DECANATO DE INGENIERIAS E INFORMATICA

Trabajo de grado para optar por el título de

Ingeniero en Sistemas de Computación

Tema:

ANÁLISIS E IMPLEMENTACIÓN DE UN SISTEMA DE RECUPERACIÓN DE DESASTRE PARA LA OFICINA PRESIDENCIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (OPTIC) UTILIZANDO EL CLOUD COMPUTING (NUBE), EN LA CIUDAD DE SANTO DOMINGO DURANTE EL PERIODO SEPTIEMBRE - DICIEMBRE DEL 2016.

Sustentantes:

Ledy Gissel Gómez Rodríguez 2011-1929

Yaritza Pamela Moreta Rodríguez 2012-2259

Edwin Alexander Sánchez Vásquez 2013-1827

Asesor:

Ing. Freddy Jiménez

Santo Domingo, Rep. Dom.

Noviembre 2016

Índice de Contenido

DEDICATORIAS

La presente tesis es dedicada a mi tío ***Wilfredo Gómez****, porque en el encontré el apoyo y la confianza para poder alcanzar esta meta tan importante para mí.*

Tío me siento inmensamente agradecida por su apoyo, quiero que sepa lo valioso que usted es para mí, su afecto y cariño me dieron las fortalezas necesarias para poder llegar hasta el final de esta carrera.

Me siento muy afortunada de tener como tío, un ser tan maravilloso, el cual respeto y adoro con todo mi corazón.

Le pido a Dios que lo llene de muchísima salud, que lo bendiga hoy mañana y siempre.

Daré lo mejor, en mi desarrollo profesional.

¡Tío, lo logré!

Ledy G. Gómez R.

Te dedico este logro a ti, mi señora bonita ***Patria Rodríguez*** *a la mujer que amo con locura, mi madre y amiga, una mujer plena, agradecida y llena de fe, quien me brindó su amor y cariño desde que estaba en su vientre, a lo largo de los años me ofreciste estímulo, apoyo, compresión y paciencia constante, cosas así solo las hace quien ama de verdad! gracias por creer en mí.*

Mi señora bonita, quien me ha regalado la vida y parte de la suya, quien me apoya incondicionalmente, te dedico cada logro, dedicación, trabajo, esfuerzo y meta realizada, me has hecho crecer, agradezco infinitamente el apoyo que me das día a día y por compartir tanto tus aciertos como tus errores que puedo usar de lecciones, aportándome crecimiento.

Gracias por ser la mujer maravillosa, trabajadora y luchadora incansable que tengo la dicha de llamar mamá, quien da todo por mí y mis hermanas, brindado la mayor cantidad de lecciones y consejos, forjando mi carácter e inculcado valores que hoy forman parte de mí. Te agradezco cada recomendación, pero más aún, la oportunidad de elegir, de permitirme ser independiente. Papá Dios me dio el mejor regalo al tenerte como madre, este logro es por ti! Te amo.

Yaritza P. Moreta R.

Esta tesis es para ti, Madre, ***Sonia Vásquez****. Por ser la mejor madre del mundo, porque desde que tengo memoria me has entregado lo mejor de ti. Por enseñarme con tu ejemplo de sacrificio, esfuerzo y dedicación que todo se puede.*

Por nunca escatimar esfuerzos por mí, por enseñarme a no conformarme y a querer ser más. Por darme tu amor y cariño de forma incondicional.

Eres la razón por la cual emprendí este camino y por la cual he permanecido firme para concluirlo.

¡Este logro es por ti y para ti!

Edwin A. Sánchez V.

AGRADECIMIENTOS

*Primero a **Dios** las gracias, el ilumina mi camino, guía mis pasos, me llena de perseverancia para lograr mis metas, me bendice y me ama. Gracias por ayudarme a sobre pasar obstáculos que pude encontrar.*

*Les agradezco a mis padres **Belkis Rodríguez y Aníbal Gómez.** Ellos depositan su confianza en mí, gracias por estar ahí cuando los necesito, gracias por sus consejos, gracias por su amor, compresión y dedicación hacia sus hijos. Le doy las gracias todos los días a Dios por tenerlos como padres, los amo demasiado.*

*A mis hermanos **Sthefani Gómez y Sais Gómez**, espero servirle como ejemplo y brindarle todo mi apoyo por el resto de mi vida.*

*A mi **abuelo Federico Gómez,** por su amor, por sus consejos sabios, por sus cuidados, por su apoyo incondicional y gracias por ser el mejor abuelo del mundo. Que Dios lo bendiga papá.*

*A mi novio **Ricky Soto,** por caminar junto conmigo en esta etapa de mi vida, por tu amor, cariño y apoyo que pude encontrar en ti.*

*A mis amigos y colegas **Johanna Sosa, Génesis Pimentel, Gael Abreu, Cindy Vázquez, y Emmanuel De los Santos**, le doy gracias a Dios, por permitirme conocerlos.*

*A mis compañeros de tesis, **Edwin Sánchez y Yaritza Moreta,** gracias por aportar su granito de arena, que nos permitió culminar este trabajo de grado.*

*Agradezco sinceramente a nuestro asesor de tesis **Ing. Freddy Jiménez,** por su esfuerzo y dedicación.*

Ledy G. Gómez R.

*Gracias papá **Dios** por regalarme la dicha de vivir, por la fuerza de voluntad, salud y esperanza en aquello que no veo, gracias a ello me has permitido arriesgarme y por ello he culminado una meta más, con esfuerzo y empeño, gracias por rodearme de personas que me impulsan a continuar, por la hermosa familia que has regalado.*

*A mis padres **Patria Rodríguez y Carlos Moreta**, mis viejos adorados, quienes me brindan amor, comprensión paciencia, me enseñaron a luchar por lo que quiero, con perseverancia y puesta en manos de Dios todo se puede. Los adoro.*

*A las hermanas grandiosas que papa Dios me prestó, **Carla Paola Moreta R. y Carla Paloma Moreta R.** con quienes he reído y llorado, con las que puedo contar en los momentos más lúcidos y en los más oscuros, y el infinito apoyo me dan. Este logro también es gracias a ustedes.*

A mis amigos, con quienes compartí muchas anécdotas, problemas y soluciones en el transcurso de la travesía, compartiendo en equipo y brindándonos apoyo mutuo.

*A mis compañeros de tesis **Ledy G. Gómez y Edwin Sánchez** gracias por los conocimientos aportados, con ella la paciencia, perseverancia en que lograríamos llevar a cabo, ¡lo hicimos! El mérito es nuestro.*

*También a la universidad Acción Pro-Educación y Cultura (**UNAPEC**), a la que le debo mi formación y desarrollo. Con ella, a cada profesor que, aportado a lo largo de mi formación, compartiendo sus conocimientos, experiencias, apoyo y paciencia. En especial, al **Ing. Freddy Jiménez** quien nos ha guiado para realizar cada línea escrita, ofreciendo su entera disposición, aportando consejos y pautas que debemos seguir.*

Es la hora de partir, la dura y fría hora que la noche sujeta a todo horario.

Pablo Neruda

Yaritza P. Moreta R.

