Presidencia de la República

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

NORTIC B1 2016

NORMA PARA LA IMPLEMENTACIÓN Y GESTIÓN DE LA CONECTIVIDAD EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana
29 de Julio, 2016

Presidencia de la República

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

NORTIC B1 2016

NORMA PARA LA IMPLEMENTACIÓN Y GESTIÓN DE LA CONECTIVIDAD EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana

29 de Julio, 2016

NORTIC B1:2016
Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano

Edición: 1era

Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)
Departamento de Estandarización, Normativas y Auditoría Técnica

Fecha de aprobación: 22 de enero de 2015
Fecha de Lanzamiento: 29 de Julio del 2016

Categoría: B

Serie de documento: 1

Año de publicación: 2016

Versión 0.1.0

Diagramado y Diseñado por el Departamento de Multimedia, OPTIC
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 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 departamento de Estandarización, Normativas y Auditoría Técnica, 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 organismos gubernamentales.

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

1. **Categoría A** (normas universales), para los aspectos normativos que aplican a todos los organismos gubernamentales.
2. **Categoría B** (normas para los departamentos de TIC), para aquellas normas necesarias y exclusivas a la efectiva gestión de los departamentos o áreas de TIC, dentro de los distintos organismos del Estado Dominicano.

3. **Categoría C** (normas municipales), para las normas que aplican a las iniciativas de TIC en los ayuntamientos o municipios.
4. **Categoría D** (normas para embajadas), para las normas que aplican únicamente a las iniciativas de TIC de las embajadas, consulados o misiones en el extranjero.
5. **Categoría E** (normas especiales), para las normas que aplican a organismos gubernamentales con características específicas dependiendo de sus funciones y estructura orgánica, así como para iniciativas, proyectos o programas de Gobierno, en el cual se haga uso de las TIC.

De modo, que esta Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano, por tener un alcance para los departamentos de TIC, pertenece a la categoría B; mientras que por ser la primera NORTIC elaborada en esta categoría, su denominación sería NORTIC B1:2016, 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 B1-1:2016, 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 para garantizar la Administración de Infraestructuras Tecnológicas del Estado Dominicano en las plataformas y los procesos tecnológicos que son implementados por los 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 personales, esta norma se ampara en la propia **Constitución de la República Dominicana** del 26 de enero de 2010.

- **Artículo 44.-** Derecho a la intimidad y el honor personal. Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto:
    - Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.

- Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley.
- El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley.

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

- **Artículo l.-** Objeto de la Ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de la información y comunicación, y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de estos, las transacciones y acuerdos comerciales o de cualquier otra índole que se llevan a cabo por su medio y la confidencialidad de estos, son todos bienes jurídicos protegidos.

4. La **Ley No. 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.
5. La **Ley No. 126-02** sobre Comercio Electrónico, Documentos y Firma Digital.
6. La **Ley 65-00** sobre Derecho de Autor.
    - **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 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;
7. El **Decreto No. 229-07**, el cual es el instructivo de aplicación de Gobierno Electrónico, contentivo de las pautas generales para el desarrollo de la Estrategia de Gobierno Electrónico en la República Dominicana.
8. El **Decreto No. 709-07** sobre las normas y estándares elaboradas por la OPTIC.

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

9. El **Decreto No. 615-07**, que Instruye a la OPTIC a coordinar el procedimiento para la elaboración de los inventarios respecto a los programas incorporados a las computadoras y su licenciamiento.

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

INTRODUCCIÓN

La Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano, establece la directrices que debe seguir cada organismo para la correcta implementación de la conectividad de su infraestructura, de modo que los mismos puedan aprovechar al máximo sus recursos tecnológicos con el aprovisionamiento de nuevas tecnologías que cumplan con los estándares de calidad y seguridad establecidos en esta normativa, permitiendo reducir los costos operacionales y de mantenimiento, obteniendo con esto la optimización de los recursos utilizados en los organismos gubernamentales.

El capítulo sobre planificación de la red[1] de datos, indica las etapas que deben cumplir los organismos para realizar una correcta planificación, estableciendo las estrategias para el levantamiento, estructuración y diseño, antes de ejecutar cualquier proceso para la implementación de una red, con el objetivo de garantizar la fiabilidad, seguridad y tolerancia a fallas en la misma.

El siguiente capítulo sobre diseño de la red de datos, contiene los lineamientos necesarios para la correcta elaboración del diseño de una red, abarcando los puntos de segmentación, flujo del tráfico y comportamiento de la red, así como también las directrices para la adquisición de equipos y nuevas tecnologías a implementar.

El capítulo IV sobre Implementación y Configuración de la Infraestructura TIC, presenta las directrices y los procesos para la implementación de una red, logrando estructurar, configurar y mantener la infraestructura TIC más eficiente, de modo que pueda ser funcional y sostenible en el tiempo.

[1] Conjunto de dispositivos y software interconectados en una estructura organizada por medio de otros dispositivos físicos a través del cual se intercambian datos.

Para el capítulo final sobre gestión y monitoreo de la infraestructura TIC, se establece los procesos de gestión y actividades de monitoreo en cada uno de los elementos, dando así, una información detallada del desempeño y funcionamiento de los dispositivos que en ella operan.

CAPÍTULO I

NORMA PARA LA IMPLEMENTACIÓN Y GESTIÓN DE LA CONECTIVIDAD EN EL ESTADO DOMINICANO

Esta norma indica las directrices y recomendaciones que debe seguir cada organismo del Gobierno dominicano para la implementación y el funcionamiento de la conectividad dentro del Estado, con el objetivo de mejorar la transferencia de información a los diferentes dispositivos y optimizar la gestión de la administración pública.

SECCIÓN 1.01. Alcance

Las directrices de esta norma deben ser aplicadas por todos los organismos pertenecientes al Poder Ejecutivo, ya sean Centralizados, Descentralizados, Embajadas, Consulados, Misiones en el extranjero y Municipios. Esto también para aquellas unidades de TIC que tengan o deseen implementar conectividad en base a las buenas prácticas en sus infraestructuras.

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 al Poder Legislativo, y al Poder Judicial, así como aquellos organismos 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.

SECCIÓN 1.02. Referencias normativas

Se utilizó el estándar ANSI/TIA 942 del Instituto Nacional Estadounidense de Estándares y la Asociación de Industria de Telecomunicaciones (ANSI/TIA, por sus siglas en inglés), sobre infraestructura y telecomunicaciones para el centro de datos , en conjunto con los estándares IEEE 802 e IEEE 803 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés), en la elaboración del tema sobre los centros de datos y su estructuración, siguiendo el sistema de certificación TIER, creado por el Uptime 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 (EIA, por sus siglas en inglés), denominado ANSI/TIA/EIA-568B.

La guía de diseño de Cisco se utilizó como base para la redacción del tema sobre el diseño de la red de datos. También se utilizó el ciclo de vida de la red, formalizado por Cisco y pautado en dicho documento, como referencia para la estructuración de los capítulos que componen la normativa.

SECCIÓN 1.03. Términos y definiciones

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

Los términos “Software”, “Aplicaciones” y “Programas” se utilizarán indistintamente. También cuando se utilice el término “Activos”, este se refiere tanto a los activos físicos como los activos de información.

En esta norma utilizará el término “Cifrado de unidad” por el término en inglés Bitlocker.

CAPÍTULO II

PLANIFICACIÓN DE LA RED DE DATOS

Este capítulo presenta las directrices que deben cumplir los organismos a la hora de realizar la planificación de la estructura de manera que le permita tomar en cuenta los aspectos requeridos para aprovechar los beneficios al reducir costos, incrementar la disponibilidad de la red, aumentar la agilidad de los servicios y acelerar el acceso a las aplicaciones.

SECCIÓN 2.01. Levantamiento de los requerimientos Técnicos

(a) Para nuevas implementaciones de una infraestructura tecnológica el organismo debe realizar un levantamiento de los requerimientos técnicos en una documentación que contenga las siguientes informaciones:

(i) Identificar y validar los requerimientos técnicos requeridos.

a) Para la planificación de los requisitos técnicos deben tomarse en cuenta los siguientes aspectos:

- Crecimiento de la red.
- Tipos de aplicaciones y el estándar del cableado.
- Esquema de redundancia que se utilizará tanto de equipos activos y pasivos.

(ii) Identificar y documentar las aplicaciones y servicios requeridos para el funcionamiento del organismo.

a) Deben identificarse las aplicaciones requeridas actualmente y las planificadas a implementar.

b) Debe determinarse la importancia de cada aplicación.

c) Deben determinarse las aplicaciones que requieren alta disponibilidad y alto ancho de banda.

(iii) Definir las metas organizacionales y técnicas del organismo.

(iv) Definir las posibles restricciones organizacionales y técnicas que pueda tener el organismo.

(b) Para mejoras a la infraestructura actual, el organismo debe realizar un levantamiento donde se arroje el estado actual de la red y el mismo debe especificar lo siguiente:

- Topología de red[2] utilizada.
- Tráfico real de la red.
- Recursos y dispositivos utilizados.
- Aplicaciones utilizadas.
- Plataformas de voz y video.
- Metodología utilizada para la seguridad de la red.
- Metodología y sistemas de gestión y administración de la red.

(c) El organismo debe planificar programas de capacitación continua al personal de la unidad de TIC que trabaje directamente con la infraestructura tecnológica, asegurándose de que dicho personal posea las capacidades y competencias necesarias para el mantenimiento de la misma.

SECCIÓN 2.02. Documentación

Con el objetivo de elaborar registros que permitan el control de los proyectos nuevos y los ya existentes relacionados con TIC, en esta sección se establecen parámetros para la documentación con la que debe contar todo organismo gubernamental.

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

Sub-sección 2.02.1. Documentación del proyecto

Antes de implementar o realizar alguna modificación a su infraestructura, los organismos gubernamentales deben contar con procesos, documentaciones y controles que permitan la correcta ejecución del proyecto a gestionar, de manera que el resultado final cumpla con los objetivos establicido, por lo que deben seguir las directrices que se describen a continuación:

(a) Los proyectos TIC en su fase 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.
- Código.
- Partes involucradas.
- Director del proyecto y su nivel de autoridad dentro del mismo.
- Descripción.
- Requisitos.
- Criterios de aceptación.
- Riesgos.
- Objetivo general
- Objetivos específicos.
- Resumen de hitos.
- 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:** Titular del organismo.

(ii) El acta de constitución debe estar aprobada y firmada por la persona encargada 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[3]). Los documentos mencionados anteriormente se detallan a continuación:

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

- Nombre.
- Código.
- 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 encargada 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 A. Diagrama de planificación de proyectos TIC**, y contener los siguientes componentes:

a) Una escala inicial, en donde se especifique el nombre del proyecto y el código.

b) Una escala intermedia, en la cual se muestren las principales partes o componentes del proyecto.

[3] Es una descomposición jerárquica, orientada al producto entregable del trabajo que será ejecutado por el equipo del proyecto, para lograr los objetivos del proyecto y crear los productos entregables requeridos.

c) 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.

d) 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 B. 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 especifiquen 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 del solicitante.
  - Lugar, fase o capa en donde se realizará el cambio.
  - Descripción.
  - Justificación.
  - Impacto.
  - Duración aproximada que tomará aplicar el cambio.
  - Nombre y firma de la persona encargada de la aprobación del cambio.
  - Resultado de la solicitud del cambio: aprobada, cancelada o pendiente.

(d) Deben 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 convenidas entre las partes.

Sub-sección 2.02.2. Documentación de la red

(a) Debe elaborarse un diagrama de la Red de Área Local[4] (LAN, por sus siglas en inglés), 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 y el ancho de banda de cada línea.
- Nombre de la interfaz física de los dispositivos.

(b) Debe realizarse una documentación del direccionamiento IP[5] de la red que contenga como mínimo los siguientes requerimientos:

- Subredes[6].
- Las VLAN[7].
- Direcciones IP asignadas y su máscara de red.
- Cantidad de equipos en el segmento de red.
- Código de los equipos.

[4] Es una red de datos con un alcance geográficamente limitado.

[5] Es un protocolo de comunicación que proporciona los medios necesarios para la transmisión de bloques de datos digitales desde el origen al destino a través de redes interconectadas.

[6] Conjunto de redes dependientes de una red principal

[7] Es una red interna virtual, que permite crear redes lógicas dentro de una misma red física.

- Paquete de direcciones IP públicas provistas por los Proveedores de Servicio de Internet (ISP[8], por sus siglas en inglés).

(c) Debe elaborarse un plan de distribución del cableado especificando las siguientes informaciones:

- **Lugar de conexión:** Este incluye la conexión de los Puntos de Distribución Central (MDF[9], por sus siglas en inglés) a los Puntos de Distribución Intermedios (IDF[10], 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 o conexión cruzada horizontal, y el número de puerto de conexión 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[11] o una Base de Datos de la Gestión de Configuración[12] (CMDB, por sus siglas en inglés), esta debe proveer toda la información antes descrita y cualquier otra de interés para el organismo gubernamental.

(e) La documentación debe incluir la topología lógica de la red.

(f) Debe documentarse cualquier otro aspecto que el organismo considere importante para el levantamiento del mismo.

[8] Empresa que provee conexión a Internet.

[9] 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.

[10] Es el área dentro de una LAN donde se distribuye todo el cableado de datos correspondiente a los usuarios.

[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 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.

SECCIÓN 2.03. Compras y Contrataciones

Las compras y contrataciones efectuadas por los organismos gubernamentales deben cumplir con la Ley número 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones con modificaciones de Ley número 449-06.

(a) Para realizar una compra dentro del departamento de TIC, debe elaborarse un documento de Solicitud de Propuesta (RFP[13], 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 Acuerdo de Niveles de Servicio [14] (SLA, por sus siglas en inglés) como se especifica en la **NORTIC A1:2014 subsección 2.03.2. Niveles de Servicio.**

(c) Para realizar una solicitud 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.

[13] Documento en donde se especifican todos los detalles de una propuesta para llevar a cabo un proyecto.

[14] 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.

- 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 la unidad de TIC, debe estar aprobado por la unidad de compras del organismo.

CAPÍTULO III

DISEÑO DE LA RED DE DATOS

Con el objetivo de hacer la estructura de red de los organismos gubernamentales más eficientes, estandarizadas y seguras, se establecen en este capítulo, los parámetros necesarios para que el diseño de la misma sea estructurado acorde a las mejores prácticas, haciendo posible cumplir con los objetivos planteados.

SECCIÓN 3.01. Diseño de la arquitectura de red

En esta sección se establecen todas las directrices necesarias para la correcta implementación de una arquitectura de la red del organismo, a fin de que la misma cumpla con estándares que no comprometan el rendimiento y seguridad de la información.

Sub-sección 3.01.1. Tipos de arquitectura de red

(a) Tomando como base el tamaño del organismo, su funcionalidad y su crecimiento futuro, los organismos deben diseñar su red de datos, tomando como referencia uno de los siguientes tipos de arquitecturas:

- En los organismos donde la red de datos opere solamente dentro la misma infraestructura TIC, el diseño debe estar basado en un modelo jerárquico de tres (3) capas, como se muestra en el **Anexo C. Modelo jerárquico de la arquitectura de red** y cumplir con lo especificado en la **Subsección 3.01.2 sobre arquitectura jerárquica o por capas.**
- En los organismos donde la red de datos opere fuera de la infraestructura TIC o se comunique con una red exterior, el diseño debe estar basado en un modelo modular y cumplir con lo especificado en la **Subsección 3.01.3 sobre arquitectura modular.**

(i) En los casos donde el organismo tenga diseñada e implementada la arquitectura de red, la misma debe cumplir con los siguientes criterios:

a) El diseño debe estar segmentado, de manera que permita la resolución rápida de problemas e incidentes.

b) El diseño debe ser flexible, permitiendo la eliminación o la inclusión de nuevas áreas, sin afectar las operaciones del organismo.

c) El diseño deber ser escalable y adaptable a las nuevas tecnologías y requerimientos del mercado.

d) El diseño debe ser elástico y manejable, permitiendo que los elementos de la red puedan aumentar o disminuir sus capacidades, según lo requiera el organismo.

Sub-sección 3.01.2. Arquitectura jerárquica o por capas

(a) El modelo de diseño jerárquico debe contar con una capa de núcleo y la misma debe cumplir, como mínimo, con las siguientes características:

(i) Proveer conmutación de alta velocidad.

(ii) Proveer confiabilidad y tolerancia a fallos.

(iii) Opción de escalabilidad, respecto al crecimiento de la infraestructura.

(iv) Impedir la sobre carga de la Unidad Central de procesamiento[15] (CPU, por sus siglas en inglés) debido a la manipulación de los paquetes, en procesos tales como:

a) Sistemas o técnicas de seguridad.

b) Clasificación de la Calidad en el Servicio (QoS[16], por sus siglas en inglés).

c) Cualquier otro proceso o política relacionada.

[15] Dispositivo central dedicado a la interpretación y ejecución de instrucciones en computadores.

[16] Hace referencia al rendimiento de una red telefónica o de computadoras.

