciones IP públicas

Son un tipo de direcciones IP que se utilizan para establecer comunicación a través del internet, por lo que su uso no aplica a lo interno de una red de datos.

Dispositivo de captura de imágenes

Es un dispositivo que permite convertir un documento o imagen física en una imagen digital.

División de sub-redes

Es una técnica utilizada para la división de redes de datos en redes más pequeñas, bajo una misma mascara de red.

DjVu

Es un formato de archivo para guardar imágenes escaneadas.

Documento de declaración de aplicabilidad

Hace referencia al documento que establece cuáles controles se aplicarán al organismo gubernamental en la implementación del SASI.

Documento Office Open XML (DOCX)

Es un formato de archivo libre especial para documentos de texto con formato.

Documento primario

Hace referencia a documentos que han sido publicados o liberados desde su fuente origen, de manera que se pueda garantizar la integridad en su contenido y autenticidad.

Elasticidad

Es la capacidad que tienen los servicios ofrecidos, a través de la nube computacional, para aumentar o reducir sus recursos en tiempo real, de acuerdo a la necesidad del usuario.

Energy Star

Es un programa de la Agencia de Protección Ambiental de los Estados Unidos (EPA, por sus siglas en inglés) creado en 1992 para promover los productos eléctricos con consumo eficiente de electricidad.

Enlace

Los enlaces, también conocidos como hipervínculos o hiperenlaces, son elementos dentro de un portal web que hacen referencia a otros contenidos que se encuentran dentro del mismo portal web o en un portal externo.

Enrutadores

También conocido como router, son dispositivos utilizados para crear e intercomunicar sud-redes de datos.

Entorno de producción

Es el ambiente real en donde los usuarios finales utilizan los sistemas de información y manejan datos concretos. Además, en este entorno las fallas ocurridas pueden afectar al usuario u organismo.

Entradas y/o Salidas (I/O)

Para fines de esta norma, es la forma de comunicación que se da entre un sistema de información con un medio de almacenamiento externo.

Estándar de Cifrado Avanzado (AES)

Es un algoritmo de cifrado publicado por el Instituto Nacional de Normas y Tecnologías (NIST, por sus siglas en inglés) del gobierno de Estados Unidos. Se conoce popularmente como Rijndael y es utilizado para la criptografía simétrica.

Estándar Triple de Cifrado de Datos (TDES)

Encriptación de triple cifrado con una longitud de la clave de 112 bits.

Estándares abiertos

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

Estándares cerrados

Hace referencia a formatos que permiten su uso para consulta, pero sin permisos de manipulación.

Fast Ethernet

También conocido como Ethernet de alta velocidad, es un conjunto de estándares de la IEEE para redes Ethernet con velocidades de 100 Mbps.

Fibra óptica

Es un hilo de vidrio o plástico, por el cual se transmiten datos en forma de pulsos de luz.

Fibra óptica monomodo

Es un tipo de fibra óptica, en el cual los pulsos de luz tienen un solo modo o vía para ser transmitidos dentro de la fibra óptica.

Fibra óptica multimodo

Es un tipo de fibra óptica, en el cual los pulsos de luz toman diferentes modos o vías para ser transmitidos dentro de la fibra óptica.

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 ISO

Es en donde se encuentra almacenada una copia exacta de algún sistema de archivo, ya sea discos duros, CD, DVD, entre otros.

Formatos

Hace referencia al tipo de codificación de la información en un archivo.

Fuerza bruta

Hace referencia al método de recuperar una contraseña probando todas las combinaciones posibles hasta encontrar el acceso.

Función Hash

Es una función que utilizada un algoritmo de computación para realizar, a partir de cualquier dato de entrada, la conversión del mismo a una cadena que solo es posible volver a crear con dicha entrada.

Gigabit Ethernet

Es un estándar para los tipos de cables cuya velocidad de transmisión de datos es de 1,000 Mbps.

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 formato de imagen orientado a la compresión sin pérdida de calidad. Soporta transparencia, al igual que el GIF y no soporta animaciones.

Gráficos Vectoriales Redimensionables (SVG)

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

Grupo Conjunto de Expertos en Fotografía (JPG)

Es un formato orientado a la captura de imágenes digitales de compresión con pérdida. Aunque su uso es muy común en la web, este no permite transparencia y se puede lograr un tamaño de imagen superior a los 65 mil pixeles, tanto de anchura como de altura.

Hardware

Se refiere a todas las partes físicas o tangibles de un sistema de información.

Herramienta de búsqueda

Es una herramienta de consulta que arroja resultados basados en los criterios de búsqueda del usuario.

Hoja de Cálculo de Documento Abierto (ODS)

Es un formato de archivo de estándar abierto especial para hojas de cálculo.

Hoja de Cálculo Office Open XML (XLSX)

Es un formato de archivo libre especial para hojas de cálculo.

Identificador Uniforme de Recursos (URI)

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

IEEE 802.1

Es una norma de la IEEE para el control de acceso a la red mediante el uso de puertos de comunicación.

IEEE 802.3u

Es un estándar de la IEEE para medios de transmisión Ethernet con velocidades de 100 Mbps.

Incidente

Es cualquier funcionamiento incorrecto de cualquiera de los servicios tecnológicos.

Información reutilizable

Hace referencia a datos o informaciones del sector público que puedan ser consumidas y/o transformadas por personas físicas o jurídicas, ya sea para fines comerciales o no.

Infraestructura como Servicio (IaaS)

Es un servicio de computación en la nube, en el cual el cliente tiene a su disposición una infraestructura de datos virtual.

Infraestructura de TIC

Para fines de esta norma, hace referencia al conjunto de equipos y elementos en lo que se sustenta un sistema de información.

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

Es una organización profesional dedica al avance de la innovación tecnológica y a la creación de estándares tecnológicos.

Instituto Nacional Estadounidense de Estándares (ANSI)

Promueve el uso de las normas estadounidenses internacionalmente. Además,

defiende las posiciones en la política, en cuanto a normas de Estados Unidos y las posiciones técnicas en organizaciones dedicadas a las normas internacionales.

Interfaz de Sistema para Pequeñas Computadoras versión 3 (SCSI 3)

Es una interfaz de datos para transferir información en serie, con una velocidad trasmisión de 20MB/s a 80MB/s dependiendo de su implementación, con soporte para 15 dispositivos.

Interfaz de usuario

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

Interfaz física

Para fines de esta norma, es el medio que utilizan los dispositivos o computadores para conectarse a la red de datos.

Intranet

Es una red interna para compartir de forma segura cualquier información o aplicación y evitar que cualquier usuario de Internet pueda ingresar a la red.

Inventario

Es un registro organizado de los activos pertenecientes o bajo la responsabilidad de un organismo determinado.

Lenguaje de Consulta Estructurados (SQL)

El SQL es un lenguaje de programación utilizado para acceder a bases de datos relacionales.

Lenguaje de consulta para RDF (SPARQL)

Es un lenguaje de consulta para grafos estandarizados en RDF.

Lenguaje de Marcado Geográfico (GML)

Es un lenguaje de marcado geográfico abierto para modelar información geográfica.

Lenguaje de Marcado Keyhole (KML)

Es un lenguaje de marcado geográfico abierto para modelar información geográfica en tres dimensiones.

Lenguaje de Marcas de Hipertexto, versión 5 (HTML5)

Es la versión 5 del lenguaje de programación HTML, de ahí su nombre HTML5, para desarrollo 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.

Licencia de Base de Datos Abierta (ODBL)

Es un contrato de licencia en donde se permite la libre manipulación de una base de datos.