*Gracias a **Dios** por guiar cada uno de mis pasos, por permitirme llegar donde estoy, por darme las fuerzas necesarias para alcanzar esta meta. Todo lo que he logrado se lo debo a Él.*

*A mi madre, **Sonia Vásquez** por su gran esfuerzo y dedicación en guiar mis pasos desde niño para ser un hombre de bien, por ser quien me ha dado todo. Por apoyarme en cada una de mis decisiones, por preocuparse por mí, por darme su amor y cariño día tras día. Siempre doy gracias a Dios porque el mejor regalo que me ha dado eres tú.*

*A **José Belén Coronado.** Abuelo, aunque ya no estés presente, nunca olvidaré tu cariño, ánimo y apoyo en cada momento.*

*A mi padre, **Edward Sánchez,** por estar siempre pendiente de mis estudios y animarme a seguir hacia adelante.*

*Gracias a **Denzel Pére**z por ser una gran amiga, por darme ánimo y estar ahí en cada momento que lo necesité. A mis amigos y compañeros de estudio, los cuales me brindaron su apoyo durante esta travesía. **Emmanuel Abreu, Ambiorix Pérez y Danny Rodríguez**, ustedes son parte de este logro.*

*A **Charli Polanco** y mis compañeros de trabajo, por su ayuda y comprensión, sin los cuales no habría logrado esta meta.*

*También, a mis compañeras de tesis **Yaritza P. Moreta y Ledy G. Gómez**, por seguir adelante a pesar de las adversidades. Gracias por darme la oportunidad de compartir esta experiencia con ustedes.*

*A nuestro asesor **Ing. Freddy Jiménez**, gracias por todo su apoyo en medio de este proyecto. Por corregirnos y guiarnos cuando era necesario. Por su paciencia y dedicación con nosotros. Gracias.*

Edwin A. Sánchez V.

INTRODUCCIÓN

La República Dominicana se encuentra emergida en los avances tecnológicos que son aplicados para simplificar y ampliar los recursos en las empresas, hogares y en la vida cotidiana. A través de la Oficina Presidencial de Tecnologías de la Información y Comunicación de la Republica Dominicana (OPTIC), poder establecer y marcar el desarrollo de las instituciones y, por consiguiente, obtener el desarrollo tecnológico visualizado.

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) es la responsable de planificar, dirigir y ejecutar las acciones necesarias para implementar el Gobierno Electrónico en el país mediante la difusión y uso de las Tecnologías de la Información y Comunicación (TIC).

La información se ha convertido en el activo más importante de las organizaciones de hoy en día, por lo cual es necesario asegurar la integridad, confidencialidad y disponibilidad de la misma. Por lo cual se hace necesario el uso de las TIC con el objetivo de poder administrar de forma correcta la información.

Actualmente, la OPTIC brinda múltiples servicios de forma interna y externa a diferentes instituciones del estado como también a los ciudadanos. Dentro de los servicios que ofrece se encuentra alojamiento de correos, alojamiento de páginas web, alojamiento de aplicaciones, atención ciudadana vía telefónica, entre otros.

La OPTIC no posee actualmente un plan de recuperación de desastres que permita mantener sus servicios activos ante una eventualidad en corto tiempo. Un plan de recuperación de desastres es un conjunto de procesos y mecanismos que permiten mantener la disponibilidad de los servicios ante cualquier desastre que se presente.

La idea central de este proyecto es proporcionar a la OPTIC un centro de datos bajo los lineamientos adecuados; y así cumplir las expectativas que ofrece como instrumento para fomentar el acceso a la información, haciendo más eficiente los procesos que permiten proveer los servicios, teniendo como resultado final el desarrollo

socioeconómico del país y cumplir con las expectativas planteadas. Además, se busca disminuir el tiempo de recuperación de las operaciones ante cualquier eventualidad.

Para ello se desarrollan los diferentes ítems, los cuales incluyen desde las generalidades de la OPTIC, datacenter (que incluye los planos del Datacenter), la nube, plan de recuperación de desastre (DRP) y propuesta técnica del proyecto, hasta llegar a las conclusiones y recomendaciones generales del proyecto.

Al tratar estos temas se pretende proporcionar el entorno sobre el cual se sustenta un plan de recuperación de desastre. Partiendo desde la OPTIC hasta la propuesta.

En el capítulo 1, se resalta la importancia y el rol de la Oficina Presidencial de Tecnologías de la Información y Comunicación de la Republica Dominicana, en el cual se describe los antecedentes históricos, servicios e importancia, para poder entender el desarrollo del proyecto.

El capítulo 2, describe las herramientas que resultan necesarias e imprescindibles para el desarrollo de la infraestructura física y tecnológica en las empresas el Datacenter, buscando un enfoque estratégico para su uso. Puntualizando en las redes, topología, niveles de redundancia y la seguridad que amerita un Datacenter.

En el capítulo 3, describe la arquitectura tecnológica de servicios Cloud, lo cual permite aumentar la eficiencia, en el cual se detallan los beneficios, tipos de nube, la arquitectura orientada al servicio, niveles de servicios y la virtualización, dichos conceptos son necesarios para poder entender y desarrollar la propuesta final.

El desarrollo de un DRP, se desglosa en el capítulo 4, donde se encuentra la estructura que debe tener un Plan de Recuperación de Desastre (DRP), desde su origen, funciones, fases, entre otros, con la finalidad de disminuir los riesgos o en caso de ser posible eliminarlos.

Para finalizar, se realiza la propuesta técnica del proyecto desarrollada en el capítulo 5, basándose en las normas, métodos y herramientas ya explicadas, se define el diseño, plan estratégico para la implementación, considerando los beneficios que puede brindar la reestructuración planteada.

RESUMEN

La evolución constante que sufre la tecnología, ha provocado que las empresas generen gran cantidad de información que resulta de gran importancia y amerita tener un grado de seguridad mayor al que se implementaba años atrás.

El servicio y almacenamiento de la información en las empresas, debe considerar la posibilidad de interrupciones en el servicio, dichas interrupciones pueden ser errores humanos, factores externos, como el caso de desastres naturales o tecnológicos, provocando perdida potencial de información.

Actualmente, las informaciones relevantes de las compañías se encuentran almacenadas en los centros de procesamiento de datos o Datacenter o alojadas en sitios remotos, a través de los años, se han creado nuevas posibilidades de llevar a cabo la seguridad, integridad, confidencialidad y disponibilidad de la información deseada a través del uso de la nube.

La nube proporciona seguridad de la información alojada y recuperación de información en caso de eventos que provoquen interrupción en el servicio o aún peores pérdidas significativas para la empresa, y en consecuencia se vea afectada la imagen y rentabilidad en los servicios.

Sí bien muchas compañías cuentan con un plan de recuperación de desastres sencillo, es decir, no abarca las pérdidas que podrían presentarse en momento de ocurrir un evento, generando mayores gastos, perdidas y en casos muy extremo, el cierre de la misma. Para ello, la elaboración minuciosa de un plan de recuperación de desastre, marca la diferencia entre lo necesario y lo importante.

ASPECTOS METODOLÓGICOS

Objetivo General

Analizar el plan de recuperación ante desastres de la Oficina Presidencial de Tecnologías de la Información y Comunicación(OPTIC), determinar e identificar las necesidades específicas con el fin de poder tomar las mejores medidas y prácticas que garantice la mejora continua de los procesos en el diseño y elaboración, así lograr minimizar el impacto.

Objetivos Específicos

- Determinar las incidencias en el departamento de TI en la OPTIC.
- Conocer la funcionalidad del plan de recuperación, personal involucrado, equipos alternativos, configuraciones y documentación existente.
- Identificar las causas de interrupción de las operaciones de la institución.
- Evaluar las vulnerabilidades existentes y determinar el riesgo e integridad de las informaciones de la empresa.