(v) Debe contemplar como mínimo los siguientes requerimientos:

a) Soporte para líneas de enlace de Red de Área Amplia[17] (WAN, por sus siglas en inglés), tales como los especificados en la **Subsección 3.02.3 Diseño de la Red de Área Amplia (WAN).**

b) Conmutadores[18] de capa 2[19] y capa 3, que cumplan con lo especificado en la **subsección 4.02.2. Conmutadores.**

c) En el diseño debe presentarse gráficamente las conexiones físicas entre los equipos correspondientes.

(b) El modelo de diseño jerárquico debe contar con una capa de distribución.

(i) La capa de distribución debe cumplir como mínimo con las siguientes características:

a) Permitir la agregación de enlaces LAN.

b) Permitir las políticas de seguridad basadas en Nivel de Control de Acceso (ACL[20], por sus siglas en inglés).

c) Proveer enrutamiento entre las LAN del organismo, así como también entre las VLAN.

d) Proveer un límite para la agregación y sumarización de rutas hacia la capa de núcleo.

e) Permitir la aplicación de QoS.

f) Proveer soporte para las VLAN.

(ii) Debe contemplar como mínimo los siguientes requerimientos:

a) Conmutadores de capa 2 que cumplan con lo especificado en la **subsección 4.02.2. Conmutadores.**

[17] Red de computadoras que une múltiples redes LAN.

[18] También conocido como switch, son dispositivos utilizados para conectar dos o más segmentos de redes.

[19] 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.

[20] Es una lista de control que filtra el tráfico de la red mediante la especificación los derechos de accesos autorizados, denegados o auditados para un elemento de confianza.

b) Los conmutadores deben enviar el tráfico de la red[21] hacia la capa de acceso.

(c) El modelo de diseño jerárquico debe contar con una capa de acceso.

(i) La capa de acceso debe cumplir como mínimo con las siguientes características:

a) Proveer conexión entre las estaciones de trabajo y servidores de red.

b) Brindar conmutación de capa 2.

c) Proveer alta disponibilidad de operación.

d) Soportar seguridad de puertos.

e) Proveer clasificación del QoS y creación de rutas redundantes y confiables.

f) Soporte para la inspección mediante el Protocolo de Resolución de Direcciones (ARP[22], por sus siglas en inglés).

g) Proveer ACL.

h) Permitir la utilización del Protocolo de Árbol Expandido (STP[23], por sus siglas en inglés).

(ii) Debe contemplar como mínimo los siguientes requerimientos:

a) Filtrado de direcciones de Cotrol de Acceso al Medio[24] (MAC, por sus siglas en inglés).

b) Segmentos de red separados mediante dominios de colisión.

c) Uso del ancho de banda compartido.

d) Utilización del balanceo de cargas.

[21] Cantidad de datos enviados y recibidos por los usuarios de una red.

[22] Protocolo de comunicaciones que opera en la capa de red encargado de resolver la dirección de acceso al medio correspondiente a una determinada dirección IP.

[23] Protocolo de red que opera en el nivel dos (2) del modelo OSI para gestionar la detección de bucles en topologías provocados por enlaces redundantes.

[24] Es el conjunto de mecanismos y protocolos de comunicaciones a través de los cuales varios "interlocutores" (dispositivos en una red, como computadoras, teléfonos móviles, etcétera) se ponen de acuerdo para compartir un medio de transmisión común (por lo general, un cable eléctrico o fibra óptica, o en comunicaciones inalámbricas el rango de frecuencias asignado a su sistema).

(d) En los casos de los organismos que, por su estructura, tamaño o recursos, no puedan tener un diseño basado en un modelo de 3 capas, debe utilizarse un modelo de 2 capas que cumpla con lo siguiente:

(i) La capa de núcleo y la capa de distribución deben estar unificadas y cumplir con los criterios mencionados anteriormente.

(ii) La capa de acceso debe estar presente y cumplir con los criterios mencionados anteriormente.

Sub-sección 3.01.3. Arquitectura modular

(a) La arquitectura modular debe contar con un bloque de distribución central, donde se encuentren todos los dispositivos principales de transmisión y comunicación de la red de datos y cumplir con lo especificado en la **Subsección 3.01.2. directriz (b) y directriz (c).**

(b) Debe contar con un bloque de servicios, donde estén identificados todos los servicios que se proveen a nivel de la red datos y la infraestructura TIC, como son:

- Controles de accesos inalámbricos.
- Servicios de comunicación unificada.
- Servicios de políticas para las puertas de enlace.
- Cualquier otro servicio relacionado.

(c) Debe contar con un bloque dedicado al centro de datos, responsable de la gestión y mantenimiento de todos los datos del sistema procesados por el organismo, como son:

- Datos financieros.
- Datos propios del sistema.
- Datos del personal.
- Y cualquier otro dato o información importante o sensitiva para el organismo, como se especifica en la **NORTIC A7:2016, Capítulo II, Administración y Tratamiento de la Información.**

(d) Debe contar con un bloque dedicado a las conexiones de Internet o enlaces WAN, responsable de la conectividad a nivel de voz, datos, video y cualquier servicio hacia fuera del organismo.

- Este debe cumplir con lo especificado en la **directriz 3.01.2.a.**

SECCIÓN 3.02. Diseño de la red de datos

En esta sección se establecen directrices para el diseño de la red del organismo con la finalidad de satisfacer las necesidades de conectividad existentes mediante parámetros generales y específicos dependiendo del tipo de red a diseñar. Dependiendo del tamaño, uso de datos, personal y otros factores, la red a diseñar para el organismo variará entre LAN, WLAN[25] y WAN.

(a) La topología de la red de datos de los organismos debe estar estructurada como se establece en la **directriz 3.02.1.e sobre topologías de red.**

(b) La red de datos debe contar con un diseño lógico de su topología, el cual permita la rápida identificación de los diferentes segmentos de red y direccionamiento.

(c) El diseño lógico debe contener las siguientes informaciones:

(i) Deben identificarse los dispositivos conectados a la red de datos.

(ii) Deben identificarse los puertos utilizados o a utilizar de los dispositivos.

(iii) Debe especificarse el esquema de direccionamiento, el cual debe cumplir con lo especificado en las siguientes directrices:

a) Todo direccionamiento de la red debe estructurarse en base a una de estas clases de direcciones IP privadas:

- 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.

[25] 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.

- 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.

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

i) División de subredes como técnica de direccionamiento de la red.

ii) Máscaras de subred de tamaño Variable (VLSM, por sus siglas en inglés) como solución de direccionamiento y reducir el desperdicio de direcciones IP.

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

iv) Cualquier otro que se considere necesario.

c) En caso de que el organismo implemente direccionamiento IPv6, este debe contemplarse dentro del esquema.

i) Para el direccionamiento en IPv6, el tamaño del prefijo a utilizar debe ser de acuerdo al tamaño del organismo y el mismo debe cumplir con los siguientes lineamientos básicos:

- Prefijos diferentes para la infraestructura interna y pública.
- Prefijos diferentes para enlace punto a punto y servicios como DNS, correo entre otros.

(iv) Debe especificarse el tipo de protocolo de enrutamiento a usar, el cual debe cumplir con lo especificado en la **subsección 4.01.4 sobre protocolos de red.**

(v) Deben especificarse las VLAN y su direccionamiento, así como los puertos asignados.

(d) La red de datos debe contar con un diseño físico de su topología, en el cual se muestre la localización física de los dispositivos, puertos configurados e instalación del cableado, y cumplir con lo especificado en la **sección 4.01. Cableado estructurado.**

(i) Deben identificarse los cuartos de telecomunicaciones como los IDF y MDF.

(ii) Debe identificarse el cableado principal de conexión, así como el cable secundario horizontal.

(iii) Debe identificarse cualquier otro lugar de conexión o de localización de equipos que sea necesario.

(iv) El diseño físico debe contar como mínimo con los siguientes elementos:

a) Debe contar con dispositivos finales tales como:

i) Computadores.

- Estaciones de trabajo.
- Computadoras portátiles.
- Servidores de archivos.
- Servidores web.
- Y cualquier otro equipo necesitado por el organismo.

ii) Impresoras de red.

iii) Teléfonos de Voz sobre IP[26] (VoIP, por sus siglas en inglés) .

iv) Cámaras de seguridad IP.

v) Dispositivos móviles.

vi) Y cualquier otro equipo final necesitado por el organismo.

b) Debe contar con dispositivos intermedios tales como:

[26] Son recursos que permiten que una señal de voz sea transmitida, a través de Internet, mediante el protocolo IP.

i) Dispositivos de acceso a la red.
   - Conmutadores.
   - Puntos de acceso inalámbricos.

ii) Dispositivos de red intermedios.
   - Enrutadores[27].

iii) Dispositivos de seguridad.
   - Cortafuegos[28].
   - IPS[29].
   - IDS[30].

iv) Y cualquier otro equipo intermedio necesitado por el organismo.

Sub-sección 3.02.1. Diseño de la Red de Área Local (LAN)

(a) Para fines de diseño de la LAN, el organismo debe evaluar las necesidades existentes, considerando las siguientes 3 (tres) variables:

- **Variables del entorno**, las cuales incluyen la ubicación de los dispositivos terminales, servidores y otros nodos[31] finales, el tráfico proyectado para el entorno y los costos proyectados de la entrega de diferentes niveles de servicios.
- **Variables de desempeño**, se refiere a la confiabilidad de la red, el rendimiento de tráfico, y las velocidades de computación cliente/servidor.
- **Variables de red**, las cuales incluyen la topología de red, capacidades de línea y tráfico de paquetes.

[27] También conocido como router, son dispositivos utilizados para crear e intercomunicar subredes de datos.

[28] También conocido como firewall, es un sistema que brinda protección contra la infiltración de intrusos a los recursos de una red, equipo o servicio.

[29] Software utilizado para evitar el acceso no autorizado a los sistemas computacionales de una red.

[30] Programa cuya función es detectar la presencia de accesos no autorizados a un computador o a la red.

[31] Hace referencia a un computador u ordenador conectado a una red de datos.

(b) Para el diseño de la LAN, debe realizarse un levantamiento con información sobre el organismo, en donde se establezcan los objetivos generales del mismo y los requerimientos técnicos necesarios para cumplir dichos objetivos:

(i) El levantamiento debe contener las siguientes informaciones:

- Información sobre el organismo.
- Objetivo general.
- Estructura organizacional.
- Estructura geográfica.
- Estructura del personal.
- Políticas.
- Información técnica.
- Desempeño.
- Aplicaciones.
- Administración.
- Seguridad.

(c) El organismo debe realizar un levantamiento sobre la red, el cual debe contener:

- Aplicaciones utilizadas.
- Protocolos de red.
- Identificación de los cuellos de botella potenciales que existan o puedan existir.
- Disponibilidad existente de la red.
- Herramientas de administración de red utilizadas.

(d) El diseño de la arquitectura de la LAN debe ir acorde a lo establecido en la **Subsección 3.01.1 Tipos de arquitectura de red.**

(e) El diseño de la LAN del organismo debe estructurarse en base a las siguientes topologías de red:

- **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.

(f) El diseño de la LAN debe estar segmentado de manera que permita la resolución rápida de problemas e incidentes.

(g) Toda documentación debe realizarse en base a las directrices especificadas en la **sección 2.02.1 Documentación del proyecto.**

Sub-sección 3.02.2. Diseño de la Red Local Inalámbrica (WLAN)

(a) El organismo debe identificar en el diseño de la WLAN las áreas que tendrán acceso a los recursos de red de manera inalámbrica.

(i) El organismo debe contemplar el uso de puntos de acceso inalámbricos o cualquier otro dispositivo de red que preserve el QoS dentro del área de servicio establecida.

(ii) El diseño de la WLAN debe asegurar la disponibilidad de la red para el usuario al trasladarse dentro de un Conjunto de Servicio Básico[32] (BSS, por sus siglas en inglés).

(iii) El usuario debe tener disponibilidad de la red al trasladarse entre los distintos BSS dentro del Conjunto de Servicio Extendido[33] (ESS, por sus siglas en inglés).

(b) En el diseño de la WLAN deben contemplarse las medidas de seguridad a implementar en dicha red. **Ver subsección 5.01.4 Gestión de la Red de Área Local Inalámbrica (WLAN).**

(c) El diseño de la WLAN debe proveer funcionalidad para las Zonas Desmilitarizadas[34] (DMZ, por sus siglas en inglés), el protocolo de Autenticación Remota para Servicios de Marcado a Usuarios[35] (RADIUS, por sus siglas en inglés) y el Protocolo de Configuración Dinámica de Host[36] (DHCP, por sus siglas en inglés).

[32] Grupo de estaciones que se intercomunican entre ellas.

[33] Conjunto de uno o más BSS que funcionan como un único BSS para la capa lógica de red (N2 LLC).

[34] 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.

[35] Es la implementación de Microsoft de un servidor de servicio de usuario de acceso telefónico de autenticación remota (RADIUS) y el proxy.

[36] Es un protocolo de red, el cual permite a los ordenadores obtener una dirección IP de manera automática, así como otros parámetros de configuración.

(d) La WLAN debe estar en una subred diferente a las demás redes y con segmentación del tráfico.

(e) Los dispositivos utilizados en la WLAN deben estar bajo el estándar IEEE 802.11[37].

(i) El organismo debe seleccionar la versión del estándar que mejor se ajuste a las necesidades determinadas como se especifica en el **Anexo D. Estándares para redes inalámbricas.**

Sub-sección 3.02.3. Diseño de la Red de Área Amplia (WAN)

(a) Para el diseño de la WAN el organismo debe tomar en cuenta las variables especificadas para el diseño de la LAN y la documentación realizada en la **subsección 3.02.1 Diseño de la Red de Área Local (LAN).**

(b) Para la selección de la arquitectura de la WAN, el organismo debe analizar los siguientes factores, los cuales le permitirán identificar los requerimientos a cubrir en el diseño de la WAN.

- Alta disponibilidad de la red.
- Soporte para el crecimiento de la red.
- Gastos operativos de la red.
- Complejidad de la operación de la red.
- Costo de implementación.
- Soporte de segmentación de la red.
- Soporte para voz y video.
- Cualquier otro factor que el organismo considere necesario.

(c) Para el diseño de la WAN, el organismo debe seleccionar el tipo de tecnología para utilizar en su estructura que más se ajuste a sus requisitos técnicos.

- Conmutación de circuito, para conexiones de datos que se puedan iniciar y terminar cuando sea necesario.

[37] Es una norma de la IEEE para el control de acceso a la red mediante el uso de puertos de comunicación.

- Módem análogo.
- Red Digital de Servicios Integrados[38] (ISDN, por sus siglas en inglés).
- Línea de Suscripción Digital[39] (DSL, por sus siglas en inglés).

- Líneas dedicadas, para cuando el organismo requiera conexiones dedicadas permanentes.
- Metro Ethernet.
- Tecnologías Inalámbricas.
  - WiMAX.
  - Enlaces Inalámbricos.
  - Antenas propias.

(d) El organismo debe diseñar, para protocolos específicos, los siguientes puntos:

- Lista de acceso.
- Encriptación.
- Servicios de proxy.
- Compresión.
- Encolamiento[40].

(e) El organismo debe planificar, seleccionar e incluir en el diseño el modelo de redundancia que utilizará para aumentar la fiabilidad y asegurar la alta disponibilidad de la WAN.

(i) El organismo debe seleccionar la opción que más se ajuste a sus necesidades para la redundancia de la WAN:

- Dial de copia de seguridad.
- Circuito Virtual Permanente de respaldo.
- Tunnel segurida IP[41] (IPSec, por sus siglas en inglés) a través de Internet.

[38] Red que facilita conexiones digitales de extremo a extremo y que proporciona una amplia variedad de servicios, los cuales son accedidos por los usuarios a través de un conjunto de interfaces normalizados. Entrega de los servicios críticos por múltiples vías para evitar que la caída de uno afecte la calidad del servicio.

[39] Es una familia de tecnologías que proporcionan el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica local. Es un término utilizado para referirse de forma global a todas las

[40] Representan los distintos estados de los mensajes en el servidor al pasar por el motor de transporte.

[41] Es un conjunto de protocolos que proporcionan seguridad al protocolo IP en cuanto a la autenticación y cifrado de los datos.

SECCIÓN 3.03. Diseño de la red del centro de datos

En esta sección se establecen los parámetros para el diseño de la red del centro de datos de los organismos gubernamentales con la finalidad de aumentar la disponibilidad y calidad de los sistemas utilizados. Al mismo tiempo también busca la reducción de costos, fallos, inconsistencias y cualquier otro inconveniente que afecte de manera negativa el rendimiento de la infraestructura tecnológica del organismo. Entre las directrices establecidas, se cuenta con políticas de seguridad para la protección de los activos, así como también el establecimiento de topologías y cableado para la preservación del QoS.

Sub-sección 3.03.1. Topología del centro de datos

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

(b) Debe contar con un Cuarto de Entrada[42] (ER, por sus siglas en inglés) para la conexión del proveedor del servicio.

(c) Debe contar con un Área Central de Distribución[43] (MDA, por sus siglas en inglés) para la conexión del cableado Cruzado Principal (MC, por sus siglas en inglés).