Licencia de Bienes de Creación Común de Atribución-CompartirIgual (CC BY-SA)

Es una licencia de derecho de autor que permite al beneficiario manipular en todos los sentidos el contenido o producto, manteniendo los principios de esta licencia.

Licencia Pública General de GNU (GNU/GLP)

Es una licencia que permite al usuario, compañía u organismo, dar uso público a un contenido o código fuente de manera libre y sin restricción.

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.

Mascara de red

Permite a los dispositivos identificar cuál es la sub-red a la que pertenecen.

Máscaras de sud-red de tamaño variable (VLSM)

Es una técnica para brindar una mayor flexibilidad en uso de sub-redes, permitiendo al organismo dividir un sistema independiente utilizando más de una máscara de sub-red.

Matriz de Control en la Nube (CCM)

Es una matriz de control desarrolla por la CSA para ayudar a los clientes a evaluar los niveles de riesgos de seguridad de los proveedores de servicio en la nube computacional.

Medios Ethernet

Son los diferentes tipos de vías por la cual se puede establecer una conexión entre dos o más dispositivos o computadores dentro del estándar Ethernet.

Menú

Son una serie de opciones dispuestas para el usuario para poder acceder a diferentes secciones o páginas internas de un portal web.

Metadatos

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

Micrones

Es la millonésima parte de un metro, y corresponde a una unidad de medida de longitud en el cableado de fibra óptica.

Módulos

Los módulos son funciones extras que extienden la funcionalidad de una plataforma; estos pueden brindar funcionalidades sin depender de una plataforma.

Multimedia

Se refiere al conjunto de elementos de audio, video, textos, imágenes o animaciones usados para comunicar una información.

Navegador web

Es un tipo de software utilizado para acceder de forma gráfica a los recursos disponibles en una red o Internet.

N-capas

Es utilizado para referirse al número de niveles que componen la arquitectura de un software.

Notación de objetos de JavaScript (JSON)

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

Notación Turtle

Conocido también como Lenguaje de Notación 3 o "N3", es un lenguaje utilizado para sintaxis XML de RDF.

Ogg Theora

Es un formato abierto de video que permite compresión sin pérdida.

Ogg Vorbis

Es un formato abierto de audio general con pérdida.

Opus

Es un formato abierto de audio que permite compresión con pérdida.

Organización Internacional de Normalización (ISO)

Es una organización encargada de la creación de normas y estándares internacionales en diferentes áreas como tecnologías, seguridad, servicios, entre otros.

Par Trenzado sin blindaje (UTP)

Es un tipo de cable de par trenzado utilizado para las telecomunicaciones. El trenzado de estos cables anula las interferencias de fuentes externas.

Plataforma como Servicio (PaaS)

Es un servicio de computación en la nube, en el cual el cliente tiene a disponible

una plataforma para desarrollar y ejecutar diferentes tipos de software, siempre y cuando estos sean compatibles con dicha plataforma de información.

Plataforma de TIC

Para fines de esta norma, se refiere al tipo de arquitectura, sistema operativo, lenguaje de programación o interfaz de usuario, que en conjunto establecerán el sistema base para hacer operar determinados hardware o software dentro de un organismo.

Portal web

Es un conjunto de páginas electrónicas que presentan información y recursos de interés al usuario.

Portales web

Es un conjunto de páginas electrónicas que presentan información y recursos de interés al usuario.

Protocolo de Autenticación Remota para Servicios de Marcado a Usuarios (RADIUS)

Es un protocolo de autentificación para acceso a redes.

Protocolo de configuración Dinámica de Host (DHCP)

Es un protocolo de red, el cual permite a los ordenadores obtener una dirección IP de manera automática, así como otros parámetros de configuración.

Protocolo de Datos Abiertos (ODATA)

Es un protocolo abierto de acceso a base de datos.

Protocolo de Información de Enrutamiento (RIP)

Es un protocolo de tipo vector-distancia empleado para intercambiar información sobre redes IP, el cual utiliza la cantidad de enrutadores presentes en una ruta.

Protocolo de Internet (IP)

Es un protocolo de comunicación de datos, a través de un medio digital.

Protocolo de Internet versión 4 (IPV4)

Es la cuarta versión del protocolo IP de 32 bits de longitud y fue la primera versión en ser implementada.

Protocolo de Internet versión 6 (IPV6)

Es la sexta versión del protocolo IP de 64 bit de longitud, con el fin de cubrir el agotamiento de las direcciones IPV4.

Protocolo de Red de Telecomunicación (Telnet)

Es un protocolo que nos permite acceder remotamente a otro equipo mediante una terminal, es decir sin gráficos.

Protocolo de Transferencia de Hipertexto (HTTP)

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

Protocolo del Primer Camino Más Corto (OSPF)

Es un protocolo de enrutamiento de tipo estado-enlace que utiliza el algoritmo Dijkstra para calcular la ruta más corta hacia un destino en específico.

Prototipo

Es la representación inicial de un producto entregable, con el objetivo de aplicarle mejoras o correcciones.

Proveedores de Servicio de Internet (ISP)

Son todas aquellas empresas que ofrecen el servicio de conexión a Internet.

Publicación Electrónica (ePub)

Es un formato estándar de código abierto utilizado en publicaciones electrónicas para leer textos e imágenes.

Puerto de conexión

Hace referencia a una interfaz física para transferencia de datos.

Punto de consolidación

Son los puntos de interconexión entre cableados horizontales.

Puntos de Distribución Central (MDF)

Es el área dentro de una LAN donde se encuentra todo el cableado de datos principal y desde esta área se distribuye el cableado hacia el/los IDF.

Puntos de Distribución Intermedios (IDF)

Es el área dentro de una LAN donde se distribuye todo el cableado de datos correspondiente a los usuarios. Comúnmente también se alojan equipos de redes, tales como, conmutadores, enrutadores o servidores de respaldos.

Raster

Es un formato de imagen que su contenido está compuesto por pixeles.

Rastro de navegación

Muestra la profundidad en la que estamos navegando en un portal, este comúnmente se encuentra en la parte superior donde esta fácilmente visible al usuario.

Red de Área Local (LAN)

Es una red de datos con un alcance geográficamente limitado.

Red de Área Local Inalámbrica (WLAN)

Es un sistema de comunicación inalámbrico, utilizado como otra opción a las redes locales, usando la tecnología de radiofrecuencia para llevar información de un punto a otro, permitiendo mayor movilidad y disminución en las conexiones cableadas.

Red de Área Local Virtual (VLAN)

Es una red interna virtual, que permite crear redes lógicas dentro de una misma red física.

Red de datos

Hace referencia a un conjunto de dispositivos o computadores interconectados

entre sí para el intercambio de información.

Red Privada Virtual (VPN)

Es una red virtual privada que permite de forma segura la interacción de datos sobre redes compartidas utilizando como vínculo el Internet.

Redes sociales

Son medios virtuales de comunicación que funcionan como una plataforma para que los usuarios puedan interactuar con otras personas que tienen intereses en común.

Repositorio

Es un sitio en la red donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

Resolución de pantalla

Es la cantidad máxima de pixeles que pueden ser mostrados en un monitor.

Sistema de Respuesta de Voz Interactiva (IVR)

Es un sistema telefónico capaz de recibir una llamada e interactuar con el humano, a través de grabaciones de voz y el reconocimiento de respuestas simples, mediante las teclas del teléfono o el móvil.

Riesgo

Es la posibilidad o probabilidad potencial de que un daño o amenaza afecte a un organismo.