Planteamiento del Problema

Las organizaciones de hoy día, buscan adaptarse al contexto actual, donde la productividad, la competencia continua y la globalización han provocado una dependencia completa de las tecnologías de la información para sus operaciones cotidianas.

Por lo cual se hace vital contar con un plan de recuperación de desastres que permita no solo mantener la disponibilidad de la información, sino que además brinde continuidad de operaciones ante posibles situaciones críticas. Este plan debe ser desarrollado acorde a los lineamientos estratégicos de la empresa con el fin de poder cumplir con los objetivos necesarios para mantener el funcionamiento de la misma.

La siguiente investigación busca indagar los riesgos de los sistemas, servicios, equipos de redes y aplicaciones. Para asegurarnos de cómo se ejecutaría el plan de recuperación de desastre, si se percibe una falla.

Delimitación del Problema

La actividad fundamental en la OPTIC es la implementación del gobierno electrónico en la Republica Dominicana, con el fin de fomentar el crecimiento tanto económico como tecnológico, a través de lineamientos, políticas y estrategias que permiten promover y desarrollar nuevas tecnologías, para determinar el diseño y la planificación de las acciones y sustentar la forma más práctica y de menor costo.

Como institución del Estado se procederá a definir las variables y relevancia del problema de estudio, dividido de la siguiente manera:

Marco Espacial

El planteamiento del problema y la investigación, se realizará en base a la Oficina Presidencial de Tecnologías de la Información y Comunicación en su localidad principal de Santo Domingo, Distrito Nacional.

Marco Temporal

Esta investigación se delimita al periodo Agosto – Diciembre del 2016.

Marco Poblacional

Para llevar a cabo el objetivo de la investigación sobre la OPTIC, se seleccionó la muestra no probabilística. Las personas seleccionadas procederán al proceso de entrevista, encuesta y observación, así lograr documentar las expectativas.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Capítulo I

Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

Introducción

La Oficina Presidencial de Tecnologías de la Información y Comunicación de la Republica Dominicana (OPTIC), es la institución dedicada a la implementación del Gobierno Electrónico en el país, creada bajo los lineamientos con la finalidad de la difusión y uso de las tecnologías de comunicación, a través del procesamiento y transmisión de información por los diferentes medios.

En este capítulo, se aborda una visión general de la OPTIC, donde se explora todos los aspectos relacionados con la necesidad de la implementación del acceso a la tecnología brindando asistencia a instituciones gubernamentales. Se introducen los antecedentes históricos, principales características, servicios e importancia que llevaron a la implementación del mismo, a través de políticas que promueven la cultura que sea de provecho tecnológico tanto para el gobierno como el país.

1.1Descripción de la OPTIC [1]

La Oficina Presidencial de Tecnologías de la Información y Comunicación de la Republica Dominicana (OPTIC), institución con dependencia del Poder Ejecutivo, creada con la responsabilidad de planificar, dirigir y ejecutar las acciones necesarias para implementar el Gobierno Electrónico en el país mediante la difusión y uso de las tecnologías de la información y comunicación (TIC).

Las Tecnologías de la Información y Comunicación (TIC) son un conjunto de herramientas de tecnología que facilitan el procesamiento y transmisión de información por medios electrónicos, como las siguientes: teléfonos, Internet, televisión interactiva, intranet, entre otros.

1.1.1 Historia de la OPTIC [2]

En el año 2004, buscando modernizar el Estado, aumentar la competitividad del sector productivo y socializar el acceso a la información, el Gobierno Dominicano identificó la necesidad de contar con un organismo de alto nivel gubernamental, articulando iniciativas sectoriales en el sentido de manifestar en el país el uso de las tecnologías de la información y comunicación (TIC). Siendo de interés particular, fomentar, desarrollar y diseñar proyectos, políticas y estrategias que tiendan a democratizar el uso, acceso y aplicación de las tecnologías de la información y comunicación (TIC), asimismo, reducir la brecha digital, el cual consiste en la diferencia de acceso al conocimiento, la información y las tecnologías de la información y comunicación (TIC) entre personas, con un nivel adquisitivo menor.

En base a esto, se creó el organismo encargado de coordinar las iniciativas y proyectos de desarrollo, apoyándose en las tecnologías de información y comunicación (TIC) de manera armónica y articulada acorde a los planes generales y estratégicos trazados por

[1] https://www.optic.gob.do/index.php/sobre-nosotros-m

[2] https://www.optic.gob.do/index.php/sobre-nosotros/historia

el Poder Ejecutivo, capaz de crear el ambiente necesario para la competitividad, eficientica y transparentar el desempeño de la Administración Pública, así como de invertir en las áreas que propicien la participación de toda la ciudadanía.

Sumado al interés como país de cumplir con los acuerdos suscritos con las Naciones Unidas para alcanzar los Objetivos del Milenio y erradicar la pobreza, conjuntamente, dar cumplimiento a los acuerdos de: la Declaración de Bávaro, la Declaración de Principios y el Plan de Acción de la Cumbre Mundial para la Sociedad de la Información en su primera fase, en Ginebra, diciembre 2003, y en su segunda fase el Compromiso y Programa de Acción celebrado en Túnez, noviembre 2005.

Estas necesidades motivaron que el día 3 de septiembre de 2004, mediante Decreto No. 1090-04, la creación de la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), con dependencia directa del Poder Ejecutivo, autonomía financiera, estructural y funcional.

En el mismo orden, este decreto adhiere a la OPTIC, las funciones del Instituto Audiovisual de Informática (IADI), en la actualidad denominado Centro de Estudios de Tecnologías de la Información y Comunicación (CETIC) y de la Comisión Nacional de Informática (CNI), con la finalidad de integrar bajo un mismo seno las iniciativas de Tecnologías de la Información y Comunicación (TIC) y Gobierno Electrónico.

Al mismo tiempo, mediante Decreto No. 212-05, se crea la Comisión Nacional de la Sociedad de la Información y Conocimiento (CNSIC), con la responsabilidad de elaborar, desarrollar y evaluar la Estrategia Nacional de la Sociedad de la Información, la formulación de políticas derivadas de dicha estrategia y la definición de iniciativas, programas y proyectos para su realización.

Otros Decretos han sido emitidos, No. 228-07 y No. 229-07, en miras de institucionalizar el desarrollo e implementación de la Agenda Nacional de Gobierno Electrónico. Estos Decretos establecen el Centro de Contacto Gubernamental y el instructivo de aplicación de Gobierno Electrónico respectivamente.

1.1.2 Visión [3]

Ser la institución que impulse la transformación, el fortalecimiento institucional y la eficiencia del Estado, propiciando el desarrollo de la ciudadanía y del sector empresarial mediante el uso de las TIC.

1.1.3 Misión

Formular e implementar políticas, estrategias y controles que garanticen la mejora continua de los procesos, a través de las TIC en la administración pública, facilitando el acceso de los ciudadanos a los servicios del Estado.

1.2Valores

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), vela por una política de trabajo basada en los siguientes valores:

- Transparencia.
- Integridad.
- Ética.
- Compromiso.
- Innovación.
- Trabajo en Equipo.
- Excelencia.