(d) Debe contar con un Área Horizontal de Distribución[44] (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[45] (ZDA, por sus siglas en inglés) para el punto de consolidación.

(f) Debe contar con un Área de Distribución de Equipos (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.

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

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

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

[45] Es un área donde se distribuye el cableado proveniente de la MDA.

Sub-sección 3.03.2. Cableado del centro de datos

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

- **(i)** Contar con un cableado horizontal desde el HDA a una entrada en el EDA o ZDA.
- **(ii)** El tipo de cable a utilizar debe tener las especificaciones indicadas en la **sección 4.01 sobre cableado estructurado.**
- **(iii)** La distribución del cableado debe ser mediante bandejas o canaletas que posean las diferentes divisiones, tanto para cableado de Par Trenzado sin Blindaje[46] (UTP, por sus siglas en inglés), 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.
- **(v)** El cableado horizontal principal de las áreas de distribución para los conmutadores de cableado horizontal debe tener fibra o par metálico redundantes.

Sub-sección 3.03.3. Diseño físico y ambiental del centro de dato

(a) Para el diseño del centro de datos deben tomarse en cuenta los siguientes factores físicos y ambientales:

- **(i)** La altura mínima del centro de datos debe ser de 3 (tres) metros sobre piso elevado y no menor de 60 (sesenta) centímetros entre el techo y el equipo más alto.
- **(ii)** El tamaño de la puerta debe ser igual o superior a 1 metro de ancho y 2.13 metros de alto.
  - **a)** La puerta debe abrir hacia fuera y mantenerse cerrada bajo el sistema de seguridad que desee implementar el organismo.
- **(iii)** Para el diseño de la ubicación de los Racks y gabinetes[47] deben seguirse las directrices a continuación:

[46] Es un tipo de cable de par trenzado utilizado para las telecomunicaciones. El trenzado de estos cables anula las interferencias de fuentes externas.

[47] Es la caja o lugar donde se alojan todos los componentes internos del computador. Su función es la de proteger los componentes del computador.

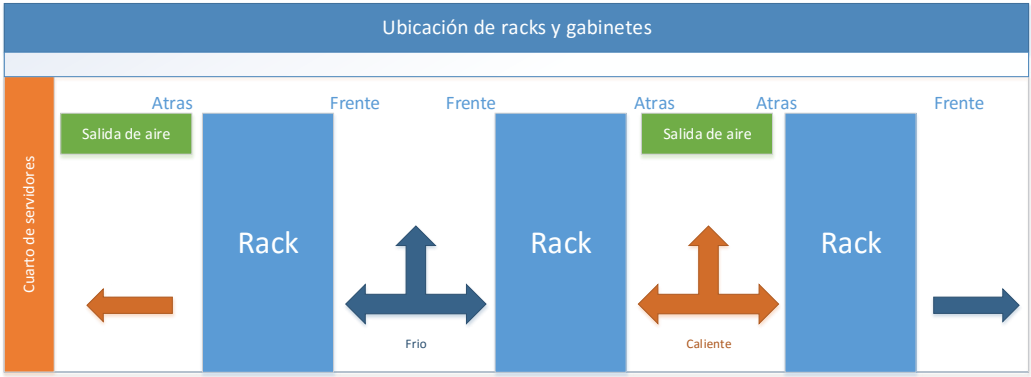
(iv) Los racks y gabinetes deben colocarse en líneas y de manera alternada formando líneas donde estén posicionados de manera frontal y reversa para la creación de pasillos fríos y calientes. **Ver figura No. 1. Ubicación de racks y gabinetes.**

a) Todos los racks y gabinetes deben tener identificada su parte frontal y trasera.

b) Los gabinetes deben contar, como mínimo, con 90 (noventa) centímetros de espacio de trabajo libre alrededor de los equipos y paneles de telecomunicaciones.

i) La distancia de 90 (noventa) centímetros para el espacio de trabajo debe medirse a partir de la superficie más salida del gabinete.

Figura No. 1 Ubicación de racks y gabinetes



(v) Debe tener sistemas de aire acondicionado que cumpla con las capacidades para suplir la climatización del centro de datos.

a) Los sistemas de aire acondicionado deben ser proyectados para la operación continua 7 días/ 24 horas /365 días del año e incorporar un mínimo de redundancia N+1.

b) La temperatura debe estar entre 20 y 25 grados Celsius.

(vi) Debe tener un sistema de reducción de oxígeno.

(vii) Debe tener un sistema de extinguidores automático.

(viii) La ubicación del centro de datos y sus componentes no deben estar visibles o accesibles al público.

(ix) El centro de datos debe tener un sistema de detección de incendios, y a la vez tener redundancia del mismo.

(x) El centro de datos debe tener un sistema de alimentación aislado de los demás departamentos del organismo; y el mismo debe tener redundancia.

(xi) El organismo debe tener medidas de seguridad como salidas de emergencia en casos de terremotos.

SECCIÓN 3.04. Adquisición de equipos y tecnologías

(a) Los dispositivos adquiridos deben contener catálogos y manuales donde se detallen las características y especificaciones del equipo, dicha documentación debe ser original.

(b) El organismo debe solicitarle al proveedor de los dispositivos una evaluación de preinstalación y pruebas de operatividad del equipo.

(c) El organismo debe solicitarle al proveedor los certificados de garantía de los dispositivos.

(d) Para los dispositivos que requieran mantenimiento periódico, el organismo debe solicitarle al proveedor un programa de mantenimiento preventivo y correctivo hasta finalizar la garantía de los mismos.

(e) El organismo debe solicitarle al proveedor un plazo de entrega de los dispositivos.

(f) Los sistemas de aire acondicionado deben tener la capacidad de controlar la humedad.

(g) Los sistemas de detección de incendios deben cumplir con los estándares de la Agencia Nacional de Protección contra Incendios[48] (NFPA, por sus siglas en inglés).

(h) Los equipos electrónicos deben estar certificados bajo el programa de Energy Star.

[48] Es reconocida alrededor del mundo como la fuente autoritativa principal de conocimientos técnicos, datos, y consejos para el consumidor sobre la problemática del fuego y la protección y prevención. Con sede en Quincy, Massachusetts, EE.UU., la NFPA es una organización internacional que desarrolla normas para proteger gente, su propiedad y el medio ambiente del fuego.

CAPÍTULO IV

IMPLEMENTACIÓN Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TIC

Este capítulo establece las directrices que deben seguir los organismos para la correcta implementación y configuración de la infraestructura TIC. El mismo tiene como finalidad pautar las mejores prácticas para la interconexión de los dispositivos utilizados, el método de etiquetado, la alimentación eléctrica, áreas físicas establecidas, protocolos y que las herramientas utilizadas sean las correctas.

SECCIÓN 4.01. Cableado estructurado

La estructuración del cableado para la interconexión entre dispositivos, tiene como objetivo servir de canal para la transferencia de datos entre dos o más computadores dentro de la red de datos. La interconexión fuera de la LAN es provista con ayuda de proveedores de servicios, y la interconexión a lo interno del organismo es responsabilidad del departamento de TIC, por lo que deben tenerse en cuenta las siguientes directrices:

(a) Debe existir un cuarto de entrada (ER) para la interconexión entre el cableado estructurado del organismo y el cableado que proviene de los proveedores.

- **(i)** Deben existir dos cajas de acceso de telecomunicaciones y dos caminos de entrada diferentes hasta el ER.
- **(ii)** Debe haber una separación como mínimo de 20 metros entre los dos caminos por todo el curso y que los mismos lleguen al ER por lados opuestos.

(b) El organismo debe contar con los servicios de por lo menos dos operadoras de telecomunicaciones.

(i) Para la contratación de las operadoras el organismo debe verificar que los cables de una misma operadora no presten servicios a la segunda, para evitar un punto único de falla.

(c) Todo el cableado debe estar centralizado en el MDF. **Ver Apartado 4.01.1.1 sobre estructuración del MDF.**

(d) Dependiendo la densidad del cableado, partiendo desde el MDF, deben existir IDF, los cuales distribuyen el cableado a otras zonas de la edificación o campus. **Ver Apartado 4.01.1.2 sobre estructuración del IDF.**

(e) Las canalizaciones horizontales[49] que vinculan las salas de telecomunicaciones con las áreas de trabajo, deben ser diseñadas para soportar los tipos de cables recomendados en la norma TIA-568[50], entre los que se incluyen el cable UTP de 4 pares, el cable Par Trenzado Blindado[51] (STP, por sus siglas en inglés) y la fibra óptica.

(f) Las canalizaciones horizontales deben cumplir con las siguientes directrices:

(i) No deben utilizarse ductos flexibles para las canalizaciones horizontales.

(ii) No debe existir tramos mayores a 30 metros sin puntos de registro e inspección.

(iii) No debe existir más de dos quiebres de 90 grados en cada tramo.

(iv) Cuando se utilicen ductos o bandejas sobre cielorraso para las canalizaciones horizontales estas deben cumplir con las siguientes directrices:

a) Solo deben ser utilizado cuando el acceso a estos sea sencillo.

[49] Corresponde al cableado que se extiende desde el punto cross-connect (en el área de distribución principal o MDA o en la de distribución horizontal) hasta la salida en el área de distribución de equipo activo.

[50] Conjunto de estándares de telecomunicaciones para el cableado utilizado para la interconexión de dispositivos en una red.

[51] Es un tipo de cable de par trenzado utilizado para las telecomunicaciones. En el trenzado de estos cables, cada par posee una pantalla protectora y es capaz de anular las interferencias de fuentes externas y además es resistente a altas temperaturas.

b) Las bandejas o ductos sobre cielorraso deben estar adecuadamente fijados al techo por medio de colgantes, nunca apoyados directamente sobre la estructura propia del cielorraso.

c) Los cables deben estar dentro del ducto o bandeja, no sobre la estructura del cielorraso.

(g) Para la selección del cableado deben tomarse en cuenta las características siguientes:

- El ciclo de vida del cableado.
- Ancho de banda soportado por el cableado.
- La aplicación y uso del cableado.
- La compatibilidad y crecimiento.

(h) Para la implementación del cableado debe tomarse en cuenta los siguientes criterios:

(i) Para el cableado en el interior del organismo debe utilizarse el cableado UTP.

(ii) Para el cableado en áreas desprotegidas o a la intemperie debe utilizarse el cableado STP para exteriores.

(iii) El cableado debe cumplir con el estándar TIA-568C.

(iv) El cableado debe ser etiquetado bajo el estándar TIA-606B[52]. **Ver subsección 4.01.2 sobre etiquetado.**

(i) Los tipos de cableado de fibra óptica que deben ser utilizado son los siguientes:

(i) Cable de fibra óptica multimodo[53] 62.5/125 micrones[54], 50/125 micrones, o algún otro superior, aprobado por el estándar ANSI/TIA/EIA-568-B.3.

[52] Estándar para el etiquetado de los componentes de un sistema.

[53] Es un tipo de fibra óptica mayormente utilizada en el ámbito de la comunicación en distancias cortas, como por ejemplo un edificio o un campus. Los enlaces multimodo típicos tienen un ratio de datos desde los 10 Mbit/s a los 10 Gbit/s en distancias de hasta 600 metros (2000 pies) más que suficiente para cumplir las premisas de distintas aplicaciones.

[54] Es la millonésima parte de un metro, y corresponde a una unidad de medida de longitud en el cableado de fibra óptica.

(ii) Cable de fibra óptica monomodo[55], certificado bajo el estándar ANSI/TIA/EIA-568-B.

(j) Si la longitud del segmento de red[56] de datos es igual o menor a 100 metros, debe utilizarse la configuración en base a:

- 100BASE-T[57], para Fast Ethernet[58] sobre UTP.
- 1000BASE-T[59], para Gigabyte Ethernet sobre UTP.

(k) Si la longitud máxima del segmento es de 550 metros, debe utilizarse Gigabit Ethernet[60] 1000BASE-LX[61].

(l) Si la longitud máxima del segmento es de 220 metros, debe utilizarse Gigabit Ethernet 1000BASE- SX[62] 62.5 de micrones.

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

- 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.

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

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

- Para UTP:

[55] Es un medio de transmisión, empleado habitualmente en redes de datos y telecomunicaciones, consiste en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

[56] Es la conexión que existe entre un dispositivo o computador y un equipo de la red datos como un conmutador o un enrutador.

[57] Es estándar para cables de par trenzado sin blindaje, utilizado para recorrer distancias no mayores a 100 metros a una velocidad de transmisión de 100 Mbps.

[58] También conocido como Ethernet de alta velocidad, es un conjunto de estándares de la IEEE para redes Ethernet con velocidades de 100 Mbps.

[59] 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.

[60] Es un estándar para los tipos de cables cuya velocidad de transmisión de datos es de 1,000 Mbps.

[61] Es un estándar para cables de fibra óptica que recorren una distancia menor a los 10 kilómetros.

[62] Es un estándar para cables de fibra óptica que recorren una distancia menor a los 550 kilómetros.

- Conector Registrado 45[63] (RJ-45, por sus siglas en inglés) para el cableado UTP.

- Para STP:
  - Conector Registrado 49[64] (RJ-49, por sus siglas en inglés) para el cableado STP.
- Para fibra óptica[65]:
  - Conector Cuadrado y el Conector Cuadrado Dúplex[66] (SC[67], por sus siglas en inglés).
  - Conector de Punta Recta (ST[68], por sus siglas en inglés).
  - Conector Lucent[69] (LC, por sus siglas en inglés).
  - Conector de Canal de Fibra[70] (FC, por sus siglas en inglés).
  - Conector de Interfaz[71] de Datos Distribuida por Fibra[72] (FDDI[73], por sus siglas en inglés).

[63] Es un conector utilizado en el cable UTP para establecer conexiones con los dispositivos de una red de datos.

[64] Es un conector modular de 8 posiciones y 8 contactos (8p8c) utilizado como terminal de cables de par trenzado blindados.

[65] Es un hilo de vidrio o plástico, por el cual se transmiten datos en forma de pulsos de luz.

[66] 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.

[67] 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.

[68] Conector de liberación rápida con sistema bayoneta. Es el conector más común para las fibras multimodo.

[69] Es un conector para cable de fibra óptica utilizado para transmisiones de datos de alta densidad.

[70] Es un tipo de conector para cables de fibra óptica utilizados en ambientes con altas vibraciones.

[71] Dispositivo capaz de transformar las señales generadas por un aparato en señales comprensibles por otro.

[72] Es un tipo de conector utilizado en redes de fibra óptica.

[73] Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida (WAN) o de área local (LAN), mediante cables de fibra óptica. Se basa en la arquitectura Token Ring y permite una comunicación tipo dúplex (completo). Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

Sub-sección 4.01.1. Estructuración del cuarto de telecomunicaciones

(a) Cada organismo debe contar con un cuarto de telecomunicaciones.

(b) El cuarto de telecomunicaciones no debe estar compartido con equipamientos de energía.

(c) El cuarto de telecomunicaciones debe contener un MDF y de acuerdo al tamaño de la arquitectura de red del organismo, uno o más IDF.

(d) El cuarto de telecomunicaciones debe contar con una fuente de climatización para mantener la temperatura constante.

- **(i)** La temperatura dentro de las salas de telecomunicaciones debe mantenerse entre 21 y 27 grados Celsius.
- **(ii)** El margen de humedad relativa debe estar comprendida entre 30% y 55%.

Apartado 4.01.1.1 Estructuración del MDF

(a) Para la estructuración del MDF deben seguirse las directrices a continuación:

- **(i)** El MDF debe ser diseñado para uso exclusivo de servicios de comunicaciones y el mismo no debe ser compartido con equipos que no cumplan un propósito en el cuarto.
- **(ii)** Dependiendo de la naturaleza y el tamaño del organismo solo será requerido un espacio destinado para estos fines.
- **(iii)** El MDF debe estar ubicado en un área de fácil acceso.
  - **a)** Debe estar ubicado en un área central que garantice la comunicación a todas las vías de comunicación de la infraestructura del organismo.
  - **b)** No deben existir dentro del MDF ningún tipo de tuberías portadoras de agua u otro líquido.
  - **c)** Debe evitarse ubicar el MDF adyacente a los elevadores, debajo de habitaciones con flujos de agua o que se consideren propensas a futuras filtraciones.

d) La puerta del MDF debe tener como mínimo una dimensión de 36 pulgadas de ancho y 84 pulgadas de alto.

i) Debe estar asegurada a través del sistema de control de acceso que el organismo haya implementado, permitiendo solo el acceso a personas autorizadas.

ii) La puerta del MDF debe comunicar directamente a un pasillo público, evitando que el personal deba cruzar por oficinas, almacenes u otros espacios para poder acceder al MDF.

iii) En caso de que el MDF se encuentre ubicado dentro una habitación mecánica o eléctrica más grande, el mismo debe estar dividido, asegurado y ventilado.

iv) El MDF debe contar con barra de puesta a tierra, las cuales deben estar conectadas al aterramiento del edificio.

v) El techo del MDF debe tener una altura mínima de 8 pies y 6 pulgadas.

vi) Dentro del MDF deben albergarse los componentes activos y pasivos de comunicación, como son:

- Enrutadores y conmutadores.
- Cortafuegos o cualquier otro equipo de seguridad.
- Central telefónica.
- Controladores de red.