Riesgo residual

Hace referencia al riesgo que queda luego de haber tomado todas las medidas preventivas de reducción de riesgos.

Segmento de red

Es la conexión que existe entre un dispositivo o computador y un equipo de la red datos como un switch o un router.

Seguridad del protocolo IP (IPsec)

Es un conjunto de protocolos que proporcionan seguridad al protocolo IP en cuanto a la autenticación y cifrado de los datos.

Servidores

Son equipos informáticos que forman parte de una red de datos y que proveen servicios a otros equipos en dicha red, llamados clientes.

Sindicación Realmente Simple (RSS)

Es un formato XML utilizado para compartir contenidos en la Web.

Sistema de inventario

Software que permite realizar y controlar todo el proceso de inventario.

Sistema operativo

Es un software utilizado en los sistemas de información para gestionar y administrar los recursos de los dispositivos o computadores.

Sitio de almacenamiento

Hace referencia a un lugar específico dentro de un medio de almacenamiento. Esto puede ser una carpeta determinada dentro de un repositorio de documentos o carpetas.

Software

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

Software como Servicio (SaaS)

Hace referencia a un modelo de distribución de software donde los datos y el soporte del mismo están alojados en una compañía que da servicios de TIC donde este es accedido desde el navegador.

Software gubernamental

Para fines de esta norma, son todas las herramientas aplicaciones y software

desarrollados a la medida o para soluciones específicas, utilizadas por el estado.

Software propietario

Es el software que para su uso debe pagarse un licenciamiento al proveedor y cuya modificación no es permitida.

Sub-portal

Es un portal web que depende de otro portal, es básicamente una extensión del portal madre, específicamente para presentar una información exclusiva que tiene mucha relevancia, pero que sigue estando relacionado con el portal principal.

Sub-redes

Se refiere a una serie de redes contenidas dentro de una red, las cuales se han dividen para aprovechar mejor las direcciones IPV4.

Sumarización de direcciones IP

Es un método para reducir el número de entradas de direcciones IP al enrutador, teniendo como resultado una automatización en el cálculo de rutas.

Tarjeta de red

Es una tarjeta o adaptador que permite la comunicación entre dos dispositivos en una red datos, a través de un medio físico o inalámbrico.

Texto de Documento Abierto (ODT)

Es un formato de archivo libre especial para documentos de texto con formato.

Tipo de fuente

Es la forma en la cual se representa o visualiza una letra, número o símbolo.

Topología de red

Es la arquitectura física y lógica de una red. En esta se representan todos los enlaces y dispositivos que se relacionan entre sí.

Usabilidad

Es la facilidad con la que el usuario puede interactuar con un software para la

realización de una tarea en específica. Este término fue definido por primera vez por Jakob Nielsen considerado el padre la usabilidad.

Usuario

Hace referencia a la persona que consume o manipula un producto, servicio o información.

Valores Separados por Comas (CSV)

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

Valores Separados por Delimitadores (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.

Ventanas emergentes

Las ventanas emergentes, también conocidas como pop-up, son ventanas o navegadores que abren automáticamente para presentar un contenido específico, los cuales, en su mayoría, abren sin el permiso o consentimiento del usuario.

Virtualización

Es el uso de un software para crear máquinas virtuales para emular un computador físico.

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.

Voz sobre Protocolo de Internet (VoIP)

Son recursos que permiten que una señal de voz sea transmitida, a través de Internet, mediante el protocolo IP.

Vulnerabilidad

Hace referencia a la incapacidad de defensa frente a una amenaza.

WebM

Es un formato abierto de video que permite compresión con baja pérdida de calidad, este fue creado con el fin de establecer un nuevo estándar de video en la web.

WebP

Es un formato de imagen que permite compresión con pérdida y compresión sin perdida.

XviD

Es una códec de compresión de video que permite una alta compresión con baja pérdida de calidad.

ZIP

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

Zonas Desmilitarizadas (DMZ)

Es una red de datos localizada entre la red de datos del organismo y la red externa, esta funciona como una zona de seguridad en donde las conexiones externas tienen restringido el acceso a la red de datos del organismo, evitando así, comprometer la seguridad del mismo.

ABREVIATURAS Y ACRÓNIMOS

NO.	ABREVIATURAS Y ACRÓNIMOS	INGLÉS	ESPAÑOL
1	(I/O)	Input/Output	Entradas y/o Salidas
2	AES	Advanced Encryption Standard	Estándar de Cifrado Avanzado
3	ANSI	American National Standards Institute	Instituto Nacional Estadounidense de Estándares
4	Bzip2	BSD Zip	Zip bajo licencia BSD
5	CAMWEB	N/A	Comité Administrativo de los Medios Web
6	CC BY-SA	Creative Commons Attribution-Share Alike	Bienes de Creación Común de Atribución-Compartir Igual
7	CCM	Cloud Control Matrix	Matriz de Control en la Nube
8	CMDB	Configuration Management Database	Base de Datos de la Gestión de Configuración
9	COETIC	N/A	Comité de Estándares de Tecnologías de la Información y Comunicación
10	CONTI	N/A	Comité de Continuidad
11	CRM	Customer Relationship Management	Sistema para la Administración de la Relación con los Clientes
12	CSA	Cloud Security Alliance	Alianza de Seguridad en la Nube
13	CSV	Comma-Separated Values	Valores Separados por Coma
14	DCAT	Data Catalog Vocabulary	Vocabulario para Catálogo de Datos
15	DHCP	Dynamic Host Configuration Protocol	Protocolo de Configuración Dinámica de Host
16	DIGEIG	N/A	Dirección General de Ética e Integridad Gubernamental.

17	DMZ	Demilitarized Zone	Zonas Desmilitarizadas
18	EDA	Equipment Distribution Area	Área de Distribución de Equipos
19	EDT	N/A	Estructura de Desglose del Trabajo
20	EIA	Electronic Industries Alliance	Alianza de Industrias Electrónicas
21	ePub	Electronic Publication	Publicación Electrónica
22	ERP	Enterprise Resource Planning	Sistema para la Planificación de Recursos Empresariales
23	FDDI	Fiber Distributed Data Interface	Interfaz de Datos Distribuida por Fibra
24	FLAC	Free Lossless Audio Codec	Códec Libre de Compresión de Audio sin Pérdida
25	GML	Geographic Markup Language	Lenguaje de Marcado Geográfico
26	GNU/GPL	GNU General Public License	Licencia Pública General de GNU
27	Gzip	GNU Zip	Zip bajo licencia GNU
28	HDA	Horizontal Distribution Area	Área Horizontal de Distribución
29	HTML5	HyperText Markup Language, version 5	Lenguaje de Marcas de Hipertexto, versión 5
30	HTTP	Hypertext Transfer Protocol	Protocolo de Transferencia de Hipertexto
31	IaaS	Infrastructure as a Service	Infraestructura como Servicio
32	IDF	Intermediate Distribution Frame	Puntos de Distribución Intermedios
33	IEEE	Institute of Electrical and Electronics Engineers	Instituto de Ingenieros Eléctricos y Electrónicos
34	IPsec	Internet Protocol security	Seguridad del protocolo IP
35	ISO	International Organization for Standardization	Organización Internacional de Normalización
36	ISP	Internet Service Provider	Proveedores de Servicio de Internet