[3] https://www.optic.gob.do/index.php/sobre-nosotros-m

1.3Política Integrada de Gestión[4]

La OPTIC se compromete a satisfacer las necesidades de los clientes, mediante el cumplimiento de los requisitos legales y normativos aplicables, la mejora continua de los procesos y servicios, con el fin de asegurar y mantener los sistemas de gestión de acuerdo a los estándares de calidad, seguridad de la información y los servicios de TI y así contribuir con la transformación del Estado Dominicano.

La OPTIC garantiza servicios de excelencia, profesionales, eficientes, disponibles y seguros a los ciudadanos dominicanos.

1.4 Organigrama[5]

Esta es la Estructura Orgánica, la misma se presenta ya certificada por el Poder Ejecutivo y El Ministerio de Administración Pública (MAP).

[4] http://optic.gob.do/index.php/sobre-nosotros-m
[5] https://www.optic.gob.do/index.php/sobre-nosotros/organigrama

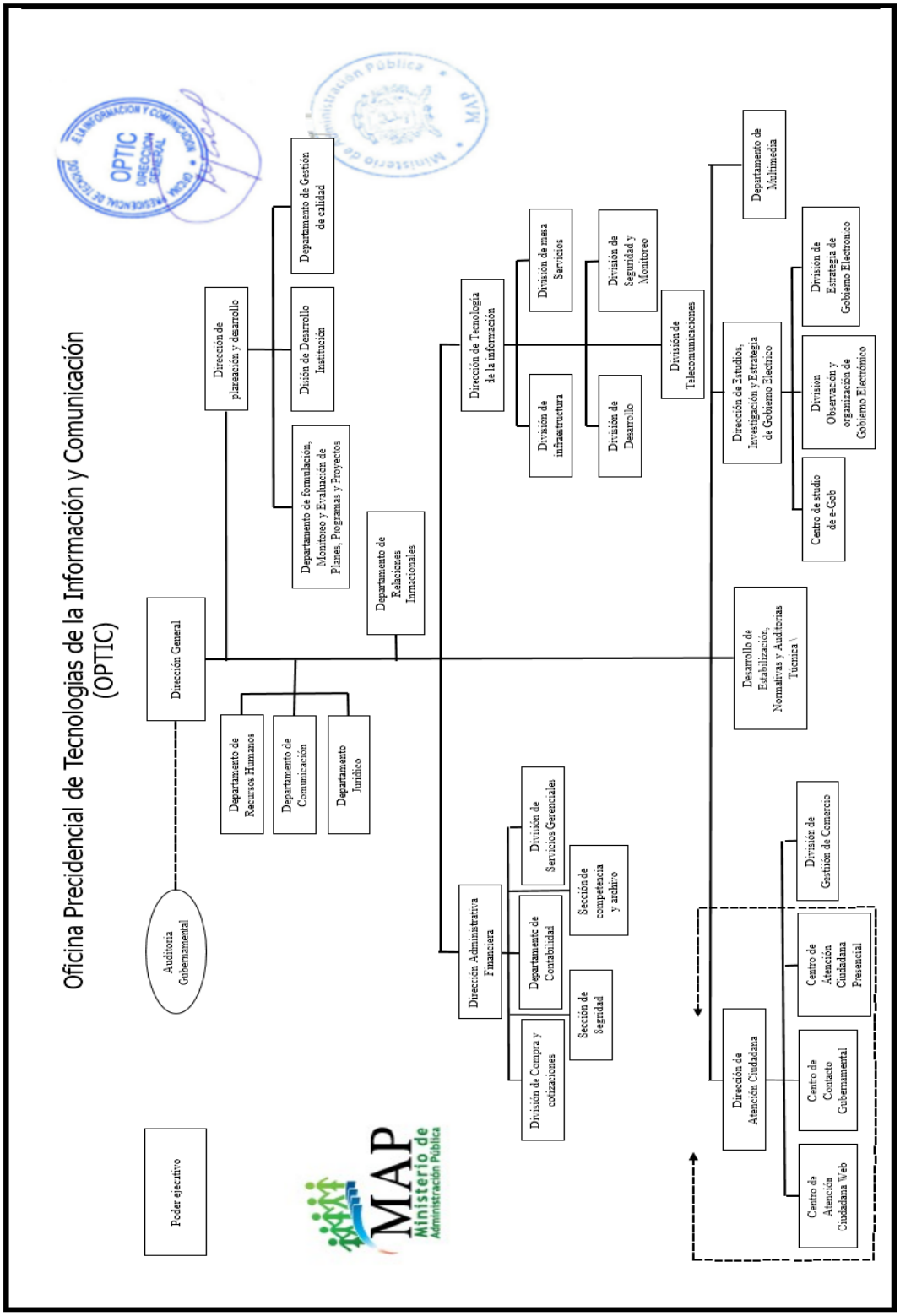


Figura 1. Dirección de diagnóstico y diseño organizacional, abril 2013

Fuente: www.optic.gob.do

1.5 Descripción de Puestos[6]

- Dirección General

Traza los objetivos y políticas desarrolladas en la planificación estratégica. Además, se encarga de coordinar, supervisar y controlar cada uno de las metas propuestas.

- Dirección Administrativa y Financiera

Esta dirección compuesta por la división de Compras y Contrataciones, Contabilidad, Servicios Generales, Seguridad y la división de Correspondencia y Archivo. Cada uno de estos departamentos vela por un bien en común, ya que una parte de esta dirección se encarga de la parte administrativa, en específico la parte operativa, como es la seguridad, servicios generales, correspondencia y archivo. Por otro lado, está la financiera, como son contabilidad, compras y contrataciones, la cual permite el buen funcionamiento económico que debe tener la organización.

- Dirección de Atención Ciudadana

Se compone del Centro de Atención Ciudadana, Centro de Contacto Gubernamental y Centro de Atención Ciudadana Presencial. El centro de atención ciudadana brinda informaciones vía internet, mientras que el centro de contacto gubernamental las ofrece vía telefónica. Por último, el centro de atención ciudadana presencial, que permite al ciudadano ir a un lugar en específico y realizar varios procesos; ya que se encuentran varias dependencias del Estado en ese local.

- Dirección de Tecnologías de la Información

Se encarga del buen funcionamiento de las Tics, ofreciendo servicios; tanto interno como externo, como es el alojamiento de portales, correos, creación de aplicaciones, entre otros.

[6] http://optic.gob.do/index.php/sobre-nosotros/departamentos

- Dirección de Tecnologías de la Información

Esta dirección realiza la planificación de los proyectos y el desarrollo de los mismos. Creando pautas a seguir para lograr la consecución del proyecto final.

- Dirección de Estudios, Investigación y Estrategia de Gobierno Electrónico.

Tiene por responsabilidad Planificar, dirigir e implementar la estrategia de Gobierno Electrónico mediante la promoción de actividades y proyectos TIC orientadas al ofrecimiento de servicios interactivos y transaccionales a los ciudadanos con énfasis en el gobierno central y las municipalidades, elaboración de Programas de Capacitación disponibles en el Centro de Estudios de e-Gob, la actualización del Observatorio de Investigación de Gobierno Electrónico y la página de Gobierno Electrónico según los avances nacionales e internacionales, Representar y participar en eventos nacionales e internacionales de gobierno electrónico con el fin de mejorar la imagen y posicionamiento internacional del país en asuntos TIC y de Gobierno electrónico.

- Departamento de Comunicaciones

Este departamento gestiona todo lo relacionado con la imagen, dígase, campañas publicitarias, comunicación estratégica, entre otros.