Apartado 4.01.1.2 Estructuración del IDF

(a) El IDF debe ubicarse en un espacio libre y con mecanismos de seguridad.

(b) La construcción del IDF debe completarse antes de la instalación del cableado para comunicaciones.

Los IDF en pisos adyacentes deben posicionarse uno sobre el otro.

(c) Un mínimo de dos (2) conductos de cuatro (4) pulgadas resistentes al fuego deben conectar el IDF y el MDF.

(d) La puerta debe tener como mínimo 36 pulgadas de ancho y 84 pulgadas de alto.

(e) La puerta debe estar protegida bajo un sistema de control de acceso o en su defecto bajo llave.

(f) El techo debe tener como mínimo una altura de 8 pies y 6 pulgadas.

(g) El canal a tierra debe soportar hasta 100 amperes con un mínimo de cinco (5) puntos de terminación y conectado a la tierra del edificio.

(h) La habitación de telecomunicaciones debe contar con un sistema de Calefacción, Ventilación y Aire Acondicionado (HVAC, por sus siglas en inglés) para mantener una temperatura constante.

(i) La temperatura dentro de la habitación de telecomunicaciones debe permanecer entre 21 y 27 grados Celsius.

(j) Una de las paredes debe construirse en madera contrachapada resistente al fuego de 3/4 pulgadas.

(k) No debe haber conductos o equipos que desprendan agua o cualquier otro líquido en el cuarto del IDF.

(l) El piso que se encuentre justo encima del IDF debe prescindir de tuberías y equipos que puedan provocar inundaciones.

Sub-sección 4.01.2. Etiquetado

(a) Deben ser etiquetados e identificados todos los elementos o componentes de la red, como son:

- Terminales de cableado[74].
- Sistemas de terminación.
- Patch Panel[75].
- Cajas plásticas.
- Sistemas de tierra[76].

[74] Componentes ubicados en los extremos de un cable para conectarlos con un dispositivo final.

[75] Es un dispositivo en el cual se organizan las conexiones físicas de red.

[76] Es la desviación de toda energía eléctrica anormal a un punto común denominado tierra para que no afecte al equipo o al usuario.

- Gabinetes.
- Filas de gabinetes.
- Cuartos de comunicaciones.
- Paneles eléctricos.
- Escalerillas.
- Registros.
- Y cualquier otro identificado por el organismo.

(b) Deben utilizarse los siguientes componentes para el etiquetado de la red:

- Impresoras portátiles: Para etiquetas de vinil y etiqueta en componentes como escalerillas, registros Racks, entre otros.
- Impresoras estacionarias térmicas[77]: Para etiquetas en cableado, barras de tierra, paneles, entre otros.
- Material gastable: Consiste en el conjunto de etiquetas para cada solución incluyendo etiquetas con el color adecuado referente al código de colores definido en el estándar TIA 606B.
- Software de manejo de etiquetas: Este software tendrá como responsabilidad la gestión y control del sistema de etiquetado.

Sub-sección 4.01.3. Fuente de alimentación eléctrica, aterrizaje y sistema de protección

(a) Todas las instalaciones donde se utilice un servicio eléctrico, deben cumplir ciertos criterios de protección contra electrocución especificados en la normativa de la NFPA-NEC[78].

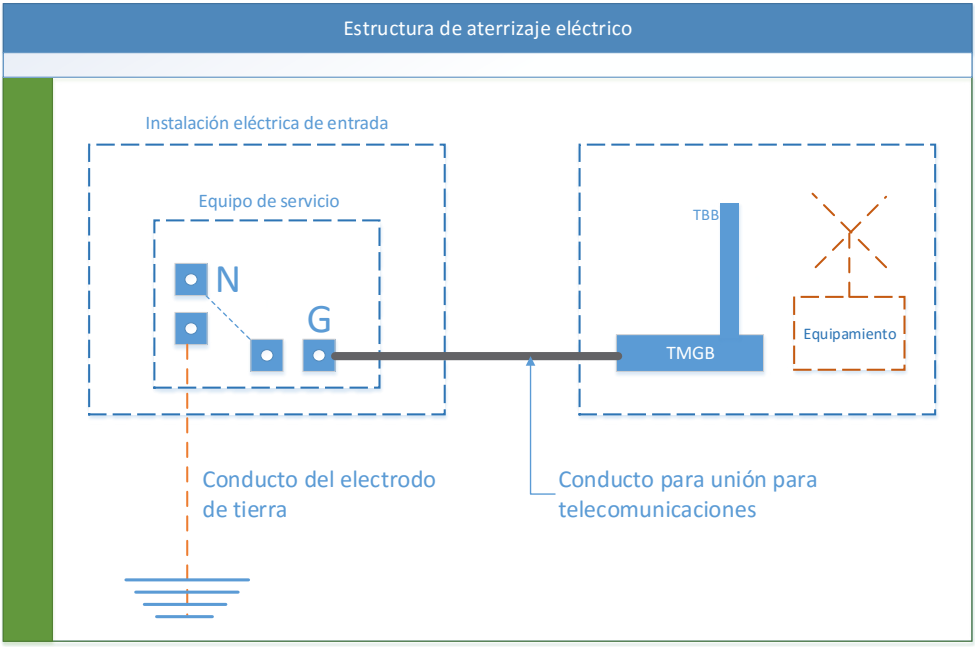
[77] La impresora térmica se basa en una serie de agujas calientes que van recorriendo el papel termosensible, que al contacto se vuelve de color negro.

[78] Es un estándar de los Estados Unidos para la instalación segura de cableado y equipos eléctricos

(b) Debe llevarse a tierra todos los componentes metálicos de los sistemas como se especifica en la **figura No. 2. Sobre el aterrizaje, tales como:**

- Registros.
- Gabinetes.
- Escalerillas.
- Tuberías.
- Herrajes de paredes falsas.
- Herrajes de cielos acústicos.

Figura No. 2 Sobre el aterrizaje



(c) Los aterramientos para los sistemas de telecomunicaciones que parten del aterramiento principal del edificio deben tener, desde este punto, un conductor de tierra para telecomunicaciones hasta la Barra Principal de Tierra para Telecomunicaciones (TMGB, por sus siglas en inglés).

(i) El conductor de tierra debe estar forrado, preferentemente de color verde.

(ii) Debe tener una sección mínima de 6 AWG.

(iii) Debe estar correctamente identificado mediante etiquetas adecuadas.

(iv) El conductor de tierra de telecomunicaciones no debe estar ubicado dentro de canalizaciones metálicas.

a) En caso de ser necesario alojarlo dentro de tuberías metálicas, estas deben estar conectadas al conductor de tierra en ambos extremos.

(d) La TMGB debe estar ubicada en las instalaciones de entrada, o en la sala de equipos.

(i) Debe ser una barra de cobre, con perforaciones roscadas según el estándar Asociación Nacional de Frabricantes Eléctronicos[79] (NEMA, por sus siglas en inglés).

(ii) Debe tener como mínimo 6 mm de espesor, 100 mm de ancho y largo adecuado para la cantidad de perforaciones roscadas necesarias para alojar a todos los cables que lleguen desde las otras barras de tierra de telecomunicaciones.

a) Para el ancho de la barra debe tomarse en cuenta futuros crecimientos.

(e) En la Sala de Equipos y en cada Sala de Telecomunicaciones debe ubicarse una Barra de Tierra para Telecomunicaciones (TGB, por sus siglas en inglés).

(i) Debe ser una barra de cobre, con perforaciones roscadas según el estándar NEMA.

(ii) Debe tener como mínimo 6 milímetros de espesor, 50 milímetros de ancho y largo adecuado para la cantidad de perforaciones roscadas necesarias para alojar a todos los cables que lleguen desde los equipos de telecomunicaciones cercanos y al cable de interconexión con TMGB.

a) Para el ancho de la barra debe tomarse en cuenta futuros crecimientos.

(f) Debe usarse supresores de picos para proteger los sistemas, debido

[79] Es la asociación de comercio más grande en los Estados Unidos la cual representa los intereses de los fabricantes de la industria eléctrica.

al redireccionamiento de descargas y sobre voltajes a tierra.

(g) El sistema de aterrizaje debe contar con los siguientes componentes:

(i) Debe contar con un sistema de alimentación ininterrumpida que garantice el correcto funcionamiento de la infraestructura de telecomunicaciones con el uso de un Sistema de Alimentación Ininterrupida (UPS, por sus siglas en inglés).

a) Deben existir módulos UPS redundantes para N+1.

(h) La capacidad y voltaje del sistema debe determinarse en base a los equipos de comunicación activo.

(i) La distribución eléctrica debe mantener siempre la disponibilidad para los equipos críticos.

Sub-sección 4.01.4. Protocolos de red

(a) Para los protocolos de red orientados a la administración debe utilizarse lo siguiente:

(i) El Protocolo de Descubrimiento de Capa de Enlace (LLDP[80], por sus siglas en inglés) para el intercambio de información de gestión y conectividad entre los sistemas de la red.

a) Este protocolo nunca debe configurarse de manera global en los enrutadores y conmutadores.

(ii) El Protocolo Simple de Administración de Red (SNMP[81], por sus siglas en inglés), para la administración de los dispositivos de red y el diagnóstico de problemas.

a) Este protocolo debe ser configurado en la versión 3, con las características de autenticación y encriptación.

(iii) Protocolo de Tiempo de Red (NTP[82], por siglas en inglés), para la sincronización del tiempo de los dispositivos de la red.

[80] Protocolo de la capa de enlace para la identificación de los dispositivos de red.

[81] Protocolo que opera en la capa de aplicación para facilitar la administración de los dispositivos de red.

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

a) Toda la infraestructura tecnológica debe tener la hora estandarizada en todos los equipos.

b) En los casos donde no se necesite la rigurosidad del NTP, puede utilizarse el Protocolo Simple de Tiempo de Red (SNTP[83], por sus siglas en inglés).

(iv) Tanto el SNMP y NTP debe habilitarse y configurarse a los siguientes activos:

- Los relojes de asistencia.
- Los controles de acceso.
- Los cortafuegos.
- Los enrutadoress /dispositivos inalámbricos.
- UPS.
- Sensores de temperaturas y humedad.

(v) En caso de que no se cuente con un servidor dedicado para NTP, el servidor designado debe ser el Controlador de Dominio Primario (PDC[84], por sus siglas en inglés) de la infraestructura de servidores.

a) Debe especificarse a todos los dispositivos de la infraestructura que el PDC es el NTP.

b) En los casos de las estaciones de trabajo y laptops debe especificarse el servidor NTP vía Política de Grupo (GPO[85], por sus siglas en inglés).

(vi) Para la administración remota debe habilitarse el protocolo Intérprete de Órdenes Seguro (SSH[86], por

[83] Es un protocolo de internet creado con el fin de sincronizar de manera simple los relojes de los sistemas informáticos que no requieran gran precisión.

[84] El controlador de dominio es el centro neurálgico de un dominio Windows, tal como un servidor Network Information Service (NIS) lo es del servicio de información de una red Unix.

[85] Conjunto de una o más políticas o reglas que controlan el uso de los elementos de un sistema.

[86] Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X (Sistema de Ventanas X) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows).

sus siglas en inglés), con llave Rivest, Shamir y Adleman [87] (RSA, por sus siglas en inglés). de 4096 bits para la administración remota de todos los equipos.

a) Debe deshabilitarse en todos los equipos de red el protocolo telnet[88].

(b) Para los protocolos de Vector Distancia deben cumplirse las siguientes directrices:

(i) El Protocolo de Enrutamiento de Gateway Interior Mejorado (EIGRP[89], por sus siglas en inglés), en las redes de organismos gubernamentales que requieran la implementación de este protocolo o aquellas que estén por implementarlo, deben cumplir las siguientes directrices:

a) En los enrutadores o dispositivos en donde este habilitado el protocolo EIGRP deben tener la última actualización del sistema operativo del fabricante.

b) Para el filtrado de rutas deben aplicarse mapas de rutas, listas de distribución, filtrado de prefijo o lista de perfiles de ruta.

c) Impedir las actualizaciones a través de las interfaces del enrutador.

d) Controlar la publicación de rutas en las actualizaciones de enrutamiento.

e) Controlar el proceso de actualizaciones de enrutamiento.

f) Aplicar autenticación para el protocolo de EIGRP entre todos los enrutadores que estén usando este protocolo para la nube de enrutadores.

g) Establecer tiempo de vida como medida de programación de control de intercambio de llaves.

(c) En los protocolos de estado de enlace deben cumplirse las siguientes directrices:

[87] Sistema criptográfico de clave pública utilizado para cifrar y firmar digitalmente.

[88] Es un protocolo que nos permite acceder remotamente a otro equipo mediante una terminal, es decir sin gráficos.

[89] Protocolo de encaminamiento que mide el vector distancia y es utilizado para los enlaces.

(i) El Protocolo de Gateway de Frontera (BGP[90], por sus siglas en inglés) en las redes de organismos gubernamentales que requieran la implementación de este protocolo o aquellas que estén por implementarlo debe cumplirse lo siguiente:

a) Deben estar actualizado en su última versión estable.

b) Cumplir con la IETF y las actualizaciones RFC 4893 y RFC 5398.

c) El número de Sistema Autónomo (AS, por sus siglas en inglés) que se aplicará en los enrutadores deber ser comprendido en el rango de 64,512 - 65,535.

d) Permitir la integración para enlaces redundantes en esquemas de BGP Externo (EBGP[91], por sus siglas en inglés) o de BGP Interno (IBGP[92], por sus siglas en inglés).

e) Permitir que la redundancia multihomed o de múltiples ISP se realice con ISP diferentes de diferentes compañías.

f) Hora sincronizada con el servidor NTP designado en la infraestructura TIC.

g) No debe utilizarse BGP en los siguientes casos:

i) En infraestructuras de una conexión a Internet.

ii) En enrutadores de borde donde los mismos cuenten con 1 GB de memoria RAM.

iii) Si el personal del organismo no cuenta con niveles de comprensión para aplicar filtrado de rutas, y proceso de selección de rutas en BGP.

[90] Protocolo para el intercambio de información de ruteo y encaminamiento entre sistemas autónomos.

[91] Protocolo utilizado para el intercambio de información entre distintos sistemas autónomos.

[92] Protocolo utilizado para el intercambio de información entre los distintos conmutadores dentro de un sistema autónomo.

(ii) Para la utilización del protocolo del Camino más Corto Primero (OSPF[93], por sus siglas en inglés) debe cumplirse con las siguientes directrices:

a) Debe aplicarse el filtrado de rutas, mapas de rutas, listas de distribución y filtrado de prefijo.

b) Los enrutadores u otros dispositivos que tengan habilitado el protocolo OSPF deben tener la última actualización del sistema operativo del fabricante.

c) La hora debe estar sincronizada con el sevidor interno NTP de la infraestructura.

d) Debe aplicarse contraseñas de 15 caracteres mínimo y cumplir con combinación de caracteres alfanuméricos.

e) Debe controlarse las actualizaciones de enrutamiento.

SECCIÓN 4.02. Dispositivos de red

Esta sección tiene como finalidad establecer los dispositivos a utilizar para la estructuración de la red y las características que estos deben cumplir para alcanzar los niveles necesarios de seguridad y confiabilidad, por esto se contemplan las siguientes directrices.

(a) El equipamiento de telecomunicaciones del centro de datos, así como el equipamiento de almacenaje deben tener módulos redundantes.

(b) Durante la instalación del hardware[94] en los servidores del organismo deben tomarse en cuenta las siguientes medidas de seguridad:

(i) Debe asegurarse de que el servidor no está conectado a la corriente cuando se están instalando dispositivos.

[93] 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.

[94] Se refiere a todas las partes físicas o tangibles de un sistema de información.

(ii) Debe usarse una pulsera antiestática ESD[95] para descargar la electricidad estática.

(iii) La pulsera antiestática debe conectarse entre la muñeca y una conexión a tierra.

(c) Para la selección del hardware en los servidores deben tomarse en cuenta los siguientes aspectos:

- La carga de usuarios.
- El tipo de hardware.
- El tipo de software.

(d) Para la identificación de los objetivos técnicos del hardware debe verificarse y documentarse que todos los controladores del hardware sean compatibles con el Sistema Operativo de Red (NOS[96], por sus siglas en inglés) elegido.

Sub-sección 4.02.1. Enrutadores

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

(i) Soportar mínimamente los siguientes protocolos:

- Protocolo de Información de Enrutamiento[97] (RIP, por sus siglas en inglés).
- Protocolo del Primer Camino Más Corto[98] (OSPF, por sus siglas en inglés).

(ii) Soporte para direccionamiento IPV4[99] e IPV6[100].

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

[95] Es una corriente eléctrica de corta duración, no repetitiva, que fluye entre 2 objetos cuando éstos entran en contacto, o cuando se aproximan a una distancia de unos pocos milímetros.