37	ITIL	Information Technology Infrastructure Library	Biblioteca de Infraestructura de Tecnologías de Información
38	IVR	Interactive Voice Response	Sistema de Respuesta de Voz Interactiva
39	JPG	Joint Photographic Experts Group	Grupo Conjunto de Expertos en Fotografía.
40	JSON	JavaScript Object Notation	Notación de objetos de JavaScript
41	KML	Keyhole Markup Language	Lenguaje de Marcado Keyhole
42	LAN	Local Area Network	Red de Área Local
43	LC	Lucent Connector	Conector Lucent
44	MC	Main Cross-connect	Cableado Cruzado Principal
45	MDA	Main Distribution Area	Área Central de Distribución
46	MDF	Main Distribution Frame	Puntos de Distribución Central
47	MRSID	Multi-resolution Seamless Image Database	Base de Datos de Imagen con Multi-Resolución Constante
48	OAI	N/A	Oficina de Libre Acceso a la Información
49	ODATA	Open Data Protocol	Protocolo de Datos Abiertos
50	ODBL	Open Database License	Licencia de Base de Datos Abierta
51	ODS	Open Data Spreadsheet	Hojas de Cálculo de Documento Abierto
52	ODT	Open Document Text	Texto de Documento Abierto
53	OPTIC	N/A	Oficina Presidencial de Tecnologías de la Información y Comunicación
54	OSPF	Open Shortest Path First	Primer Camino Más Corto
55	PaaS	Platform as a Service	Plataforma como Servicio
56	PDF	Portable Document Format	Formato de Documento Portátil
57	PNG	Open Document Text	Gráficos de Red Portátiles

58	PPP	N/A	Puntos Por Pulgadas
59	QoS	Quality of Service	Calidad de servicio
60	RADIUS	Remote Authentication Dial-In User Service	Autenticación Remota para Servicios de Marcado a Usuarios
61	RAID	Redundant Array of Independent Disks	Conjunto Redundante de Discos Independientes
62	RDF	Resource Description Framework	Marco de Descripción de Recursos
63	RFP	Request for Proposal	Solicitud de Propuesta
64	RIP	Routing Information Protocol	Protocolo de Información de Enrutamiento
65	RJ-45	Registered Jack 45	Conector Registrado 45
66	RSS	Really Simple Syndication	Sindicación Realmente Simple
67	SaaS	Software as a Service	Software como Servicio
68	SAS	Serial Attached SCSI	Acoplamiento Serial SCSI
69	SASI	N/A	Sistema para la Administración de la Seguridad de la Información
70	SATA	Serial Advanced Technology Attachment	Acoplamiento de Serie de Tecnología Avanzada
71	SC	Square Connector	Conector Cuadrado
72	SCSI 3	Small Computers System Interface 3	Interfaz de Sistema para Pequeñas Computadoras versión 3
73	SHA1	Secure Hash Algorithm 1	Algoritmo de “Hash” Seguro
74	SLA	Service Level Agreement	Acuerdos de Nivel de Servicio
75	SNMP	Simple Network Management Protocol	Protocolo para la Transferencia Simple de Correo Electrónico
76	SPARQL	SPARQL Protocol and RDF Query Language	Protocolo SPARQL y Lenguaje de Consulta RDF
77	SQL	Structure Query Language	Lenguaje de Consulta Estructurado

78	SSD	Solid-State Drive	Unidad de Estado Sólido
79	SSH	Secure SHell	Intérprete de Órdenes Seguras
80	SSL	Secure Sockets Layer	Capa de Conexión Segura
81	ST	Straight Tip	Conector de Punta Recta
82	SVG	Scalable Vector Graphics	Gráficos Vectoriales Redimencionables
83	TDES	Triple Data Encryption Standard	Estándar de Cifrado Avanzado Triple
84	Telnet	Telecommunication Network	Red de Telecomunicación
85	TIA	Telecommunications Industry Association	Asociación de Industria de Telecomunicaciones
86	TIC	N/A	Tecnologías de la Información y Comunicación
87	TIER	Taiwan Institute of Economic Research	Instituto de Investigación Económica de Taiwan
88	TIFF	Tagged Image File Format	Formato de Archivo de Imagen Etiquetado
89	TSV	Tab-Separated Values	Valores Separados por Delimitadores
90	URI	Uniform Resource Identifier	Identificador Uniforme de Recursos
91	UTP	Unshielded Twisted Pair	Par Trenzado sin Blindaje
92	VLSM	Variable Length Subnet Mask	Máscaras de Sud-red de Tamaño Variable
93	VPN	Virtual Area Network	Red Privada Virtual
94	WEBm	Web movies	Web película
95	Webp	Web picture	Imagen Web
96	WLAN	Wireless Local Area Network	Red de Área Local Inalámbrica
97	WPA	Wi-Fi Protected Access	Acceso Wi-fi Protegido
98	WPA2	Wi-Fi Protected Access 2	Acceso Wi-fi Protegido
99	XLSX	Office Open XML Spreadsheet	Hoja de Cálculo Office Open XML

100	XML	Extensible Markup Language	Lenguaje de Marcas Extensible
101	ZDA	Zone Distribution Area	Área de Zona de Distribución
102	ZIP	N/A	Su traducción literal sería “Cremallera”, aduciendo a su función de comprimir

BIBILIOGRAFÍA

- AENOR. (2011). Normas de Gestión Avanzada. *La Norma ISO/IEC 38500. Aspectos Básicos*.
- American National Standards Institute / Building Industry Consulting Service International. (2011). *Data Center Desing and Implementation Best Practices*. Estados Unidos: BICSI.
- American National Standards Institute / Project Management Institute. (2004). *Guía de los Fundamentos de la Dirección de Proyectos, 3*.
- Banco Central de la República Dominicana. (2013). *Instructivo sobre digitalización, truncamiento y compensación de cheques*. República Dominicana.
- Cloud Security Alliance. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*. Estados Unidos.
- Consejería de Economía y Administración Pública. (2007). Normas Técnicas. *Digitalización de documentos*. Principado de Asturias.
- Cordero, J. A. (2012). *Metodología para administrar proyectos de tecnología basados en arquitectura orientada a servicios*. Costa Rica.
- DiMinico, C. (n.d.). ANSI/TIA - 942. *Telecomunications Infrastructure Standard for Data Centers*.
- Dirección de Tecnologías de Información y Comunicaciones. (2007). *Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones*. Costa Rica.
- European Network and Information Security Agency (ENISA). (2009). *Computación en nube. Beneficio, riesgos y recomendaciones para la seguiridad de la información*. Europa.
- Gobierno de Perú. (2004). *Guía para la Administración Eficiente de Software Legal en la Administración Pública*. Perú.
- Hausman, K. K., & Susan L.Cook. (2011). *IT Architecture For Dummies*. Wiley Publishing, Inc.

- Heldman, K., & Heldeman, W. (2010). *Project Plus - Study Guide*. Canadá: Wiley Publishing, Inc.
- Information Technology Infrastructure Library. (2006). *Glosario de Términos ITIL, Definiciones y Acrónimos*.
- Instituto Nacional de Tecnologías de la Comunicación. (2010). *Guía práctica para PYMES: Cómo implantar un Plan de Continuidad de Negocio*. España.
- International Organization for Standardization. (2009). ISO 31000. *Risk management - Principles and Guidelines on Implementation*.
- International Organization for Standardization / International Electrotechnical Commission. (2005). ISO/IEC 27001. *Information technology - Security techniques - Information Security managements systems - Requirements*.
- International Organization for Standardization / International Electrotechnical Commission. (2008). ISO/IEC 12207. *Systems and software engineering - Software life cycle processes*. Suiza.
- International Organization for Standardization. (2012). ISO 22301. *Societal security - Business continuity management systems - Requirements*.
- ISACA. (2012). COBIT 5. *A Business Framework for the Governance an Management of Enterprice IT*.
- IT Governance Institute. (2007). COBIT 4.1. *Marco de trabajo - Objetivos de Control- Directrices gerenciales - Modelos de madurez*. Estados Unidos.
- ITIL V3. (2007). *Service Operation*. Londres: Office of Goverment Commerce.
- Lammle, T., & Swartz, J. (2013). CCNA Data Center. *Introducing Cisco Data Center Networking - Study Guide*. Canada: Neil Edde.
- Leavitt, M. O., & Shneiderman, B. (n.d.). *Research - Based Web Desing & Usability Guidelines*. Estados Unidos.
- Ministerio de Educación del Gobierno de Chile. (n.d.). *Guía de Inventario*. Chile.