- Departamento Jurídico

Realiza gestiones de contratos, juicios laborales y administrativos. Cabe destacar que este departamento trabaja de la mano con la división de Compras y Contrataciones.

- Departamento de Recursos Humanos

Su función consiste en planear, organizar y desarrollar todo lo relacionado a promover el desarrollo eficiente del personal que conforma la institución.

- Departamento Estandarización, Normativas y Auditorias Técnica

Se encarga de crear y establecer normas y estándares tecnológicos aplicables a los organismos del estado dominicano, y auditar su correcta aplicación.

- Departamento de Relaciones Interinstitucionales e Internacionales

Promueve y apoya los procesos interinstitucionales a nivel nacional e internacional, a través, de los acuerdos de cooperación entre instituciones, que beneficien el desarrollo de la organización.

- Oficina de Libre Acceso a la Información Pública

Responsable de tramitar y facilitar las informaciones requeridas, igualmente, ser un canal de comunicación entre las organizaciones y ciudadanos.

1.6 Servicios [7]

Los servicios ofrecidos por la OPTIC son:

- **Servicios Estructura TIC**

Consiste en proveer asesoría a las unidades de Tecnologías de la Información y Comunicación para la implementación de la Estructura Transversal de TIC, como una plataforma para el desarrollo de las Tecnologías de la Información en los organismos gubernamentales y por consiguiente el desarrollo del Gobierno Electrónico, impactando positivamente los servicios que llegan a los ciudadanos.

- **Servicio de Asesoría Técnica en Implementación de Gobierno Electrónico**

Consiste en proveer asesoría técnica en las diferentes áreas de las Tecnologías de la Información y Comunicación (TIC) y Gobierno Electrónico a las Instituciones

[7] https://www.optic.gob.do/index.php/servicios-m

Gubernamentales e Instituciones Provinciales y Municipales, así como proveer soluciones para los mismos.

- **Servicio de Estadísticas Nacionales e Internacionales sobre el Avance de Gobierno Electrónico**

La División Observatorio e Investigación de Gobierno Electrónico es el departamento encargado de ofrecer información oportuna, objetiva, confiable, continua, actualizada y comparable en materia de Gobierno Electrónico de la República Dominicana. Estas estadísticas incluyen los índices y rankings de las instituciones gubernamentales en materia de e-GOB. Dichas estadísticas están disponibles en la sección de estadísticas de la OPTIC. Cualquier información adicional puede ser requerida por la parte interesada.

- **Servicio de Estructura TIC**

Consiste en proveer asesoría a las unidades de Tecnologías de la Información y Comunicación para la implementación de la Estructura Transversal de TIC, como una plataforma para el desarrollo de las Tecnologías de la Información en los organismos gubernamentales y por consiguiente el desarrollo del Gobierno Electrónico, impactando positivamente los servicios que llegan a los ciudadanos.

- **Solicitud de Asesoría Técnica**

Consiste en proveer asesoría técnica en las diferentes áreas de las Tecnologías de la Información y Comunicación (TIC) a las instituciones gubernamentales, así como proveer soluciones para los mismos.

- **Servicio de Certificación NORTIC**

Este servicio consiste en la asesoría, auditoría y posterior certificación bajo las NORTIC sobre el compendio de normas que regirán al Estado Dominicano en materia de TIC.

- **Servicio de Representación Internacional en Asuntos TIC**

Con el respaldo de alianzas estratégicas internacionales, la DIGOB hace la función de representante comercial internacional para la OPTIC y el Estado Dominicano en asuntos relacionados con Gobierno Electrónico, Gobierno Abierto y e-Municipalidades, donde actúa como Presentador del estado de implementación del Gobierno Electrónico en la República Dominicana e intermediario y procesador de oportunidades de servicios, proyectos y programas que beneficien y/o apoyen la implementación del e-GOB en nuestro país.

También se realizan servicio de cabildeo internacional, tendente a mejorar la posición Dominicana en los índices internacionales que miden el desempeño de la implementación de la Sociedad de la Información y el Conocimiento.

- **Servicio de e-GOB Provinciales/Municipales utilizando e-Voluntarios**

Consiste en proveer asistencia en la agenda de implementación de actividades y proyectos de Gobierno Electrónico en las localidades atendidas por el programa de Comités de Tecnología Provinciales/Municipales. También asisten en la recolección de información local de asuntos de e-GOB.

Adicionalmente coordinan con las diferentes instituciones locales para el uso de los CATC y las diferentes áreas de las Tecnologías de la Información y Comunicación (TIC) y Gobierno Electrónico a las Instituciones Municipales y/o Provinciales, así como proveer soluciones para los mismos.

- **Creación de Portales Gubernamentales**

Consiste en la creación de portales de internet para las instituciones, basados en las normas y estándares de portales gubernamentales.

- **Asistencia en la Implementación de Proyectos de Gobierno Electrónico**

Consiste en coordinar y/o ejecutar el plan de trabajo establecido para las soluciones tecnológicas definidas para dar respuesta a los requerimientos planteados.

- **Servicio de Asistencia en Formulación e Implementación de Estrategias y Proyectos de Gobierno Electrónico**

Este servicio asiste en crear estrategias que ayuden a implementar el Gobierno Electrónico en la República Dominicana. Consiste en proveer apoyo a las instituciones gubernamentales, provinciales y municipales para formular y plantear sus requerimientos TIC en términos de diseñar una solución tecnológica óptima que satisfaga los requerimientos de Gobierno Electrónico.

- **Correos Electrónicos a las Institucionales del Estado**

Este servicio tiene como finalidad proveer a organismos del Estado el alojamiento de sus respectivos Correos Electrónicos Institucionales, de manera eficiente y confiable.

- **Servicio de Asistencia en la Formulación de Proyectos de Gobierno Electrónico**

Consiste en proveer apoyo a las instituciones gubernamentales para formular y plantear sus requerimientos TIC en términos de diseñar una solución tecnológica óptima que satisfaga los requerimientos levantados.

- **Servicios de Capacitación de Gobierno Electrónico a Servidores Públicos**

Consiste en formar a los servidores públicos en los conocimientos y técnicas de informática, con miras a incorporar las nuevas Tecnologías de la Información y Comunicación dentro de los procesos de la Administración Pública para el desarrollo y modernización de la gestión pública.

Servicios de Atención Telefónica al Ciudadano Ofrecido en el CCG

- **Línea *GOB (*462)**

Línea cuya finalidad es ofrecer a los ciudadanos las informaciones, consultas y/o trámites de los servicios de las Instituciones de la Administración Pública.

- **Línea 700**

Línea de comunicación directa ideada por iniciativa del Despacho de la Primera Dama, a través de la cual los ciudadanos y ciudadanas tienen acceso a realizar denuncias de abuso de niñas, niños y adolescentes.

- **Línea 311**

Tiene como finalidad poner a la disposición del ciudadano una herramienta para realizar sus Denuncias, Quejas, Reclamaciones y/o Sugerencia relativas a cualquier entidad o servidor del Gobierno de la República Dominicana.

- **Servicio de Programa de Alfabetización Digital (PAD)**

Consiste en formar a los servidores públicos en los conocimientos y técnicas de informática, con miras a incorporar las nuevas Tecnologías de la Información y Comunicación dentro de los procesos de la Administración Pública para el desarrollo y modernización de la gestión pública.