[96] Software que permite la interconexión entre ordenadores pertenecientes a una red y que estos puedan acceder a los recursos y servicios de la misma

[97] 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.

[98] 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.

[99] Es la cuarta versión del protocolo IP de 32 bits de longitud y fue la primera versión en ser implementada.

[100] Es la sexta versión del protocolo IP de 64 bit de longitud, con el fin de cubrir el agotamiento de las direcciones IPV4.

(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.

Sub-sección 4.02.2. Conmutadores

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

(i) Compatibilidad con los estándares del IEEE:

- IEEE 802. 1[101], para evitar el acceso no autorizado a la red de datos por medio de la capa 2[102].
- IEEE 802.3u[103] y superiores, como estándar para los medios Ethernet[104].

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

- SNMP.
- Protocolo de Red de Telecomunicación[105] (Telnet, por sus siglas en inglés).
- Protocolo SSH.

(iii) Protocolo de Transferencia de Hipertexto[106] (HTTP, por sus siglas en inglés). Luces que indiquen el estado del equipo, tales como:

- Encendido.
- Actividad de conexión.
- Conexión estable.

[101] Es una norma de la IEEE para el control de acceso a la red mediante el uso de puertos de comunicación.

[102] 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.

[103] Es un estándar de la IEEE para medios de transmisión Ethernet con velocidades de 100 Mbps.

[104] 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.

[105] Es una herramienta que nos permite acceder remotamente a otro equipo mediante una terminal, es decir sin gráficos.

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

- O 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.

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

(vii) Debe permitir la implementación de Red de Área Local Virtuales[107] (VLAN, por sus siglas en inglés).

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

Sub-sección 4.02.3. Dispositivos y sistemas de Seguridad en la Red

(a) El organismo debe tener sistemas y controles de seguridad para mantener un perímetro seguro de la infraestructura como se especifica en las siguientes directrices:

(i) El organismo debe tener un sistema de Circuito Cerrado de Televisión (CCTV[108], por sus siglas en inglés).

a) El organismo debe monitorear constantemente las áreas de entrada y salida de personal, así como visitantes y áreas más transitadas dentro y fuera del organismo.

(ii) Los enrutadores deben tener implementados un Sistema de Detección de Intrusos (IDS, por sus siglas en inglés).

(iii) Los enrutadores deben tener implementados un Sistema de Prevención de Intrusos (IPS, por sus siglas en inglés).

(iv) El organismo debe contar con cortafuegos y el mismo debe tener reglas que permitan la navegación de terminales a Internet por medio de autenticación de los siguientes tipos:

[107] Es una red interna virtual, que permite crear redes lógicas dentro de una misma red física.

[108] Es una tecnología de video vigilancia diseñada para supervisar una diversidad de ambientes y actividades.

- LDAPS.
- Kerberos[109].
- Autenticación Simple (SSO[110], por sus siglas en inglés).

a) El cortafuego debe soportar conectividad a través de Red Privada Virtual[111] (VPN, por sus siglas en inglés).

(v) Cuando el organismo utilice Gestión Unificada de Amenazas (UTM[112], por sus siglas en inglés), los mismos deben cumplir con las siguientes características:

- Filtro de URL.
- Inspección de contenido y protección contra ataques de Esteganografía[113].
- Inspección de Malware.
- Prevención de Pérdida de Datos (DLP[114], por sus siglas en inglés).
- IDS.
- IPS.

[109] Es un protocolo de seguridad creado por el Instituto Tecnológico de Massachussetts (MIT, por sus siglas en inglés) que usa una criptografía de claves simétricas para validar usuarios con los servicios de red, evitando así tener que enviar contraseñas a través de la red. Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

[110] Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

[111] Es una red virtual privada que permite de forma segura la interacción de datos sobre redes compartidas utilizando como vínculo el Internet.

[112] Es un término de seguridad de la información que se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red.

[113] Son ataques indetectables que se encuentran ocultos en portadores.

[114] También conocido como prevención de fuga de datos, consiste en el uso de estrategias y mecanismos para que la información sensible o crítica no sea enviada fuera de la red corporativa.

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[115], se describen las siguientes pautas que deben implementarse para una efectiva administración y configuración de esos servicios e infraestructura.

(a) Los organismos deben realizar el siguiente análisis de riesgo antes de migrar algún activo siguiendo la metodología indicada a continuación con el objetivo de determinar la viabilidad del movimiento a cualquiera de los modelos de nubes computacionales:

(i) Identificar y clasificar los activos que se desean migrar en los siguientes tipos:

- Datos
- Servicios
- Aplicaciones
- Funcionalidades
- Procesos

(ii) Para la migración de información a la nube debe cumplirse todos los aspectos de seguridad pautados en la NORTIC A7 2016, sección 6.04. Servicios en la nube.

Para esto el organismo puede responder las siguientes preguntas:

- *¿En qué forma se dañaría al organismo si el activo estuviera públicamente accesible y disponible?*
- *¿En qué forma se dañaría al organismo si un empleado del proveedor de Cloud accediera al activo?*
- *¿En qué forma se dañaría al organismo si el proceso fuera alterado por alguien externo?*
- *¿En qué forma se dañaría al organismo si el proceso o función no proporcionase los resultados esperados?*
- *¿En qué forma se dañaría al organismo si la información o los datos se alterasen de forma inesperada?*
- *¿En qué forma se dañaría al organismo si el activo no estuviera disponible durante un tiempo?*

[115] Es una tecnología que permite la utilización de servicios de cómputos por medio de Internet.

(iii) Debe identificarse el flujo de tráfico, datos y operaciones requerido para el activo que se considere migrar.

(iv) Debe realizarse una valoración de cuán importante son las operaciones y/o datos que se desea migrar para el organismo.

(v) El organismo debe determinar el modelo de despliegue que mejor se ajuste a sus necesidades y tenga el menor nivel de riesgo para el activo a migrar, el cual puede ser:

- Público.
- Privado, pero interno o en instalaciones propias.
- Privado, pero externo (incluyendo infraestructuras dedicadas o compartidas).
- Comunitarias, teniendo en cuenta la ubicación de las infraestructuras, potenciales proveedores el resto de los miembros de la comunidad.
- Híbrido, para evaluar con precisión esta opción debe tenerse en cuenta al menos una idea sobre la arquitectura que albergará los componentes, funciones y datos.

(vi) Al momento de seleccionar el modelo se servicio, el organismo debe tomar en cuenta el grado de control requerido.

a) El organismo debe establecer medidas de control de riesgo para el modelo de servicio seleccionado.

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

(i) Autoservicio bajo demanda[116], en el cual los organismos puedan solicitar recursos sin interacción con el proveedor.

(ii) Acceso a través de diferentes medios, permitiendo a los organismos acceder mediante cualquier dispositivo.

(iii) Agrupación de recursos, en el cual los recursos se encuentren agrupados en un lugar común para diferentes organismos.

[116] 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.

(iv) Elasticidad[117], en la cual los organismos puedan aumentar la capacidad de sus recursos de acuerdo a las necesidades.

(v) Medición del servicio, en donde el organismo pueda monitorear y controlar el uso de sus recursos.

(c) 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[118] (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.

(ii) Para una Plataforma como Servicio[119] (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.

[117] 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.

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

[119] 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.

(iii) Para un Software como Servicio[120] (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[121].

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

(d) 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[122], sobre técnicas de seguridad de la información y administración de sistemas. Certificada y auditada por la ISO[123].
- Controles de la Empresa de Servicios 1 y 2 (SOC 1, SOC 2, por sus siglas en inglés) junto con la Declaración sobre Normas de Auditoria 16 y el Estándar Internacional en Aseguramiento de Compromisos 340 (SSAE 16/ISAE, por sus siglas en inglés), para medir el control de las informaciones financieras de una organización o presa de servicios.
- Matriz de Control en la Nube[124] (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.

[120] 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.

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

[122] Es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

[123] Es una organización encargada de la creación de normas y estándares internacionales en diferentes áreas como tecnologías, seguridad, servicios, entre otros.

[124] 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

GESTIÓN Y MONITOREO DE LA INFRAESTRUCTURA TIC

Este capítulo establece los lineamientos necesarios para lograr efectiva gestión de las actividades que se realizan a la infraestructura TIC dentro del organismo, con la finalidad de crear un marco de gestión y monitoreo que garantice el desempeño y la continuidad de los sistemas.

SECCIÓN 5.01. Gestión de la red de datos

Esta sección establece todas las directrices necesarias para el control, administración y correcta implementación de la red del organismo gubernamental, a fin de mantener los controles necesarios para las redes internas y externas.

Sub-sección 5.01.1. Gestión de la red de datos de la infraestructura TIC

(a) Para la gestión de redes de datos de la infraestructura TIC, el proceso de gestión debe contar con lo siguiente:

- **(i)** La gestión de la red debe tener un soporte de tercer nivel[125] para todas las actividades relacionadas con la gestión, incluida la investigación de problemas mediante el uso de herramientas de software de gestión de red.
- **(ii)** Debe contar con la instalación y el uso de herramientas de análisis de paquetes que analicen el tráfico de la red, para ayudar en la resolución de problemas e incidentes.
- **(iii)** Debe contar con el mantenimiento y soporte de sistema operativo de red y software, incluyendo la gestión de parches y actualizaciones.

[125] Soporte de nivel experto en que se determinan con precisión problemas y soluciones.

(iv) Debe monitorearse el tráfico de red para identificar fallos o para detectar posibles cuellos de botella de rendimiento o problemas.

(v) La gestión de red debe contar con una supervisión y mantenimiento de sistemas de detección de intrusos como parte de la gestión de seguridad de la información. Este debe garantizar que no exista una denegación de servicio a los usuarios legítimos de la red.

(vi) Debe darse soporte para la conectividad remota a cuestiones como el acceso a la VPN y facilidades otorgadas a trabajadores remotos o proveedores.

Sub-sección 5.01.2. Gestión de la Red de Área Local y la Red de Área Local Virtual

(a) La gestión de la red LAN, debe tener sólo de una a tres Redes de Área Local Virtual (VLAN, por sus siglas en inglés) por módulo de acceso.

(b) Los enrutadores y puntos de acceso del organismo deben cumplir con las siguientes directrices:

(i) Los enrutadores deben soportar autenticación basados en el método hash[126].

(ii) El protocolo de administración debe ser por medio del Intérprete de Órdenes Seguro (SSH, por sus siglas en inglés) y su autenticación por medio de una contraseña con longitud de llave RSA de 2048 bits.

(c) Para la administración de los conmutadores debe tomarse en cuenta lo siguiente:

(i) El departamento de TIC debe tener la infraestructura de conmutadores segmentada por VLAN.

(ii) El departamento de TIC debe aplicar filtrado de dirección de Control de Acceso al Medio (MAC, por sus siglas en inglés) a las áreas del organismo que manipulen información confidencial o sensitiva. **Ver**

[126] Es un método de búsqueda que aumenta la velocidad de búsqueda, el cual no requiere que los elementos estén ordenados. Consiste en asignar a cada elemento un índice mediante una transformación del elemento. Esta correspondencia se realiza mediante una función de conversión, llamada función hash.

NORTIC A1:2014, Subsección 6.02.1. Administración de la información.

(iii) La VLAN de datos, voz, controles de accesos o cámaras de seguridad, no deben estar enrutadas entre sí.

a) En caso de que exista una sola terminal para la administración de las mismas, la conexión de esta terminal con las VLAN debe ser por dirección MAC.

(d) El protocolo de administración debe ser por medio de un SSH y su autenticación por medio de una contraseña con longitud de llave RSA de 2048 bits.

(e) La autenticación debe ser por medio de un servidor RADIUS o LDAPS.

(f) La autenticación no debe ser basada en texto plano.

(g) No debe utilizarse la VLAN 1 para todos los puertos no utilizados.

(h) Debe crearse una VLAN para asignar todos los puertos no utilizados.

(i) Debe separarse la VLAN de voz de la VLAN de datos.

(j) Debe crearse una VLAN y designarla como VLAN troncal, en caso que aplique.

(k) Debe separarse la VLAN de gestión de la VLAN trocal en los conmutadores.

(l) Debe utilizarse el estándar IEEE 802.1Q[127] en los enlaces troncales[128].

(m) Debe configurarse manualmente los puertos de acceso que no estén específicamente destinados a un enlace troncal.

(n) Sólo los protocolos de control de permisos deben ejecutarse en VLAN 1, como son:

- Protocolo Truncado Dinámico (DTP[129], por sus siglas en inglés).

[127] Fue un proyecto del grupo de trabajo 802 de IEEE para desarrollar un mecanismo que permita a múltiples redes interconectadas con puentes o conmutadores, compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio.

[128] Es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red.

[129] Protocolo propietario operativo en conmutadores Cisco utilizado para automatizar la configuración de truncado en enlaces Ethernet.

- Protocolo Truncado VLAN (VTP[130], por sus siglas en inglés).
- Protocolo de Árbol Expandido (STP, por sus siglas en inglés).
- Unidad de Datos del Protocolo de Puente (BPDU[131], por sus siglas en inglés).
- Protocolo de Agregación de Puertos (PAgP[132], por sus siglas en inglés).
- Protocolo de Control de Agregación (LACP[133], por sus siglas en inglés).
- Protocolo de Descubrimiento de la Capa de Enlace (LLDP, por sus siglas en inglés).
- Debe evitarse la gestión mediante Telnet y estar habilitado soporte SSH para la gestión de VLAN.

Sub-sección 5.01.3. Gestión de la Red de Área Extendida (WAN)

(a) Debe aplicarse la gestión de ancho banda dividiendo el tráfico de los usuarios del organismo, como también asignando ancho de banda a los servicios de correo electrónico en todos los casos que los servicios que se ofrecen requieran de la WAN.

(b) Deben utilizarse herramientas de gestión de monitoreo para los servicios de Internet.

(c) Debe supervisarse el tráfico de red en la WAN para identificar fallos o para detectar posibles cuellos de botella de rendimiento o problemas.

Sub-sección 5.01.4. Gestión de la Red de Área Local Inalámbrica (WLAN)

(a) Los enrutadores inalámbricos deben estar en una VLAN diferente a la VLAN del tráfico de los usuarios del organismo.

[130] Protocolo de mensaje utilizado para la configuración y administración de las VLAN.

[131] Tramas que contienen información del STP.

[132] Protocolo de Cisco utilizado para la agregación lógica y automatizada de puertos.

[133] Protocolo que maneja virtualmente los enlaces de la red para proveer un mejor ancho de banda y disponibilidad.

(b) El Identificador de Conjuntos de Servicios (SSID, por sus siglas en inglés) debe estar oculto.

(c) Debe supervisarse el tráfico de red en la WLAN para identificar fallos o para detectar posibles cuellos de botella de rendimiento o problemas.

(d) La gestión de los puntos de acceso y enrutadores inalámbricos debe ser a través de un controlador y este debe ser capaz de identificar fallos o detectar posibles cuellos de botella de rendimiento o problemas de seguridad.

(e) Deben implementarse medidas de seguridad a la red WLAN, las cuales deben cubrir como mínimo los siguientes puntos:

(i) Deben crearse ACL en los casos que sea necesario.

(ii) Los puntos de accesos inalámbricos deben estar implementados con IEEE 802.1X[134] y con servidor RADIUS como autenticación.

(iii) La infraestructura inalámbrica debe tener el tipo de autenticación de Acceso Inalámbrico Protegido 2[135] (WPA2, por sus siglas en inglés).

(iv) La infraestructura inalámbrica debe utilizar EAP-Autenticación Flexible vía Túnel Seguro[136] (EAP-FAST, por sus siglas en inglés) para autenticación segura.

Sub-sección 5.01.5. Gestión de la Red de Privada Virtual (VPN)

(a) Las redes VPN deben estar configuradas bajo los siguientes criterios:

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

- Protocolo Seguro de Internet (IPsec, por sus siglas en inglés).

[134] Es un estándar IEEE para un acceso de red autenticado a redes Ethernet por cable y redes 802.11 inalámbricas. IEEE 802.1X mejora la seguridad y la implementación al proporcionar la compatibilidad con la identificación de usuarios, la autenticación, la administración de claves dinámicas y la creación de cuentas de manera centralizada.

[135] Es un protocolo para la protección de las redes inalámbricas que utiliza la encriptación de datos.

[136] Es un protocolo de autentificación para acceso a redes.

- Capa de Conexión Segura (SSL[137], por sus siglas en inglés).
- Protocolo SSH.

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

- Algoritmo de Resumen del Mensaje[138] (MD5, por sus siglas en inglés).
- Algoritmo de Hash Seguro[139] (SHA, por sus siglas en inglés).

(iii) Debe tener un Algoritmo de Triple Encriptación de Datos[140](3DES, por sus siglas en inglés) de 256 bits y autenticación de dos factores[141].

SECCIÓN 5.02. Gestión del centro de datos y Servidores

(a) Para la correcta administración de los centros de datos, deben seguirse las directrices a continuación:

(i) El personal de la unidad de TIC debe tener contratos de confidencialidad sobre los datos o información que estos manipulen.