- Ministerio de Hacienda y Administraciones Públicas; Centro Criptológico Nacional. (2013). *Guía / Norma de Seguridad de las TIC - Seguridad en entornos cloud*. España.
- Ministerio de Industria, Turismo y Comercio; Instituto Nacional de Tecnologías de la Comunicación. (2011). *Guía sobre almacenamiento y borrado seguro de información*. España.
- Ministerio de Trabajo y Asuntos Sociales / Instituto Nacional de Seguridad e Higiene en el Trabajo. (n.d.). NTP 434. *Superficies de trabajo seguras*. España.
- Observatorio de Políticas Públicas. (2011). *Políticas de clasificación de la información en el Estado*.
- Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC). (2013). *Plan Estratégico 2013-2016*. República Dominicana.
- OPTIC. (2013). NORTIC A2. *Norma para la creación y administración de portales web del Gobierno Dominicano*. República Dominicana.
- OPTIC. (2013). NORTIC A3. *Norma sobre publicación de datos abiertos del Gobierno Dominicano*. República Dominicana.
- SAFECode; Cloud Security Alliance. (2013). *Practices for Secure Development of Cloud Applications*.
- Software Engineering Institute. (2010). CMMI-Dev. *Guía para la integración de procesos y la mejora de productos, 3*. Estados Unidos: Editorial Universitaria Ramón Areces.
- Universidad Pedagógica Nacional. (2012). *Guía para el mejor uso del papel*. México.
- Whitaker, S. (2013). *PMP - Training Kit*. Estados Unidos: O'Reilly Media, Inc.

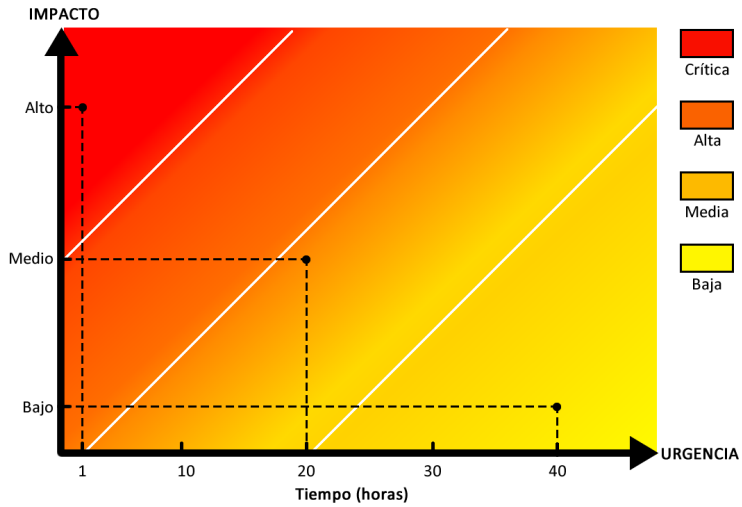
ANEXOS

Anexo A. Tabla de ponderación para selección compuesta de la estructura del departamento de TIC

ÁREA BÁSICA: TIC		
Existencia:	Requerido para todos los modelos de estructura.	
Ponderación de criterios:	**Criterios**	**Ponderación**
	Número de empleados	20%
	Localidades	20%
	Complejidad de aplicaciones desarrollo interno	10%
	Estaciones de trabajo	20%
	Número de servidores	10%
	Centro de datos de contingencia	10%
	Administra sistema de impacto externo	10%
ÁREA BÁSICA: DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS		
Existencia:	Requerido para instituciones que realizan mantenimiento a aplicaciones.	
Ponderación de criterios:	**Criterios**	**Ponderación**
	Número de empleados	10%
	Localidades	10%
	Complejidad de aplicaciones desarrollo interno	30%
	Estaciones de trabajo	10%
	Número de servidores	10%
	Centro de datos de contingencia	10%
	Administra sistema de impacto externo	20%
ÁREA BÁSICA: OPERACIONES DE TIC		
Existencia:	Requerido para todos los modelos de estructura.	
Ponderación de criterios:	**Criterios**	**Ponderación**
	Número de empleados	10%
	Localidades	20%
	Complejidad de aplicaciones desarrollo interno	5%
	Estaciones de trabajo	25%
	Número de servidores	20%
	Centro de datos de contingencia	15%
	Administra sistema de impacto externo	5%
ÁREA BÁSICA: ADMINISTRACIÓN DEL SERVICIO		
Existencia:	Requerido para todos los modelos de estructura.	

Ponderación de criterios:	**Criterios**	**Ponderación**
	Número de empleados	20%
	Localidades	20%
	Complejidad de aplicaciones desarrollo interno	5%
	Estaciones de trabajo	20%
	Número de servidores	20%
	Centro de datos de contingencia	10%
	Administra sistema de impacto externo	5%
ÁREA BÁSICA: ADMINISTRACIÓN DE PROYECTOS TIC		
Existencia:	Requerido para organismos con más de 4 proyectos de TIC que impacten al menos el 50% de la estructura organizacional.	
Estructura única.		
ÁREA BÁSICA: SEGURIDAD Y MONITOREO		
Existencia:	Requerido para organismos que administren sistemas con al menos 50 usuarios y 20 perfiles de usuario.	
Ponderación de criterios:	**Criterios**	**Ponderación**
	Número de empleados	15%
	Localidades	10%
	Complejidad de aplicaciones desarrollo interno	20%
	Estaciones de trabajo	15%
	Número de servidores	10%
	Centro de datos de contingencia	10%
	Administra sistema de impacto externo	20%

Anexo B. Diagrama de prioridades, según el impacto y la urgencia del incidente



Este diagrama de prioridades fue elaborado en base al establecido por la OSIATIS

Impacto: Determina la importancia de la incidencia dependiendo de cómo esta afecta a los procesos del organismo gubernamental y/o del número de usuarios afectados.