- **Inclusión en el Centro de Contacto Gubernamental**

Radica en proveer un canal abierto a todas las instituciones para informar a los ciudadanos sobre el estatus de procesos y/o tramitación de documentos proporcionándole las facilidades para la actualización de datos sirviendo de vía alterna para realizar encuestas.

- **Creación de Portales Gubernamentales**

Consiste en el alojamiento de portales de Internet para instituciones del Estado, este provee la capacidad de gestión descentralizada. Cuenta con servicios adicionales de protección de correos contra virus y correos no deseados (spam), a su vez provee funcionalidad de conexión a bases de datos.

1.7Importancia[8]

La OPTIC es el organismo encargado de 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 implementación 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, garantizando el acceso equitativo a los mercados al sector productivo, como esfuerzo para la política de generación de empleo, asimismo, ofrecer mejor calidad de vida, crear oportunidades de educación, trabajo, justicia, cultura y recreación.

Su enfoque va desde:

- Asesorar la planificación estratégica; formular, gestionar, ejecutar y evaluar proyectos de tecnologías de información y comunicación (TIC) en las distintas instituciones de gobierno.
- Propiciar y apoyar la creación de redes de cooperación entre el sector público, privado y sociedad civil para facilitar y optimizar la gestión de los organismos gubernamentales y la contratación administrativa.
- Realizar investigaciones y estudios, promover la transferencia de conocimientos, información y nuevas tecnologías a la sociedad y a la comunidad empresarial.
- Comunicar y difundir el uso de las tecnologías de la información y comunicación (TIC) en la sociedad dominicana.
- Formular políticas e implementar el 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 tecnologías de información y comunicación (TIC).
- Asistir a las instituciones gubernamentales centralizadas, autónomas y descentralizadas en la identificación de oportunidades de implantación de tecnologías de la información y comunicación, para la mejora y eficiencia de la

[8] https://www.optic.gob.do/index.php/sobre-nosotros/marco-legal

función pública y en el diseño de proyectos de implantación identificados, sin perjuicio de la iniciativa que debe corresponder a cada entidad, buscando promover la adopción y uso de las tecnologías de la información y comunicación en las entidades públicas, particularmente para su mejor relación con los ciudadanos.

- Proponer políticas para difundir y promover la generación de una cultura de tecnología de la información y comunicación en el país.
- Participar en los proyectos de desarrollo, innovación, implementación e integración de las Tecnologías de la Información y Comunicación (TIC), cualquiera que fuese su fuente de financiamiento, a fin de optimizar las inversiones en el ámbito del sector público.
- 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.
- Coordinar, dar seguimiento y proponer ajustes y nuevos proyectos para la ejecución de la Agenda del Gobierno Electrónico.
- Preparar y proponer el instructivo presidencial para la aplicación y desarrollo de la agenda de Gobierno Electrónico 2005-2008.
- Proponer acciones y otros instructivos presidenciales que se entiendan necesarios en vías de garantizar la buena gestión y aprovechamiento de los recursos tecnológicos por parte del Gobierno y el país para insertarnos en la sociedad de la información.

1.8 Mercado Meta

La OPTIC se caracteriza por ser una institución que ofrece servicios a toda la ciudadanía dominicana que lo requiera. Uno de los principales canales que tiene la OPTIC para mantenerse a disposición de los dominicanos es mediante el Centro de Atención al Ciudadano (CAC), que permite la asistencia vía telefónica, internet y presencial, brindándole informaciones, servicios y tramites electrónicos de las diferentes dependencias y entidades del Estado Dominicano, facilitando así el acceso de la ciudadanía a los servicios e informaciones públicas.

1.9 Marco Legal

La OPTIC cuenta con una base legal que propone diseñar 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 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.

Las leyes y decretos bajo los cuales está estipulado el funcionamiento de la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) son los siguientes[9]:

- Decreto No. 178-05

Dispone la creación del Instituto Audiovisual de Informática, denominándose como Centro de Estudios de Tecnologías de la Información y Comunicación (CETIC).

- Decreto No. 1090-04

Crea a la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), como dependencia del Poder Ejecutivo, en fecha 3 de septiembre de 2004.

- Decreto No. 709-07

Se instruye a toda la Administración Pública del Estado Dominicano a cumplir con las normas y estándares tecnológicos redactados, aprobada y coordinada por la OPTIC.

[9] OPTIC (2014), tomado de http://optic.gob.do/index.php/sobre-nosotros/marco-legal

- Decreto No. 228-07

Se establece el Centro de Contacto Gubernamental *GOB (*462), canal de voz oficial, como primer punto de contacto y principal de comunicación para atención telefónica del Gobierno.

- Decreto No. 229-07

Sobre el desarrollo del Gobierno Electrónico.

- Decreto No.335-03

Reglamento de Aplicación de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales.

- Decreto No. 486-12

Se crea la Dirección General de Ética e Integridad que coordina junto con la OPTIC, los portales de transparencia de las instituciones del Estado.

- Decreto No. 694-09

Crea el Sistema 311 de denuncias, quejas y reclamaciones. Coordinado bajo la OPTIC, en el Centro de Contacto Gubernamental.

- Ley No.53-07

Ley sobre Crímenes y Delitos de Alta Tecnología.

- Ley No. 153-98

Ley General de las Telecomunicaciones.

- Ley No. 200-04

Ley General de Libre Acceso a la Información Pública.

- Ley No. 310-14

Ley que regula el envío de Correos Electrónicos.

- Decreto No. 130-05

Reglamento Aplicación Ley General de Libre Acceso a la Información Pública.

1.10 Uso e implementación del Gobierno Electrónico[10]

A través de la Oficina Presidencial de Tecnologías de la Información y Comunicación de la Republica Dominicana (OPTIC), el gobierno dominicano ha facilitado el uso de las TIC e implementación del gobierno electrónico, con el objetivo de evaluar los procesos principalmente en los servicios, eficiencia interna y transparencia en las instituciones públicas de la Republica Dominicana, sustentada de:

Uso de las TIC; permitiendo evaluar los recursos disponibles tanto humanos como tecnológicos, así como la existencia de controles que permitan el manejo correcto de los recursos.

Implementación de e-gob; evalúa los recursos para la implementación y mejores prácticas tanto nacionales como internacionales, datos abiertos, interoperabilidad e interacción con los ciudadanos a través de las redes.

Desarrollo de e-servicios; mide el nivel de desarrollo del servicio en cada institución gubernamental, así como el nivel de avance de los servicios. El índice de uso de TIC e implementación del gobierno electrónico de la Republica Dominicana correspondiente al 2015 es de 50.99%, mejorando un 2.97% sobre el 2014.