(ii) En caso de que el organismo opte por la contratación de terceros para el almacenamiento de la información, el proveedor debe entregar un SLA, el cual debe especificar su compromiso con salvaguardar la información.

(iii) La unidad de TIC debe asegurar la redundancia de su infraestructura para eventualidades o catástrofes. **Ver NORTIC A7:2016, Capítulo IV. Plan de disponibilidad y continuidad.**

[137] Es un protocolo de seguridad para conexiones de transmisión de información, el cual emplea autenticación y cifrado de datos.

[138] Es un algoritmo de cifrado que utiliza una codificación de 128 bits.

[139] Es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST).

[140] Es el término utilizado para proteger un objeto, archivo o acción por medio de un algoritmo matemático.

[141] Es una herramienta o proceso de autenticación que cumple la función de agregar una capa de seguridad adicional al proceso de inicio de sesión de un sistema o sitio web.

(iv) Deben existir políticas de privilegios dentro del departamento de TIC, específicamente el área de operaciones TIC, para que solo el personal autorizado pueda acceder a la infraestructura del organismo. **Ver NORTIC A7:2016, sección 3.02 controles de acceso a la infraestructura.**

(b) Para la correcta administración de los servidores dentro del centro de datos, deben seguirse las directrices a continuación:

(i) Debe darse soporte y mantenimiento al sistema operativo y el software utilitario instalado.

(ii) Deben crearse políticas de respaldo y restauración.

(iii) Deben gestionarse todas licencias para los sistemas instalados en los servidores, especialmente sistemas operativos, utilidades y cualquier software de aplicación.

a) Para los temas sobre el licenciamiento el organismo debe cumplir con las directrices especificadas en la **NORTIC A1, subsección 1.05.2 Licenciamiento.**

(iv) Deben aplicarse medidas de seguridad, incluyendo la identificación y aplicación de parches de seguridad, gestión de acceso y la detección de intrusiones.

(v) Debe realizarse un mantenimiento continuo, el cual incluya la sustitución de servidores antes de estos ser obsoletos para apoyar la evolución de los servicios.

(vi) Los servidores deben tener el cifrado de unidad activado desde el Sistema Básico de Entrada/Salida (BIOS[142], por sus siglas en inglés) para la encriptación de sus datos.

(vii) Los servidores de dominio deben tener habilitado el protocolo LDAPS.

(viii) Todas las estaciones de trabajo deben estar protegidas por políticas para ser accedidas solo por el personal autorizado.

(ix) Los servidores de la infraestructura, deben tener las últimas actualizaciones y parches de seguridad.

a) Antes de la implementación en ambientes de producción, esto debe pasar por un ambiente de pruebas.

[142] Es el primer sistema que se ejecuta en dispositivos informáticos para verificar su estado.

(x) Todos los servidores deben tener una solución de antivirus actualizada que aseguren la protección de la red, así como las estaciones de trabajo.

(xi) Los controles de acceso biométricos o de tarjetas de código que estén conectados a la infraestructura de la red, deben estar conectados mediante una VLAN separada del tráfico de usuarios.

SECCIÓN 5.03. Gestión del Servicio de Voz Sobre IP

(a) Para la correcta administración del servicio de voz sobre el Protocolo de Internet (IP, por sus siglas en inglés) deben tomarse en cuenta las siguientes directrices:

(i) El Ramal Privado de Conmutación Automática (PBX[143], por sus siglas en inglés), no debe tener acceso a Internet. En caso de que sea necesario para un personal específico, deben tomarse las siguientes pautas en cuenta:

a) La PBX, en caso de ser IP, debe estar separadas de la red de datos mediante VLAN; en caso de ser análogas, debe estar aislada de la red de datos sin acceso a Internet.

(b) La gestión de telefonía basada en redes IP en las instituciones debe tener un responsable de equipo o departamento.

SECCIÓN 5.04. Herramientas y Sistemas de Monitoreo

(a) Todos los componentes de la infraestructura de TIC deben ser monitoreados continuamente en conjunción con la gestión de eventos, de modo que los posibles problemas o las tendencias puedan ser identificadas antes de que se produzcan un fallo o cualquier evento de degradación de rendimiento.

(b) La vigilancia debe ser automatizada y la misma debe tener alertas periódicas con las acciones correctivas que permitan evitar que ocurra un impacto adverso en la infraestructura.

[143] Es cualquier central telefónica que gestione mediante líneas troncales las llamadas internas, así como también las externas, ya sean entrantes o salientes.

(c) El departamento de TIC debe tener un Software de Gestión de la Infraestructura del Centro de Datos (DCIM, por sus siglas en inglés) para su monitoreo y gestión.

(i) Esta herramienta debe ser capaz de brindar información sobre cada recurso del centro de datos, incluyendo las relaciones de la infraestructura y de toda la conectividad de la misma.

(d) El departamento de TIC debe disponer de un Centro de Control de la Red (NOC[144], por sus siglas en inglés), y que el mismo brinde servicios las 24 horas, 7 días de la semana, los 365 días del año.

(e) Los componentes y elementos identificados por el organismo que deben ser objeto de seguimiento y monitoreo, como mínimo debe evaluarse lo siguiente:

- La utilización de la Unidad Central de Procesamiento (CPU, por sus siglas en inglés).
- La utilización del almacén de archivos, tales como:
  - Discos duros[145].
  - Particiones.
  - Segmentos.
- El uso de las aplicaciones.
- La utilización de bases de datos[146].
- Tasas de transacción, tasas de error y reintentos.
- Los números de sistema/aplicación inicios de sesión y usuarios concurrentes.
- Los números de nodos de red en uso, y los niveles de utilización.

[144] Es un centro de operaciones de red que monitorea todo el ambiente de TIC de la empresa a fin de asegurar que el servicio de tecnología ofrecido, en todos los niveles, corresponda a lo necesario para las actividades de organización.

[145] Es un dispositivo para el almacenamiento de datos a través del magnetismo u óptica.

[146] Son un conjunto de datos almacenados de manera ordenada y que guardan relación entre ellos para su uso posterior.

SECCIÓN 5.05. Gestión de la configuración y operación de la red

(a) Para la correcta gestión de la red, deben mantenerse los registros de configuración a través del ciclo de vida de servicio y archivándolos según los acuerdos establecidos.

(b) Debe gestionarse la grabación, recuperación y consolidación del estado actual de las configuraciones, así como el estado de todas las configuraciones anteriores para confirmar la exactitud de la información, la puntualidad, la integridad y la seguridad.

(c) Debe garantizarse que los cambios a la configuración o a la operación de la red estén debidamente documentados.

- **(i)** Toda documentación debe estar realizada en base a las directrices especificadas en la s**ección 2.02.2. Documentación de la red.**

(d) La gestión de la infraestructura TIC debe estar organizada según lo estipulado en el Artículo 6. De la Resolución 51-2013 sobre los modelos de las estructuras de las unidades de TIC.

(e) Para la correcta operación de la infraestructura de TIC[147], debe contar mínimamente con:

- **(i)** Personal encargado de todos procesos de TIC, implementación de estrategias de servicios, aplicación de mejoras y cumplimiento de la calidad, y cualquier otra función expuesta en el Artículo 6. De la Resolución 51-2013 sobre los modelos de las estructuras de las unidades de TIC.
- **(ii)** Personal encargado de los servicios de TIC y cumplir con los roles expuestos en el Artículo 7 de la Resolución 51-2013 sobre los modelos de las estructuras de las unidades de TIC.
- **(iii)** Un personal encargado de las Operaciones TIC y cumplir con los roles expuestos en el Artículo 7 de la Resolución 51-2013 sobre los modelos de las estructuras de las unidades de TIC.

[147] Para fines de esta norma, hace referencia al conjunto de equipos y elementos en lo que se sustenta un organismo gubernamental.

a) Y cualquier otro personal necesario según el modelo de estructura organizacional de TIC dispuesto en el Artículo 8. De la Resolución 51-2013 sobre los modelos de las estructuras de las unidades de TIC.

SECCIÓN 5.06. Gestión de la Infraestructura de Red y las instalaciones

(a) La gestión de los edificios debe abarcar el mantenimiento y la conservación de las infraestructura que albergan el personal de TIC y el centro de datos, así como las actividades típicas incluyendo:

- La limpieza y eliminación de residuos.
- Los controles de acceso.

(b) Debe existir un sistema de acondicionamiento ambiental y sistemas de alerta, al igual que sistemas de detección de humo y supresión de incendios, agua y sistemas de calefacción.

(c) Para la correcta gestión de la infraestructura TIC dentro del organismo, deben seguirse las directrices a continuación:

(i) El organismo debe tener un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés), para su infraestructura física **(ver NORTIC A7:2016, Sección 4.02 Plan de continuidad)**, el cual debe contemplar planes de contingencia para casos como:

- Incendios.
- Derrame de agua.
- Terremotos.
- Deslizamientos de tierra.
- Tormenta (de vientos y eléctricas).
- Sabotaje.
- Explosiones.
- Colapso de la edificación.
- Desechos tóxicos.
- Fallos de los equipos.
- Pérdidas de personal (enfermedad, huelgas, acceso, transporte).

- Pérdida de servicio (alimentación eléctrica, enfriamiento, calefacción, sistema de aire, agua).
- Inundaciones.

(ii) La ubicación del centro de datos debe ser en un área restringida, la cual sea accedida solo por el personal autorizado. **Ver NORTIC A7:2016, Sección 3.02 Controles de acceso a la infraestructura.**

SECCIÓN 5.07. Recomendaciones

- Se recomienda el uso de software libre en la implementación de la infraestructura del organismo.
- Se recomienda que el organismo gubernamental tenga seguridad perimetral, y tome en cuenta lo siguiente para la misma:
  - Sistema de detección de intruso.
  - Detector de movimiento.
  - Sistema cerraduras electrónicas con combinaciones.
  - Lectores biométricos.
  - Tarjetas inteligentes.
- Se recomienda que todas las tareas de mantenimiento del centro de datos estén automatizadas.

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 metros.

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 distancia no mayor a 100 metros a una velocidad de transmisión de 100 Mbps.

Acceso WIFI Protegido 2 (WPA2)

Es un protocolo para la protección de las redes inalámbricas que utiliza la encriptación de datos.

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 Hash Seguro 1 (SHA1)

Es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST).

Algoritmo de Resumen del Mensaje (MD5)

Es un algoritmo de cifrado que utiliza una codificación de 128 bits.

ANSI/TIA/EIA-607

Discute el esquema básico y los componentes necesarios para proporcionar protección eléctrica a los usuarios e infraestructura de las telecomunicaciones mediante el empleo de un sistema de puesta a tierra adecuadamente configurado e instalado.

Área Central de Distribución (MDA)

Es donde se encuentra localizado el cableado cruzado principal.

Área de Zona de Distribución (ZDA)

Es un área donde se distribuye el cableado proveniente de la MDA.

Área de Distribución Horizontal (HDA)

Es el área donde se localiza el cableado cruzado horizontal.

Asociación Nacional de Fabricantes Eléctricos (NEMA)

Es la asociación de comercio más grande en los Estados Unidos la cual representa los intereses de los fabricantes de la industria eléctrica.

Asociación Nacional de Protección contra el Fuego (NFPA)

Es reconocida alrededor del mundo como la fuente autoritativa principal de conocimientos técnicos, datos, y consejos para el consumidor sobre la problemática del fuego y la protección y prevención. Con sede en Quincy, Massachusetts, EE.UU. La NFPA es una organización internacional que desarrolla normas para proteger personas, propiedades y el medio ambiente del fuego.

Ataques de Esteganografía

Son ataques indetectables que se encuentran ocultos en portadores.

Autenticación de dos factores

Es una herramienta o proceso de autenticación que cumple la función de agregar una capa de seguridad adicional al proceso de inicio de sesión de un sistema o sitio web.

Autenticación Remota para Servicios de Marcado a Usuarios (RADIUS)

Es la implementación de Microsoft de un servidor de servicio de usuario de acceso telefónico de autenticación remota (RADIUS) y el proxy.

Autenticación Simple (SSO)

Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

Bases de datos

Son un conjunto de datos almacenados de manera ordenada y que guardan relación entre ellos para su uso posterior.

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.

Cable de fibra óptica monomodo

Es un medio de transmisión, empleado habitualmente en redes de datos y telecomunicaciones, consiste en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Cable de fibra óptica multimodo

Es un tipo de fibra óptica mayormente utilizada en el ámbito de la comunicación en distancias cortas, como por ejemplo un edificio o un campus. Los enlaces multimodo típicos tienen un ratio de datos desde los 10 Mbit/s a los 10 Gbit/s en distancias de hasta 600 metros (2000 pies) más que suficiente para cumplir las premisas de distintas aplicaciones.

Calidad de servicio (QoS)

Hace referencia al rendimiento de una red telefónica o de computadoras.

Canalizaciones horizontales

Corresponde al cableado que se extiende desde el punto cross-connect (en el área de distribución principal o MDA o en la de distribución horizontal) hasta la salida en el área de distribución de equipo activo.

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.

Centro de Operaciones de Red (NOC)

Es un centro de operaciones de red que monitorea todo el ambiente de TIC de la empresa a fin de asegurar que el servicio de tecnología ofrecido, en todos los niveles, corresponda a lo necesario para las actividades de organización.

Circuito Cerrado de Televisión (CCTV)

Es una tecnología de video vigilancia diseñada para supervisar una diversidad de ambientes y actividades.

Código Eléctrico Nacional (NFPA-NEC)

Es un estándar de los Estados Unidos para la instalación segura de cableado y equipos eléctricos

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 Punta Recta (ST)

Conector de liberación rápida con sistema bayoneta. Es el conector más común para las fibras multimodo.

Conector Lucent (LC)

Es un conector para cable de fibra óptica utilizado para transmisiones de datos de alta densidad.

Conjunto de Servicio Básico

Grupo de estaciones que se intercomunican entre ellas.

Conjunto de Servicio Extendido (ESS)

Conjunto de uno o más BSS que funcionan como un único BSS para la capa lógica de red (N2 LLC).

Conmutadores

También conocido como switch, son dispositivos utilizados para conectar dos o más segmentos de redes.

Control de Acceso al Medio (MAC)

Es el conjunto de mecanismos y protocolos de comunicaciones a través de los cuales varios "interlocutores" (dispositivos en una red, como computadoras, teléfonos móviles, etcétera) se ponen de acuerdo para compartir un medio de transmisión común (por lo general, un cable eléctrico o fibra óptica, o en comunicaciones inalámbricas el rango de frecuencias asignado a su sistema).

Controlador de Dominio Primario (PDC)

El controlador de dominio es el centro neurálgico de un dominio Windows, tal como un servidor Network Information Service (NIS) lo es del servicio de información de una red Unix.

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 Distribución Principal (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.

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.

Descarga Electrostática (ESD)

Es una corriente eléctrica de corta duración, no repetitiva, que fluye entre 2 (dos) objetos cuando éstos entran en contacto, o cuando se aproximan a una distancia de unos pocos milímetros.

Disco duro

Es un dispositivo para el almacenamiento de datos a través del magnetismo u óptica.

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.

Encolamiento

Representan los distintos estados de los mensajes en el servidor al pasar por el motor de transporte.

Encriptación

Es el término utilizado para proteger un objeto, archivo o acción por medio de un algoritmo matemático.

Enlaces troncales

Es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN.q Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red.

Enrutadores

También conocido como router, son dispositivos utilizados para crear e intercomunicar subredes de datos.

Estructura de Desglose del Trabajo (EDT)

Es una descomposición jerárquica, orientada al producto entregable del trabajo que será ejecutado por el equipo del proyecto, para lograr los objetivos del proyecto y crear los productos entregables requeridos.

Ethernet

Es un estándar de transmisión de datos para redes de área local.

Ethernet de alta velocidad

También conocido como Fast Ethernet, 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.

Gabinete

Es la caja o lugar donde se alojan todos los componentes internos del computador. Su función es la de proteger los componentes del computador.

Gestión Unificada de Amenazas (UTM)

Es un término de seguridad de la información que se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red.

Gigabit Ethernet

Es un estándar para los tipos de cables cuya velocidad de transmisión de datos es de 1,000 Mbps.

Hardware

Se refiere a todas las partes físicas o tangibles de un sistema de información.

IEEE 802.11

Es una norma de la IEEE para el control de acceso a la red mediante el uso de puertos de comunicación.

IEEE 802.1Q

Fue un proyecto del grupo de trabajo 802 de IEEE para desarrollar un mecanismo que permita a múltiples redes interconectadas con puentes o conmutadores, compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio.

IEEE 802.1X

Es un estándar IEEE para un acceso de red autenticado a redes Ethernet por cable y redes 802.11 inalámbricas. IEEE 802.1X mejora la seguridad y la implementación al proporcionar la compatibilidad con la identificación de usuarios, la autenticación, la administración de claves dinámicas y la creación de cuentas de manera centralizada.

IEEE 802.3u

Es un estándar de la IEEE para medios de transmisión Ethernet con velocidades de 100 Mbps.

Impresoras estacionarias térmicas

La impresora térmica se basa en una serie de agujas calientes que van recorriendo el papel termosensible, que al contacto se vuelve de color negro.