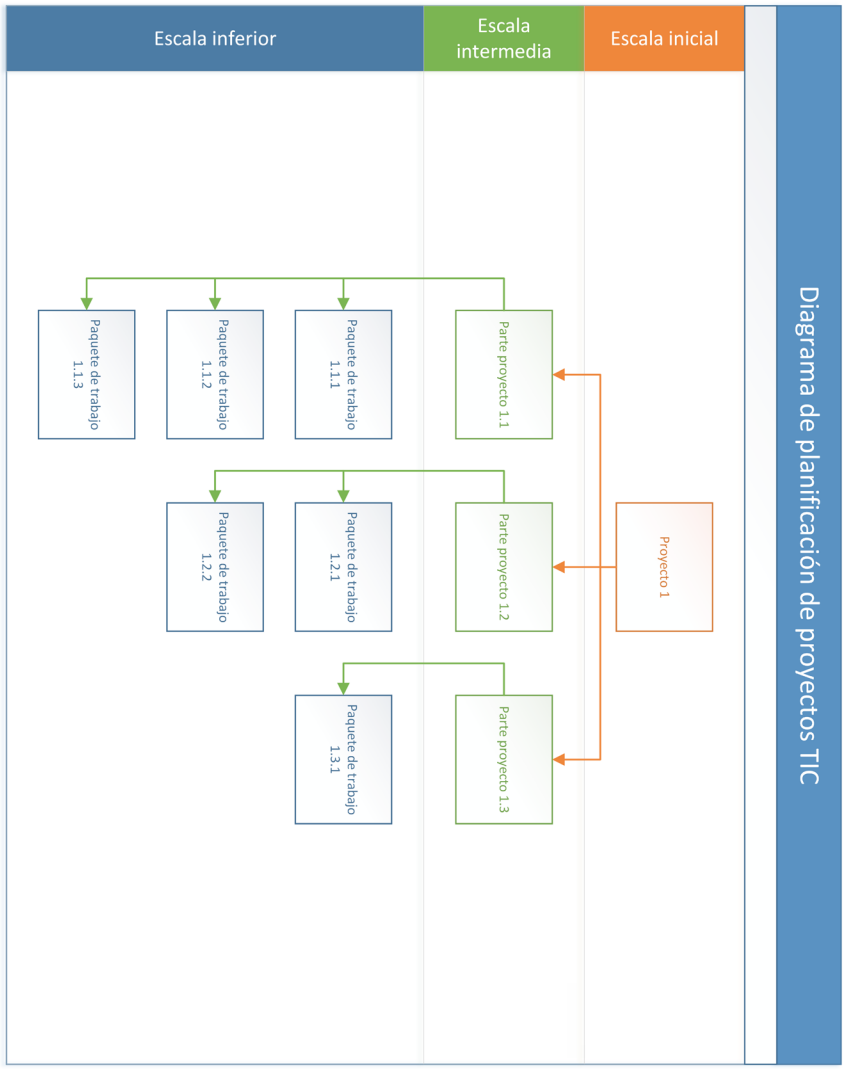
Urgencia: Depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el SLA.

> **Nota**: *El término "Impacto" utilizado en este anexo se define y se aplica únicamente para la gestión de incidentes. Sin embargo, cuando se esté utilizando el referido término para la gestión de riesgo, su definición cambiará alineada hacia este contexto.*

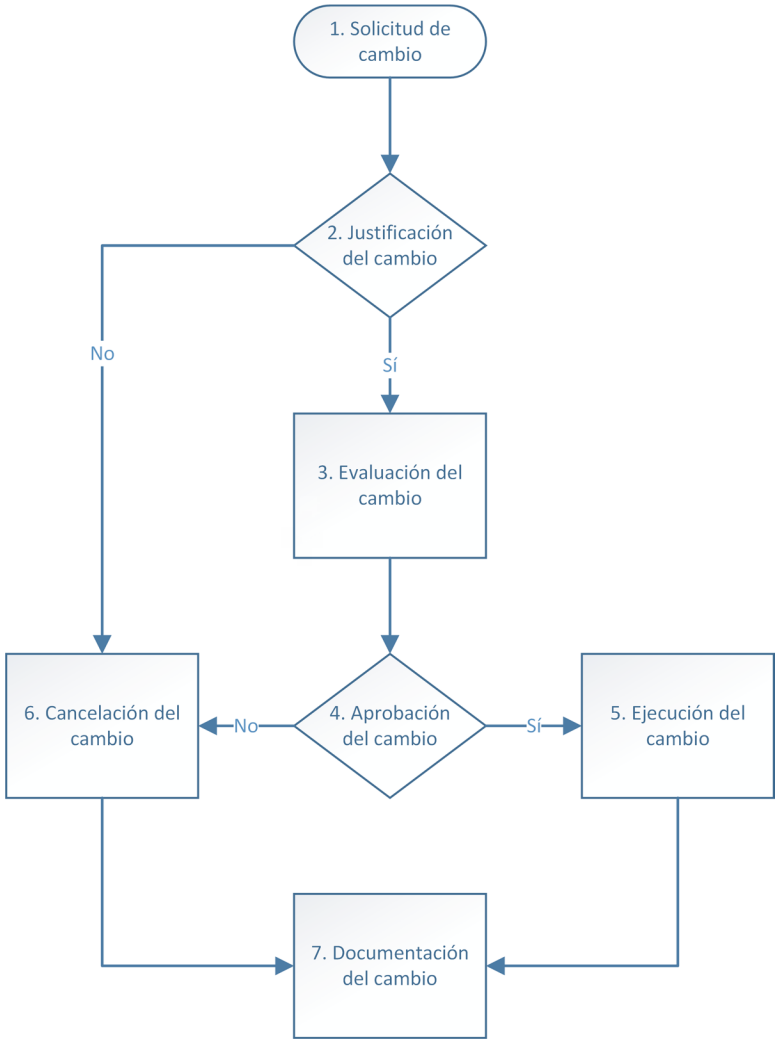
Anexo C. Matriz de escalamiento para la gestión de incidentes

Esta matriz de escalamiento fue elaborada en base la establecida por la OSIATIS.

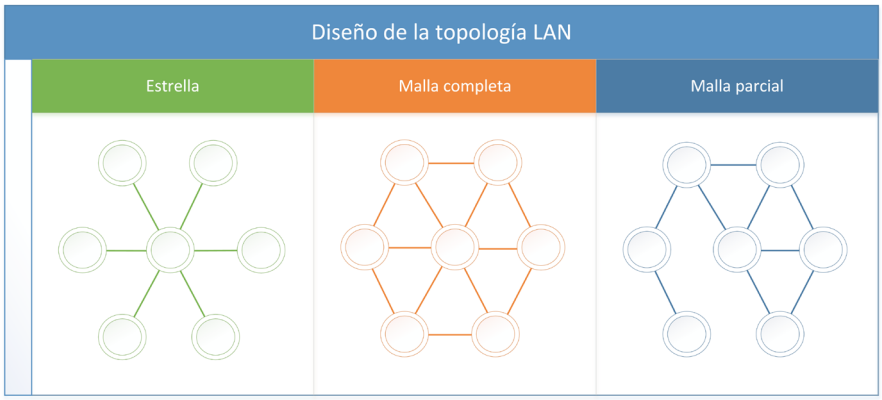
Anexo D. Diagrama de planificación de proyectos de TIC