[10] http://sisticge.dominicana.gob.do/promediopais.php

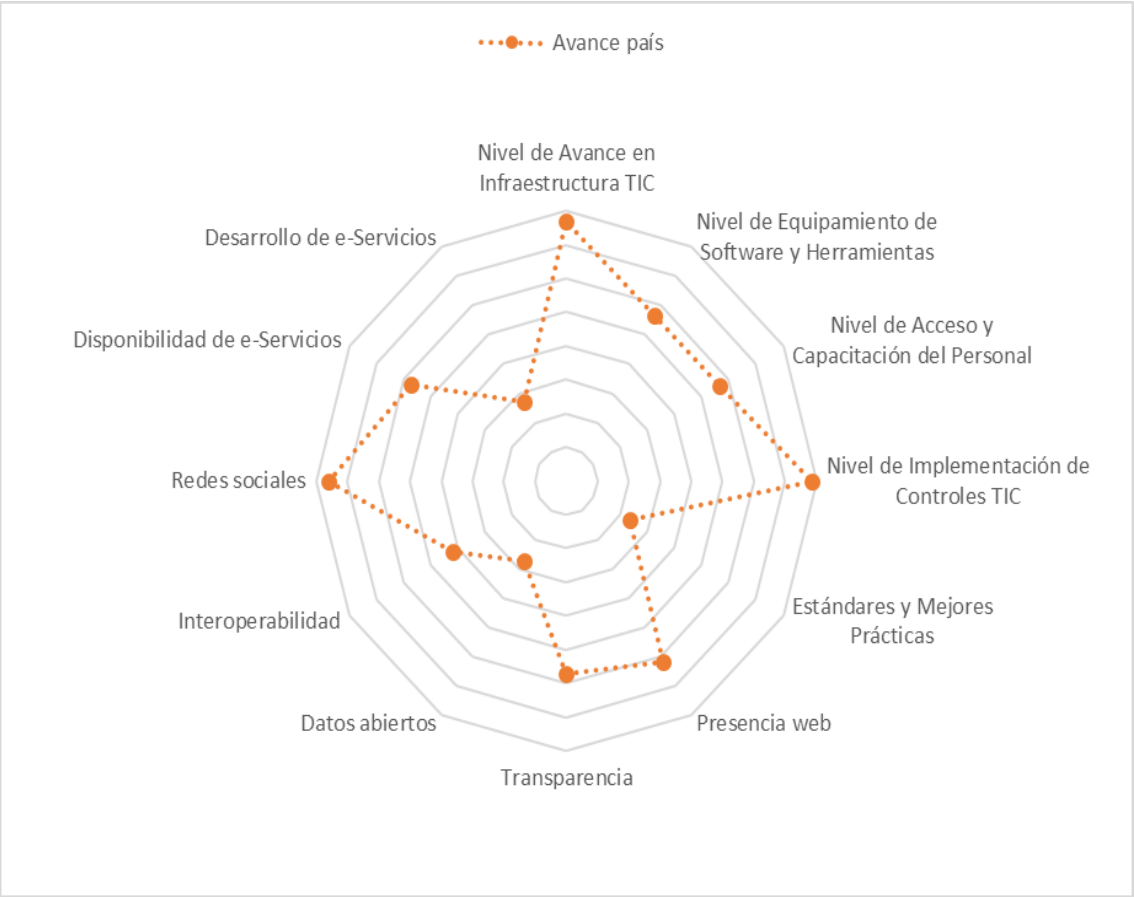


Figura 2. Índice de Uso de TIC e Implementación de Gobierno Electrónico (iTICge) de la República Dominicana, 2015

Fuente: http://sisticge.dominicana.gob.do/promediopais.php

Porcentaje de avance				
Año	Puntuación País	Uso de las TIC	Implementación e-Gob	Desarrollo e-Servicios
2014	48.02	61.32%	39.18%	29.81%
2015	50.99	68.30%	46.90%	31.85%

Tabla 1. Porcentaje de avance tecnológico 2014-2015

Fuente: http://sisticge.dominicana.gob.do/promediopais.php

República Dominicana	Peso categoría	Puntuación
iTICge 2015	100.00	50.99
USO DE LAS TIC	36.00	24.59
Nivel de Avance en Infraestructura TIC	10.00	7.71
Nivel de Equipamiento de Software y Herramientas	8.00	4.52
Políticas de software	4.00	1.96
Desarrollo de software	4.00	2.55
Nivel de Acceso y Capacitación del Personal	8.00	4.52
Brecha de género	3.50	1.56
Capacitación	2.00	1.33
Gestión de proyectos	2.50	1.63
Nivel de Implementación de Controles TIC	10.00	7.85
Seguridad física	2.00	1.51
Seguridad lógica	2.00	1.61
Otros Controles TIC	6.00	4.73
IMPLEMENTACIÓN DE GOBIERNO ELECTRÓNICO	40.00	18.76
Estándares y Mejores Prácticas	10.00	2.32
Buenas prácticas internacionales	6.00	1.26
Buenas prácticas nacionales	4.00	1.06
Presencia web	10.00	6.18
Presencia	5.00	3.72
Alineamiento del portal a normas establecidas	5.00	2.46
Transparencia	6.00	3.42
Datos abiertos	5.00	1.34
Interoperabilidad	4.00	1.68
Redes sociales	5.00	3.80
DESARROLLO DE E-SERVICIOS	24.00	7.65
Disponibilidad de e-Servicios	4.00	2.29
Desarrollo de e-Servicios	20.00	5.36
Informativos	6.00	3.43
Interactivos	6.00	0.96
Transaccionales	8.00	0.96

Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)
Avenida 27 de Febrero #419 casi esq. Núñez de Cáceres, Ens. Quisqueya, Santo Domingo, R. D.
Tel: (809) 286-1009 | Fax:1(809) 508-3691
info@optic.gob.do

Tabla 2. Uso de las TIC en República Dominicana 2015

Fuente: http://sisticge.dominicana.gob.do/promediopais.php

1.10.1 Modelo de Estructura Transversal TIC de la OPTIC

La incorporación de nuevas tecnologías conlleva cambios significativos hacia procesos y servicios cada vez más eficiente, la OPTIC ha desarrollado tres modelos de estructura transversal en los organismos gubernamentales, para garantizar las mejores prácticas internacionales, logrando elevar los niveles de transparencia y calidad de los servicios brindados, los cuales son:

Modelo de complejidad: Alto

Figura 3. Modelo A- Complejidad alto

Fuente: https://www.optic.gob.do/phocadownload/memorias-institucionales/MEMORIA-OPTIC-2012-20216.pdf

Modelo de complejidad: Medio

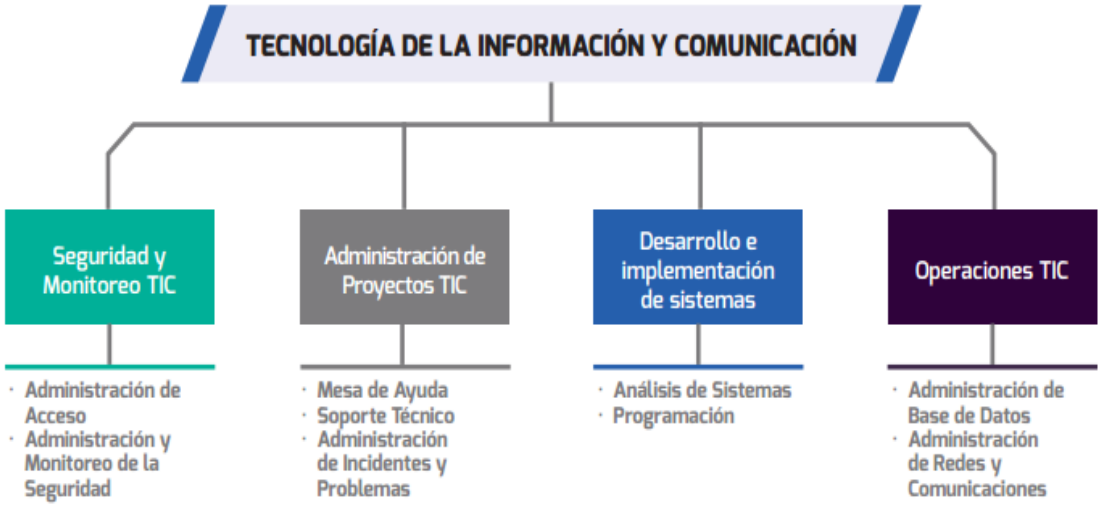


Figura 4. Modelo B- Complejidad media

Fuente: https://www.optic.gob.do/phocadownload/memorias-institucionales/MEMORIA-OPTIC-2012-20216.pdf