Infraestructura de TIC

Para fines de esta norma, hace referencia al conjunto de equipos y elementos en lo que se sustenta un organismo gubernamental.

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.

Interfaz

Dispositivo capaz de transformar las señales generadas por un aparato en señales comprensibles por otro.

Interfaz de Datos Distribuida por Fibra (FDDI)

Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida (WAN) o de área local (LAN), mediante cables de fibra óptica. Se basa en la arquitectura Token Ring y permite una comunicación tipo dúplex (completo). Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

Intérprete de Ordenes Intérprete Seguro (SSH)

Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X (Sistema de Ventanas X) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows).

ISO/IEC 27001:2005

Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por la Organización Internacional de Normalización y por la Comisión Electrotécnica Internacional.

Kerberos

Es un protocolo de seguridad creado por el Instituto Tecnológico de Massachussetts (MIT, por sus siglas en inglés) que usa una criptografía de claves simétricas para validar usuarios con los servicios de red, evitando así tener que enviar contraseñas a través de la red. Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

Línea de Abonado Digital Asimétrica (ADSL)

Es un tipo de tecnología de Línea de Abonado Digital (DSL). Consiste en la transmisión analógica de datos digitales apoyada en el cable de pares simétricos de cobre que lleva la línea telefónica convencional o línea de abonado (Red Telefónica Conmutada, PSTN), siempre y cuando la longitud de línea sea de hasta inclusive 5,5 km medidos desde la central telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

Línea de Suscripción Digital (DSL)

Es una familia de tecnologías que proporcionan el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica local. Es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica básica o conmutada, a esta familia pertenecen las líneas de abonado: ADSL, ADSL2, ADSL2+, SDSL, IDSL, HDSL, SHDSL, VDSL y VDSL2.

Lista de Control de Acceso (ACL)

Es una lista de control que filtra el tráfico de la red mediante la especificación los derechos de accesos autorizados, denegados o auditados para un elemento de confianza.

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.

Método hash

Es un método de búsqueda que aumenta la velocidad de búsqueda, el cual no requiere que los elementos estén ordenados. Consiste en asignar a cada elemento un índice mediante una transformación del elemento. Esta correspondencia se realiza mediante una función de conversión, llamada función hash.

Micrones

Es la millonésima parte de un metro, y corresponde a una unidad de medida de longitud en el cableado de fibra óptica.

Navegador web

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

Nodo

Hace referencia a un computador u ordenador conectado a una red de datos.

Nube Computacional

Es una tecnología que permite la utilización de servicios de cómputos por medio de Internet.

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 Blindado (STP)

Es un tipo de cable de par trenzado utilizado para las telecomunicaciones. En el trenzado de estos cables, cada par posee una pantalla protectora y es capaz de anular las interferencias de fuentes externas y además es resistente a altas temperaturas.

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.

Parche de seguridad

Estos parches en específico se encargan de solucionar agujeros de seguridad sin alterar la funcionalidad.

Patch Panel

Es un dispositivo en el cual se organizan las conexiones físicas de red.

Plan de Continuidad de Negocio (BCP)

Plan elaborado para restablecer las funcionalidades críticas de un sistema luego de una ruptura.

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.

Política de Grupo (GPO)

Conjunto de una o más políticas o reglas que controlan el uso de los elementos de un sistema.

Protección perimetral

Es la protección de los elementos o sistemas de un área física determinada mediante la implementación de algún mecanismo de seguridad.

Protocolo

Conjunto de reglas que normalizan la manera en que se envían los datos de los dispositivos para lograr que la comunicación sea lograda de manera eficiente.

Protocolo Camino más Corto Primero (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.

Protocolo de Agregación de Puerto (PAgP)

Protocolo de Cisco utilizado para la agregación lógica y automatizada de puertos.

Protocolo de Árbol Expandido (STP)

Protocolo de red que opera en el nivel dos (2) del modelo OSI para gestionar la detección de bucles en topologías provocados por enlaces redundantes.

Protocolo de Autenticación Extensible - Autenticación Flexible por Túnel Seguro (EAP-FAST)

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 Control de Agregación de Enlaces (LACP)

Protocolo que maneja virtualmente los enlaces de la red para proveer un mejor ancho de banda y disponibilidad.

Protocolo de Descubrimiento de Capa de Enlace (LLDP)

Protocolo de la capa de enlace para la identificación de los dispositivos de red.

Protocolo de Enrutamiento de Gateway Interior Mejorado (EIGRP)

Protocolo de encaminamiento que mide el vector distancia y es utilizado para los enlaces.

Protocolo de Gateway Fronterizo (BGP)

Protocolo para el intercambio de información de ruteo y encaminamiento entre sistemas autónomos.

Protocolo de Gateway Fronterizo Externo (EBGP)

Protocolo utilizado para el intercambio de información entre distintos sistemas autónomos.

Protocolo de Gateway Fronterizo Interno (IBGP)

Protocolo utilizado para el intercambio de información entre los distintos conmutadores dentro de un sistema autónomo.

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 que proporciona los medios necesarios para la transmisión de bloques de datos digitales desde el origen al destino a través de redes interconectadas.

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 Resolución de Direcciones (ARP)

Protocolo de comunicaciones que opera en la capa de red encargado de resolver la dirección de acceso al medio correspondiente a una determinada dirección IP.

Protocolo de Tiempo de Red (NTP)

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

Protocolo de Tiempo de Red Simple (SNTP)

Es un protocolo de internet creado con el fin de sincronizar de manera simple los relojes de los sistemas informáticos que no requieran gran precisión.

Protocolo de Transferencia de Hipertexto (HTTP)

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

Protocolo Ligero/Simplificado de Acceso a Directorios (LDAP)

Es un protocolo simple a nivel de aplicación que permite acceso a una librería de datos organizados lógica y jerárquicamente en un entorno de red.

Protocolo Simple de Administración de Red (SNMP)

Protocolo que opera en la capa de aplicación para facilitar la administración de los dispositivos de red.

Protocolo Troncado VLAN (VTP)

Protocolo de mensaje utilizado para la configuración y administración de las VLAN.

Protocolo Truncado Dinámico (DTP)

Protocolo propietario operativo en conmutadores Cisco utilizado para automatizar la configuración de truncado en enlaces Ethernet.

Proveedor de Servicio de Internet (ISP)

Empresa que provee conexión a Internet.

Proxy

Dispositivo autorizado para actuar como representante o sustituto de otro.

Punto de Distribución Intermedio (IDF)

Es el área dentro de una LAN donde se distribuye todo el cableado de datos correspondiente a los usuarios.

Ramal Privado de Conmutación (PBX)

Es cualquier central telefónica que gestione mediante líneas troncales las llamadas internas, así como también las externas, ya sean entrantes o salientes.

Red

Conjunto de dispositivos y software interconectados en una estructura organizada por medio de otros dispositivos físicos a través del cual se intercambian datos.

Red de Área Amplia (WAN)

Red de computadoras que une múltiples redes LAN.

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 Digital de Servicios Integrados (ISDN)

Red que facilita conexiones digitales de extremo a extremo y que proporciona una amplia variedad de servicios, los cuales son accedidos por los usuarios a través de un conjunto de interfaces normalizados.

Redundancia

Entrega de los servicios críticos por múltiples vías para evitar que la caída de uno afecte la calidad del servicio.

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.

Conector Registrado 45 (RJ-45)

Interfaz física utilizada para la conectar redes computacionales mediante cableado estructurado.

Conector Registrado 49 (RJ-49)

Es un conector modular de 8 posiciones y 8 contactos (8p8c) utilizado como terminal de cables de par trenzado blindados.

Rivest, Shamir y Adleman (RSA)

Sistema criptográfico de clave pública utilizado para cifrar y firmar digitalmente.

Segmento de red

Es la conexión que existe entre un dispositivo o computador y un equipo de la red datos como un conmutador o un enrutador.

Seguridad del Protocolo de Internet (IPsec)

Es un conjunto de protocolos que proporcionan seguridad al protocolo IP en cuanto a la autenticación y cifrado de los datos.

Servicio de Datos Multimegabit Conmutados (SMDS)

Fue un servicio utilizado para conectar redes LAN, MAN y WAN para el intercambio de 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.

Sistema Autónomo (AS)

Es un conjunto de redes IP con una política de rutas propia e independiente, lo que le permite gestionar por sí mismo el tráfico de red existente en el mismo.

Sistema Básico de Entrada y Salida (BIOS)

Es el primer sistema que se ejecuta en dispositivos informáticos para verificar su estado.

Sistema de Alimentación Ininterrumpida (UPS)

Dispositivo que permite el funcionamiento de los sistemas conectados después de una falla energética, aunque por tiempo limitado.

Sistema de Detección de Intrusos (IDS)

Programa cuya función es detectar la presencia de accesos no autorizados a un computador o a la red.

Sistema de Prevención de Intrusos (IPS)

Software utilizado para evitar el acceso no autorizado a los sistemas computacionales de una red.

Sistema de tierra

Es la desviación de toda energía eléctrica anormal a un punto común denominado tierra para que no afecte al equipo o al usuario.

Sistema Operativo de Red (NOS)

Software que permite la interconexión entre ordenadores pertenecientes a una red y que estos puedan acceder a los recursos y servicios de la misma

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 de Prevención de Pérdida de Datos (DLP)

También conocido como prevención de fuga de datos, consiste en el uso de estrategias y mecanismos para que la información sensible o crítica no sea enviada fuera de la red corporativa.

Solicitud de Propuesta (RFP)

Documento en donde se especifican todos los detalles de una propuesta para llevar a cabo un proyecto.

Soporte de tercer nivel

Soporte de nivel experto en que se determinan con precisión problemas y soluciones.

Subredes

Conjunto de redes dependientes de una red principal.

T1-DS1

Estándar de entramado y señalización para la transmisión digital de voz y datos basado en PCM.

Tarjeta de código

Medio físico en el que residen los códigos de acceso a un determinado sistema.

Terminales de cableado

Componentes ubicados en los extremos de un cable para conectarlos con un dispositivo final.

Texto plano

Archivo informático constituido solamente por texto formado de caracteres legibles por humanos y carente de todo tipo de formato tipográfico.

TIA-568

Conjunto de estándares de telecomunicaciones para el cableado utilizado para la interconexión de dispositivos en una red.

TIA-606B

Estándar para el etiquetado de los componentes de un sistema.

Token

Es un dispositivo electrónico que contiene claves criptográficas y son normalmente utilizados para la autenticación de usuarios como segundo factor.

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.

Tráfico de la red

Cantidad de datos enviados y recibidos por los usuarios de una red.

Unidad Central de Procesamiento (CPU)

Dispositivo central dedicado a la interpretación y ejecución de instrucciones en computadores.

Unidad de Datos de Protocolo Puente (BPDU)

Tramas que contienen información del STP.

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.

Zona Desmilitarizada (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	3DES o TDES	Triple Data Encryption Algorithm	Algoritmo de Cifrado Triple de Datos
2	ACL	Access Control List	Lista de Control de Acceso
3	ADSL	Asymmetric Digital Subscriber Line	Línea de Abonado Digital Asimétrica
4	ARP	Address Resolution Protocol	Protocolo de Resolución de Direcciones
5	AS	Autonomous System	Sistema Autónomo
6	ASF	Assignable Square Feet	Pies Cuadrados Asignables
7	ATM	Asynchronous Transfer Mode	Modo de Transferencia Asíncrono
8	ATS	Automatic Transfer Switch	Conmutador de Transferencia Automático
9	BCP	Business Continuity Plan	Plan de Continuidad de Negocio
10	BGP	Border Gateway Protocol	Protocolo de Gateway Fronterizo
11	BIOS	Basic Input Output System	Sistema Básico de Entrada y Salida
12	BPDU	Bridge Protocol Data Units	Unidad de Datos de Protocolo Puente
13	BSS	Basic Service Set	Conjunto de Servicio Básico
14	CCM	Cloud Control Matrix	Matriz de Control en la Nube
15	CCTV	Closed-Circuit Television	Circuito Cerrado de Televisión
16	CMDB	Configuration Management Database	Base de Datos de la Gestión de Configuración

17	CPU	Central Processing Unit	Unidad Central de Procesamiento
18	CSA	Cloud Security Alliance	N/A
19	DCIM	Data Center Infrastructure Management	Administración de Infraestructura del Centro de Datos
20	DHCP	Dynamic Host Configuration Protocol	Protocolo de Configuración Dinámica de Host
21	DLP	Data Loss Prevention Software	Software de Prevención de Pérdida de Datos
22	DMZ	Demilitarized Zone	Zonas Desmilitarizadas
23	DSL	Digital Subscriber Line	Línea de Suscripción Digital
24	DTP	Dynamic Trunk Protocol	Protocolo Truncado Dinámico
25	EAP-FAST	Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling	Protocolo de Autenticación Extensible - Autenticación Flexible por Túnel Seguro
26	EBGP	External Border Gateway Protocol	Protocolo de Gateway Fronterizo Externo
27	EDA	Equipment Distribution Area	Área de Distribución de Equipos
28	EDT	Work Breakdown Structure	Estructura de Desglose del Trabajo
29	EIGRP	Enhanced Interior Gateway Routing Protocol	Protocolo de Enrutamiento de Gateway Interior Mejorado
30	ER	Entrance Room	Cuarto de Entrada
31	ESD	Electrostatic discharge	Descarga Electrostática
32	ESS	Extended Service Set	Conjunto de Servicio Extendido

33	FC	Ferrule Connector / Fiber Channel	Conector de Canal de Fibra
34	FDDI	Fiber Distributed Data Interface	Interfaz de Datos Distribuida por Fibra
35	GPO	Group Policy	Política de Grupo
36	HDA	Horizontal Distribution Area	Área Horizontal de Distribución
37	HTTP	Hypertext Transfer Protocol	Protocolo de Transferencia de Hipertexto
38	IaaS	Infrastructure as a Service	Infraestructura como Servicio
39	IBGP	Internal Border Gateway Protocol	Protocolo de Gateway Fronterizo Interno
40	IDF	Intermediate Distribution Frame	Punto Intermedio de Distribución
41	IDS	Intrusion Detection System	Sistema de Detección de Intrusos
42	IEEE	Institute of Electrical and Electronics Engineers	Instituto de Ingenieros Eléctricos y Electrónicos
43	IETF	Internet Engineering Task Force	Grupo de Trabajo de Ingeniería de Internet
44	IP	Internet Protocol	Protocolo de Internet
45	IPS	Intrusion Prevention System	Sistema de Prevención de Intrusos
46	IPsec	Internet Protocol security	Protocolo de Seguridad de Internet
47	IPv4	Internet Protocol version 4	Protocolo de Internet Versión 4
48	IPv6	Internet Protocol version 6	Protocolo de Internet Versión 6
49	ISDN	Integrated Services Digital Network	Red Digital de Servicios Integrados
50	ISP	Internet Service Provider	Proveedor de Servicio de Internet

51	LACP	Link Aggregation Control Protocol	Protocolo de Control de Agregación de Enlaces
52	LAN	Local Area Network	Red de Área Local
53	LDAP	Lightweight Directory Access Protocol	Protocolo Ligero/ Simplificado de Acceso a Directorios
54	LLDP	Link Layer Discovery Protocol	Protocolo de Descubrimiento de Capa de Enlace
55	MAC	Media Access Control	Control de Acceso al Medio
56	MD5	Message-Digest Algorithm 5	Algoritmo de Resumen del Mensaje 5
57	MDA	Main Distribution Area	Área Central de Distribución
58	MDF	Main Distribution Frame	Cuarto de Distribución Principal
59	NEC	National Electrical Code	Código Eléctrico Nacional
60	NEMA	National Electrical Manufacturers Association	Asociación Nacional de Fabricantes Eléctricos
61	NFPA	National Fire Protection Association	Asociación Nacional de Protección contra el Fuego
62	NOC	Network Operations Center	Centro de Operaciones de Red
63	NOS	Network Operating System	Sistema Operativo de Red
64	NTP	Network Time Protocol	Protocolo de Tiempo de Red
65	OSPF	Open Shortest Path First	Protocolo Camino más Corto Primero
66	Paas	Platform as a Service	Plataforma como Servicio
67	PAgP	Port Aggregation Protocol	Protocolo de Agregación de Servicio

68	PBX	Private Branch Exchange	Ramal Privado de Conmutación
69	PDC	Primary Domain Controller	Controlador de Dominio Primario
70	QoS	Quality of Service	Calidad del Servicio
71	RADIUS	Remote Authentication Dial-In User Service	Autenticación Remota para Servicios de Marcado a Usuarios
72	RFC	Request for Comments	Solicitud de Comentarios
73	RFP	Request for Proposal	Solicitud de Propuesta
74	RIP	Routing Information Protocol	Protocolo de Información de Enrutamiento
75	RJ45	Registered Jack 45	Clavija Registrada 45
76	RSA	Rivest, Shamir and Adleman	Rivest, Shamir y Adleman
77	SaaS	Software as a Service	Software como Servicio
78	SC	Square Connector / Standard Connector	Conector Cuadrado
79	SC-DC	Square Connector Dual Contact	Conector Cuadrado Dúplex
80	SHA	Secure Hash Algorithm	Algoritmo de Hash Seguro
81	SLA	Service Level Agreement	Acuerdo de nivel de servicio
82	SMDS	Switched Multi-megabit Data Service	Servicio de Datos Multimegabit Conmutados
83	SNMP	Simple Network Management Protocol	Protocolo Simple de Administración de Red
84	SNTP	Simple Network Time Protocol	Protocolo de Tiempo de Red Simple
85	SOC	Service Organization Controls	Controles de la Empresa de Servicios