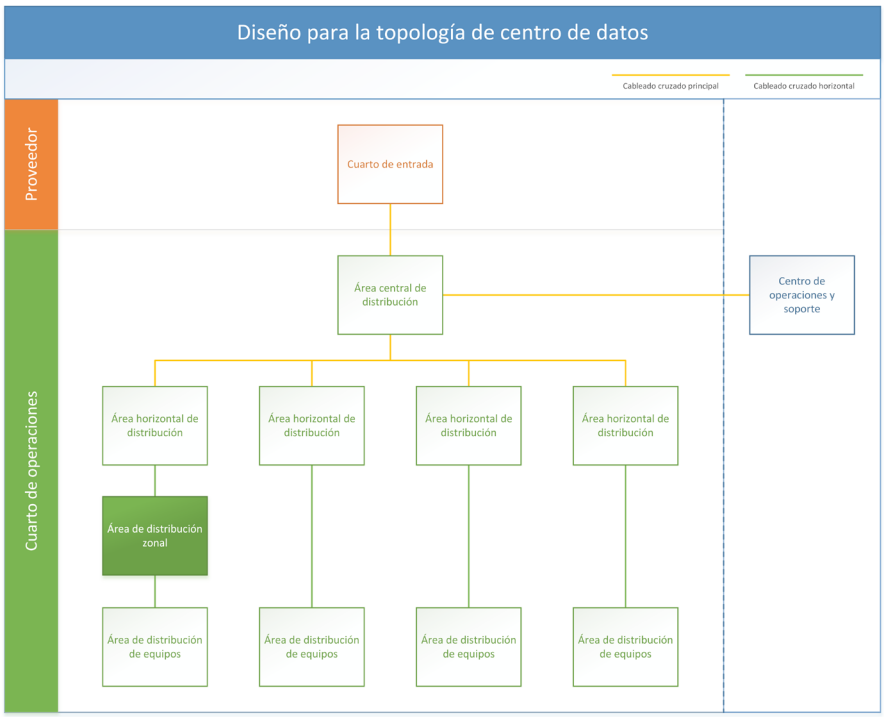
Anexo E. Proceso de solicitud de cambio



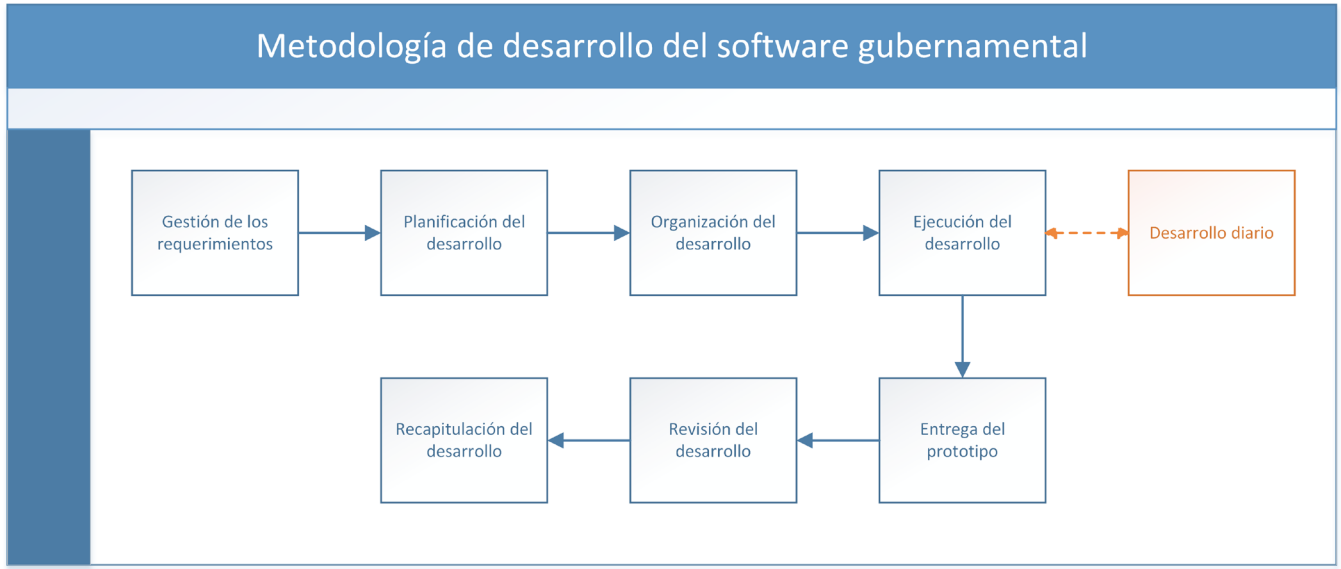
Anexo F. Diseño de la topología LAN



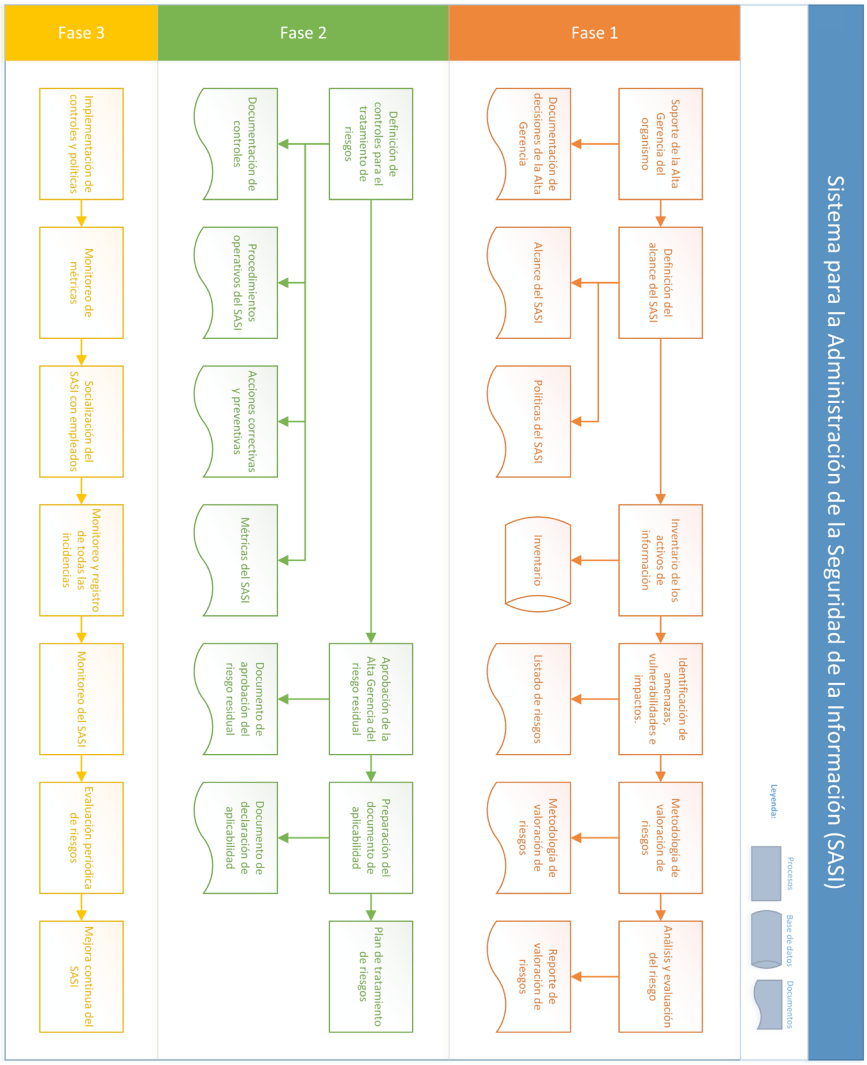
Anexo G. Diseño para la topología del centro de datos



Anexo H. Metodología de desarrollo del software gubernamental



Anexo I. Implementación del Sistema para la Administración de la Seguridad de la Información (SASI)



Anexo J. Procesos para la implementación de un SASI

ENTRADA	PROCESO	SALIDA
Requerimiento de implementación del SASI	Definición de políticas, objetivos y alcance	Políticas, objetivos y alcance
Amenazas, vulnerabilidades, impactos y metodología	Análisis de riesgos	Inventario de activos e informe del análisis de riesgos
Informe del análisis y controles	Tratamiento de riesgos	Plan de tratamiento de riesgos
Controles y plan de tratamiento de riesgos	Implantación y operación del SASI	Políticas, procedimientos, instrucciones
Auditorías, registros, revisiones y métricas	Monitoreo y revisión del SASI	Plan de mejora
Acciones correctivas y acciones preventivas	Mantenimiento y mejora del SASI	

Anexo K. Referencia para la eliminación de documentos por antigüedad

DOCUMENTOS A ELIMINAR	ANTIGÜEDAD
Información de solicitud de empleo al organismo gubernamental.	6 meses
Información de empleados fallecidos.	2 años
Información de empleados que han renunciado.	
Información de empleados cancelados.	
Información judicial, historial médico, historial de sanciones e historial de méritos.	
Toda información de accidentes de trabajo de los empleados a partir de la fecha de prescindir del recurso.	
Toda información clasificada que pierda su utilidad.	5 años
Toda información física que no agregue valor estratégico para decisiones de la Alta Gerencia.	10 años
Cualquier otra documentación no mencionada que no agregue valor.	12 años

Para fines de esta norma, la antigüedad de los documentos a eliminar se empezará a contabilizar a partir de que el organismo determine que dicho documento no agrega valor.