86	SSAE 16	Statement on Standards for Attestation Engagements No. 16	Declaración sobre Normas de Auditoría 16
87	SSH	Secure Shell	Intérprete de Ordenes Seguro
88	SSID	Service Set Identifier	Identificador del Conjunto de Servicio
89	SSL	Secure Sockets Layer	Capa de Conexión Segura
90	SSO	Single Sign-On	Autenticación Simple
91	ST	Straight Tip	Conector de Punta Recta
92	STP	Shielded Twisted Pair	Par Trenzado Blindado
93	STP	Spanning Tree Protocol	Protocolo de Árbol Expandido
94	TGB	Telecommunications Ground Bar	Barra de Tierra para Telecomunicaciones
95	TIA	Telecommunications Industry Association	Asociación de la Industria de Telecomunicaciones
96	TIC	N/A	Tecnologías de la Información y la Comunicación
97	TMGB	Telecommunications Main Ground Bar	Barra Principal de Tierra para Telecomunicaciones
98	UPS	Uninterruptible Power Supply	Sistema de Alimentación Ininterrumpida
99	UTM	Unified Threat Management	Gestión Unificada de Amenazas
100	UTP	Unshielded Twisted Pair	Par Trenzado sin Blindaje
101	VLAN	Virtual Local Area Network	Red de Área Local Virtual
102	VoIP	Voice over Internet Protocol	Voz sobre Protocolo de Internet
103	VTP	VLAN Trunking Protocol	Protocolo Troncado VLAN

104	WAN	Wide Area Network	Red de Área Amplia
105	WPA2	Wi-Fi Protected Access 2	Acceso Protegido Wi-Fi 2
106	ZDA	Zone Distribution Area	Área de Distribución Zonal

BIBLIOGRAFÍA

- ISO/IEC 27035. (2011). Internationational Organization for standardization / International Electrotechnical Commission. Information technology – Security techniques – Information Security managements systems – Information security incident managements systems - information security incident management.
- A/E Design . (2014). Guide for Drawings and Spec Section 27 17 53 WIRELESS COMMUNICATIONS. United States of America.
- Barker, K., & Wallace, K. (2015). CompTIA Network+ N10-006 Cert Guide. United States of America.
- Bruno, A., & Jordan, S. (2011). CCDA 640-864 Official Cert Guide. United States of America.
- CCNP ROUTE 642-902 Quick Reference. (2010). United States of America.
- Cisco Systems. (2014). Connecting Networks Companion Guide. United States of America.
- Cloud Security Alliance . (2011). Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Estados Unidos.
- COBIT 4.1. . (2007). United States of America.
- Department of Education. (2013). DIIT Voice/Data Cable Infrastructure Specifications Version 7.3.5. United States of America.
- DiMinico, C. (2005). ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers. United States of America.
- 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.

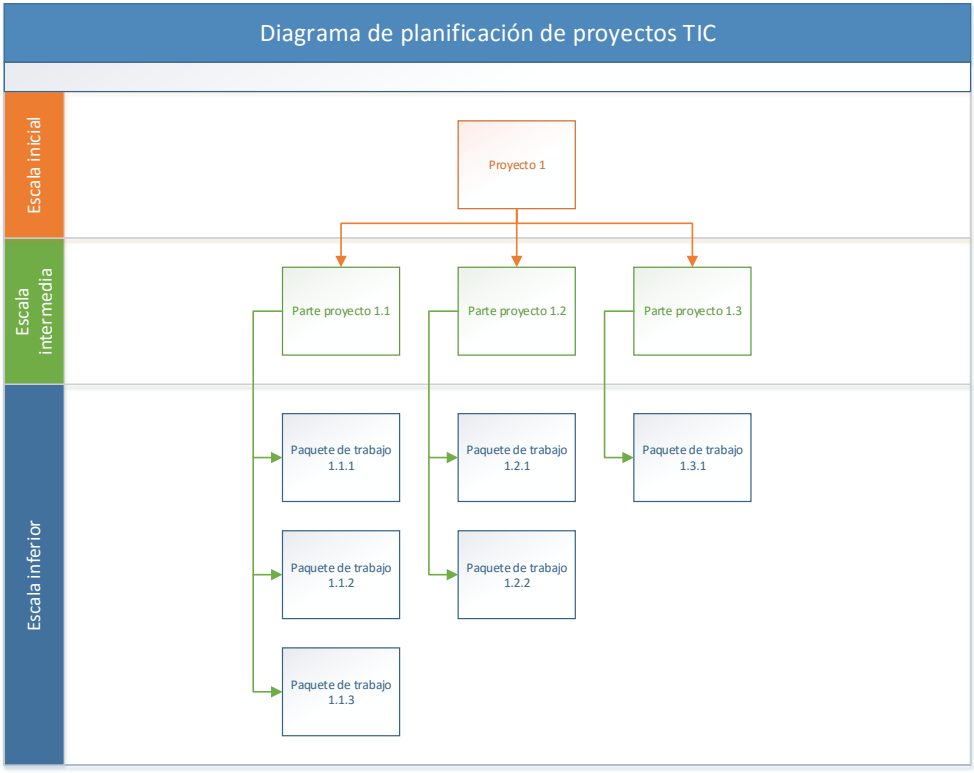
- Docter, Q., Dulaney, E., & Skandier, T. (2012). CompTIA Complete Deluxe Study Guide. United States of America.
- Fanning , P. (2005). ITIL Service Operation v3. United States of America.
- Guía de Recomendación para Data Center. (2010). Brasil.
- Guías de Seguridad de Áreas Críticas en Cloud Computing. (2009). España.
- Hausman, K., Cook, S., & Sampaio, T. (2013). Cloud Essentials CompTIA Authorized Courseware for Exam CLO-001 . United States of America.
- Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. (2010). United States of America.
- iso 20047. (s.f.).
- ISO/IEC 27000. (2013). International Organization for Standardization.
- ISO/IEC 27001. (2005). International Organization for Standardization.
- ISO/IEC 27002. (2013). International Organization for Standardization.
- ISO/IEC 27005 . (2011). International Organization for Standardization. Information technology — Security techniques — Information security risk management.
- ISO/IEC 27032. (2012). Internationational Organization for standardization / International Electrotechnical Commission. Information technology – Security techniques – Information Security managements systems – Information security incident managements sydtems-Guideline for cybersecurity.
- Jang, M. (2011). RHCSA/RHCE Red Hat Linux Certification Study Guide, Seventh Edition (Exams EX200 & EX300). United States of America.

- Joskowicz, D. (2013). Cableado Estructurado. Uruguay.
- Kay, T. (2001). Server+ Certification Bible. United States of America.
- La Agencia Europea de Seguridad de las Redes y de la Información. (2009). Computación en Nube Beneficios, Riesgos y Recomendaciones para la Seguridad de la Información. Unión Europea.
- Limoncelli, T., Hogan, C., & R, S. (s.f.). The Practice of System and Network Administration Second Edition. United States of America.
- Ministerio de Hacienda y administraciones Públicas; Centro Criptológico Nacional . (2013). Guía/Norma de Seguridad delas TIC Seguridad en entornos cloud. España.
- Ministerio de Industria, Energía y Turismo. (2012). Cloud Computing Retos y Oportunidades. España.
- Ministerio de Industria, Turismo y Comercio Instituto Nacional de Tecnologías de la Comunicación . (2011). Guía sobre almacenamiento y borrado seguro de la Información. . España.
- Oficina presidencial de tecnologías de la información y comunicación (OPTIC). (2013). Diseño, construcción, equipamiento, instalación y puesta en marcha del data center del estado dominicano. República Dominicana.
- Poulton, N. (2014). Data Storage Networking CompTIA Storage+™ Certification. United States of America.
- Salam, A., Gilani, Z., & Ul Haq, S. (2015). Deploying and Managing a Cloud Infrastructure the CompTIA Cloud Certification. United States of America.
- University of Chicago. (2011). Telecommunications Structure Cabling Guidelines and Specifications. United States of America.

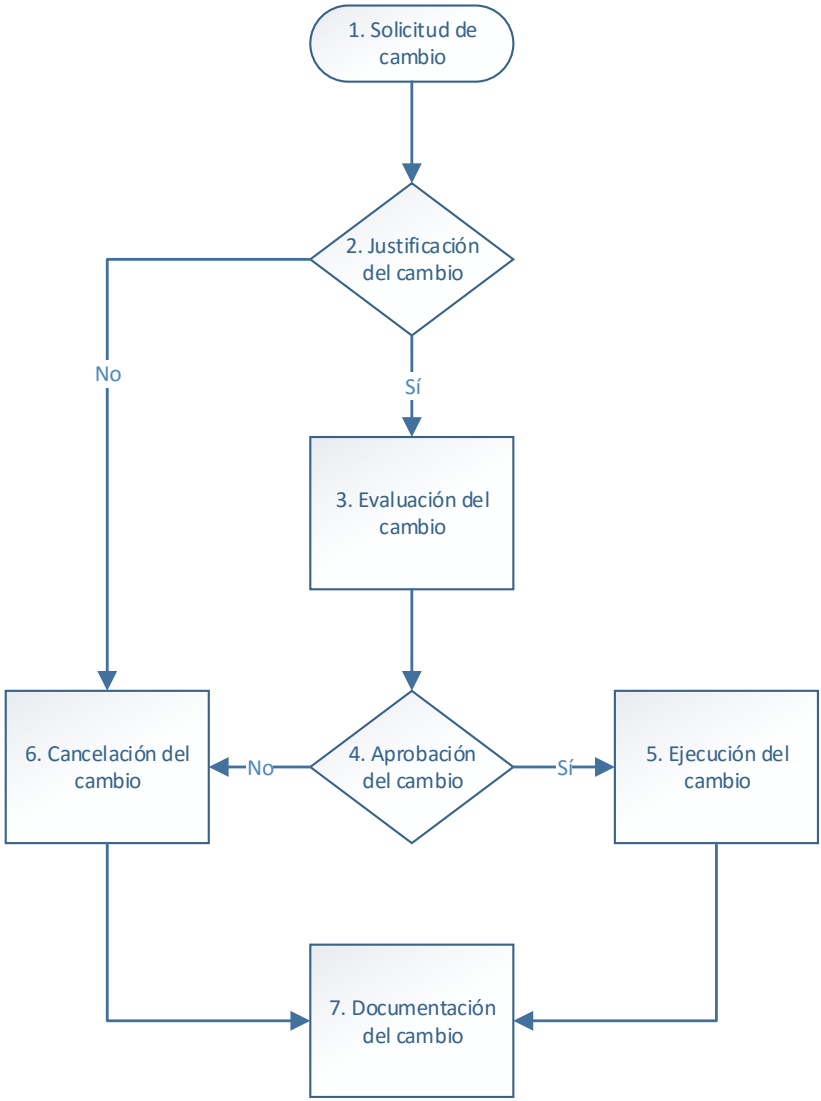
- VMware, Inc. (2009). Server Configuration Guide ESX Server 3.0.1 and VirtualCenter 2.0.1. . United States of America.
- Wallace, K. (2015). CCNP Routing and Switching ROUTE 300-101. United States of America.
- Yeluri , R., & Castro Leon , E. (2014). Building the Infrastructure for Cloud Security a Solitions View. United States of America.

ANEXOS

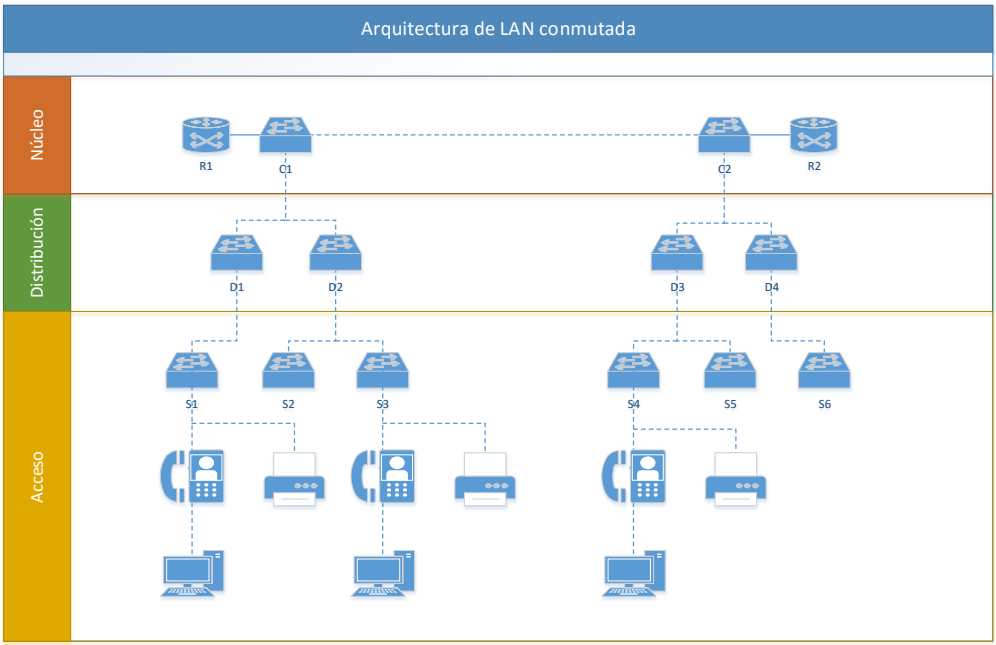
Anexo A. *Diagrama de planificación de proyectos TIC.*



Anexo B. *Proceso de solicitud de cambio.*



Anexo C. *Modelo jerárquico de la arquitectura de red.*

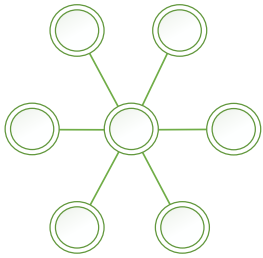
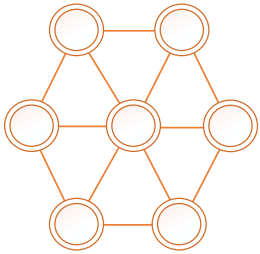
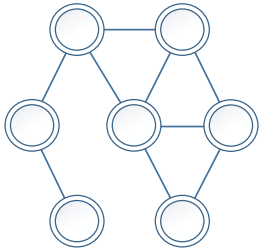


Anexo D. *Estándares para redes inalámbricas.*

Estándar	Velocidad Máxima	Frecuencia	Compatibilidad con versiones anteriores
802.11a	54 Mbps	5 GHz	No
802.11b	11 Mbps	2,4 GHz	No
802.11g	54 Mbps	2,4 GHz	802.11b
802.11n	600 Mbps	2,4 GHz o 5 GHz	802.11b/g
802.11ac	1,3 Gbps (1300 Mbps)	2,4 GHz y 5,5 GHz	802.11b/g/n
802.11ad	7 Gbps (7000 Mbps)	2,4 GHz, 5 GHz y 60 GHz	802.11b/g/n/ac

Esta tabla fue elaborada en base a la establecida por CISCO

Anexo E. *Diseño para la topología de la red LAN.*

Diseño de la topología de la red LAN		
Estrella	Malla completa	Malla parcial
		

EQUIPO DE TRABAJO

Dirección General

Armando García, Director General

Departamento de Estandarización, Normativas y Auditoría Técnica

Glenny María Castro, Gerente del ENAT

Shalem Pérez, Auditor de Estándares NORTIC

Winner Núñez, Auditor de Estándares NORTIC

Ginsy Aguilera, Consultor de Estándares y Normativas

Enyer Pérez, Consultor de Estándares y Normativas

Emmanuel Reyes, Analista de Estándares y Normativas

Comité Interno para Evaluación de las Normas (CIEN) – Equipo OPTIC

Charli Polanco, Director de TIC

Elvyn Peguero, Director de Planificación y Desarrollo

José Luis Liranzo, Director de DIGOB

Miguel Guerra, Gerente Multimedia

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

Francisco Augusto Cruz Pichardo – Instituto Dominicano de las Telecomunicaciones (INDOTEL)

Teresina Pérez – Dirección General del Catastro Nacional

Mario Herrera Hernández – Ministerio de la Juventud

Carmen Mejía Vásquez – Contraloría General de la República Dominicana

Colaboradores

Ariel Acosta

Edwin Sánchez

Hamlet Durán

Para Visualizar y descargar este documento leer este código

Av.27 de Febrero #419, Santo Domingo, R.D.
Tel.:1+ 809.286.1009 info@optic.gob.do
www.optic.gob.do www.dominicana.gob.do

OpticRD