Anexo L. Métodos de borrado adecuado en función del dispositivo

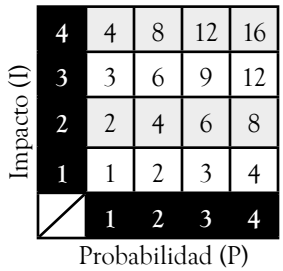
MEDIO DE ALMACENAMIENTO	MÉTODOS ADECUADOS DE BORRADO
Discos duros magnéticos	Destrucción física Desmagnetización Sobreescritura
Discos flexibles	
Cintas de respaldo	
Discos duros electrónicos	Destrucción física Sobreescritura
Discos ópticos	Destrucción física
Memorias USB	Destrucción física Sobreescritura

Anexo M. Categorías de Usuarios

CATEGORÍAS DE USUARIOS	DESTINADO A	DESCRIPCIÓN
Invitado	Personal invitado	Acceso restringido a instalación de aplicaciones
		Acceso controlado a Internet
		*Acceso restringido a descargas
Personal operativo	Personal del organismo	Acceso restringido a instalación de aplicaciones
	Usuarios con funciones no técnicas	Acceso controlado a Internet
		Acceso controlado a descargas
Personal técnico	Personal del organismo	Acceso a instalación de aplicaciones
	Usuarios con funciones técnicas	Acceso a Internet
		Acceso a descargas

** En caso de un usuario necesitar algún acceso o permiso para el desempeño de sus funciones, esta puede ser otorgada temporalmente o indefinidamente por el personal autorizado para los fines. Las categorías definidas no abarcan en concreto al personal del departamento de TIC debido a que para estos existe un perfil con menos restricciones.*

Anexo N. Referencia para determinar el nivel del riesgo identificado



- *Según el resultado de la multiplicación para obtener el riesgo, el mismo caerá dentro de diferentes niveles de atención como se menciona a continuación:*
  - *Resultado de 1 a 6: Riesgo bajo.*
  - *Resultado de 8 a 9: Riesgo medio.*
  - *Resultado de 12 a 16: Riesgo alto.*
- ***Caso de ejemplo**: siendo un huracán un riesgo detectado en República Dominicana, en una empresa X, le asignaremos un impacto de valor tres (3) y una probabilidad, también de valor tres (3), entonces, si multiplicamos el impacto por la probabilidad (R=IxR), tendríamos como resultado el valor nueve (9), quedando en el rango de los riesgos medios.*

Anexo O. Tipos de análisis de riesgos

TIPO DE ANÁLISIS	DESCRIPCIÓN	VENTAJAS	INCONVENIENTES
Cualitativo	Basado en clasificaciones descriptivas y subjetivas del riesgo	Sencillez Rapidez Equilibrio en Coste-Beneficio Uso extendido	Subjetividad
Cuantitativo	Basado en términos monetarios	Exactitud Objetividad	Complejidad para estimar costes reales

Anexo P. Comparativa de los métodos de borrado seguro

MÉTODO	VENTAJAS	DESVENTAJAS
Destrucción física	Eliminación segura de la información y destrucción de dispositivos no regrabables y ópticos	Requiere un sistema de destrucción para cada soporte
		Dificultad de certificación del proceso
		Necesidad de transportar los equipos a una ubicación externa
		Destrucción definitiva y dificultad de reciclaje de materiales
Desmagnetización	Eliminación de forma segura de la información	Una configuración del sistema para cada soporte
		Dificultad de certificación del proceso
		Necesidad de transportar los equipos a una ubicación externa
		Solo válido para dispositivos de almacenamiento magnético
		Tras el proceso, el dispositivo deja de funcionar correctamente
Sobreescritura	Eliminación de forma segura de la información	No válido para dispositivos no regrabables ni ópticos
	Una solución para todos los dispositivos	
	Garantía documental de la operación	
	Posibilidad de eliminación en las propias oficinas	
	Reutilización de los dispositivos con garantías de funcionamiento	

Anexo Q. Requerimientos técnicos para digitalización de documentos

CARACTERÍSTICAS FÍSICAS			REQUISITOS TÉCNICOS		
Tipo	**Forma documental**	**Estado**	**Captura**	**Repositorios maestros**	**Repositorios de consultas**
Textuales		Texto bien contrastado	B/N, 300 PPP	TIFF, sin compresión/ compresión sin perdida	PDF XI o superior
		Texto mal contrastado	Escala de grises, 300 PPP	TIFF, sin compresión	
Gráficos	Fotografías		Color, 300 ppp	TIFF sin compresión/ JPEG mínima compresión	
	Planos	Buena conservación/ bien contrastados	B/N, 300 ppp	TIFF sin compresión/ compresión sin perdida	
		Mala conservación/ mal contrastados	Escala de grises 300 ppp	TIFF sin compresión	
		Color (información significativa)	Color, 300 ppp	TIFF sin compresión/ JPEG mínima compresión	

EQUIPO DE TRABAJO

Dirección General
Armando García, Director General

Departamento de Estandarización, Normativas y Auditoría Técnica (ENAT)
Elvyn Peguero, Gerente del ENAT
Shalem Pérez, Analista de Estándares y Normativas
Ginsy Aguilera, Analista de Estándares y Normativas
Winner Núñez, Analista de Estándares y Normativas
Ariel Acosta, Consultor de Estándares y Normativas

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

Luis Paulino
Procuraduría General de la República

Roberto Eugenio
Oficina Técnica de Transporte Terrestre

Tulio Verigüete
Ministerio de la Mujer

Carlos Lajara
Ministerio de Relaciones Exteriores

Carmen Mejía
Contraloría General de la República Dominicana

Carlos Segura
Ministerio de Agricultura

Ubaldo Pérez
Ministerio de Hacienda

Gilberto Molina
Ministerio de Obras Públicas y Comunicaciones

Alfonso Espinal
Instituto Dominicano de las Telecomunicaciones

César Pichardo
Cámara TIC

Ricardo Rodríguez
Asociación de Nacional de Empresas Informáticas

Colaboradores

Santa García

Erick Domínguez

Samuel Luís

Joel Jaime

Edwin Sánchez

Ariela Marte

Eliaquín Encarnación

Juana Manzueta

Junior Rosa

Israel Colomé

Luis Santiago

Juan Ciprián

Cecilia Chávez

Carlos Adames

Leonardo Alcántara

José Aquino

Ly Méndez

Cándido Ramírez

Presidencia de la República Dominicana

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

Av. 27 de Febrero #. 419, Piso 7 y 8, Sector El Millón Sto. Dgo. D.N. Rep. Dom.
Tel: 1+ 809.286-1009 Fax: 1+ 809.508.3691
info@optic.gob.do www.optic.gob.do

GOBIERNO ELECTRÓNICO
REPÚBLICA DOMINICANA

/OpticRD @OpticRD /OpticRD