Modelo de complejidad: Bajo

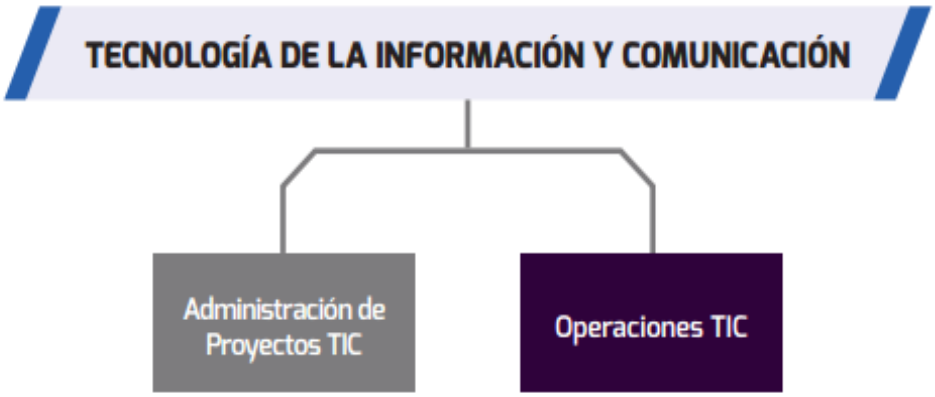


Figura 5. Modelo C- Complejidad baja

Fuente: https://www.optic.gob.do/phocadownload/memorias-institucionales/MEMORIA-OPTIC-2012-20216.pd

Conclusión

La República Dominicana ha logrado un gran avance, en el desarrollo y fortalecimiento del gobierno electrónico, lo cual ha sido de manifiesto ya que se ofrecen cerca de mil servicios de instituciones públicas que se encuentran al alcance digital de la ciudadanía dominicana. La Oficina Presidencial de Tecnologías de la Información y Comunicación ha jugado un papel fundamental en este proceso de avance ya que no solo ha realizados aportes a nivel de normativas y estándares, sino que además ha agregado plataformas tecnológicas con el fin de que sean la base para el desarrollo de nuevos servicios.

Las principales facilidades que brinda la OPTIC es a través del portal dominicana.gob.do en el cual se encuentra toda la información referente a los servicios en línea del Estado dominicano, cuenta con una plataforma de participación electrónica, garantiza asistencia y facilidades de accesibilidad para discapacitados y grupos vulnerables, así como facilidades electrónicas para las empresas.

Capítulo II

Datacenter

Introducción

Los centros de datos proporcionan un crecimiento constante, lo cual hace necesario realizar copias de seguridad periódicas que garanticen la operatividad. Por esa razón, un centro de datos se compone de una construcción robusta, que alberga los servidores, dispositivos, cables, conexión a internet, suministro de energía, refrigeración y sistemas en caso de incendios.

Este capítulo aborda uno de los temas más relevantes hoy en día, los datacenters o centros de procesamiento de datos. Un datacenter representa el cerebro de la institución, donde intervienen los procesos más críticos.

Se explica para que sirve y que beneficios nos provee la implementación a la infraestructura de la empresa. Detalla los componentes básicos de los Datacenter, características, aplicaciones y componentes que resulta fundamental para el correcto funcionamiento del servicio.

2. Datacenter

2.1 Concepto de Datacenter

Las empresas necesitan estar a la vanguardia tecnológica, lo que lleva a depender de una infraestructura física que permita hacer más eficiente y proporcionar la capacidad, además de cumplir con las necesidades.

Un Datacenter o centro de procesamiento de datos, es un espacio construido con una sofisticada infraestructura física y tecnológica, con determinadas características que lo hacen idóneo para alojar todo el equipamiento tecnológico de una compañía, brindando simplicidad, rapidez, seguridad y confiabilidad en los servicios, garantizando la continuidad del negocio.

Figura 6. Modelo Datacenter

Figura: http://data-flux.net/data-center-design-services/

Un Datacenter no cuenta con dimensiones predefinidas, este depende de la disponibilidad ya que puede ir desde un contenedor pequeño, hasta naves que alojan cientos de servidores.

En este sentido, las empresas manejan gran volumen de informaciones y aplicaciones, los cuales crecen exponencialmente, creando cierta dependencia del uso de un centro de datos, por ello, diseñar y construir el Datacenter como una unidad integral, en vez de un conjunto de partes que realicen actividades individuales, para así optimizar y mejorar el rendimiento obtenido.

Una infraestructura centralizada en maximizar la disponibilidad de los servicios de TI, que soporte la comunicación, las transacciones y recuperación de la información resulta vital para mitigar las posibles interrupciones. “en una infraestructura tecnológica, sin duda el datacenter es lo más crítico. Así, un banco necesita una operación de 7x24x365 y lo mismo pasa con los millones de usuarios que utilizan un servicio de alguna empresa”. (Schlez, 2012)

En base a esto, las interrupciones en el servicio por un diseño incorrecto, uso inadecuado, mala administración de los recursos y soporte ineficiente ponen en riesgo la efectividad de los servicios y por ende la continuidad del negocio. Dicho esto, resulta esencial el desarrollo y adaptación de normas en centro de datos.

2.2 Redes de Conexión Local

En la actualidad, el concepto de redes no es solo un conjunto de computadoras conectadas entre sí para compartir recursos y servicios. Las de redes involucran la conectividad móvil a una infinidad de servicios, que utilizan las personas y las organizaciones.

Las organizaciones cuentan con un conjunto de diferentes tecnologías para sus redes de datos. Internet es la base de muchas de ellas. Utilizando este medio, las mismas han logrado hacer negocios con sus productos o personas que realicen su trabajo a distancia.

Las primeras redes estaban limitadas a realizar el transporte de datos, generando gastos de operación y de servicio, en especial administraciones separadas. Para ser aplicadas en la estructura de la empresa, tres fases conforman el transporte de datos integrados. La primera es la convergencia de las redes, como el caso de los datos y la voz. La segunda son los servicios integrados, donde uno de ellos puede estar disponible para cualquier componente de la red, sin importar el medio de acceso.

2.2.1 Redes LAN y WAN

Según Pablo Gil Vázquez (2010), una red es un conjunto de dos o más dispositivos autónomos con la capacidad de interconectarse mediante un enlace de un medio físico. Un enlace es el medio de comunicación físico que transfiere los datos de un dispositivo a otro, donde cada punto representa un dispositivo. Las redes se pueden clasificar en función a la conexión de enlace

- Redes multipuntos o difusión, consta de un solo canal de comunicación compartido entre todos los equipos de la red, de tal manera, el paquete enviado es residido por múltiples destinos, lo cual el equipo recibe y procesa para verificar si corresponde al equipo, en caso contrario es descartado.
- Redes punto a punto, consta de varias conexiones entre pares de equipos, de tal manera el paquete visita multitud de puntos hasta llegar a su destino.

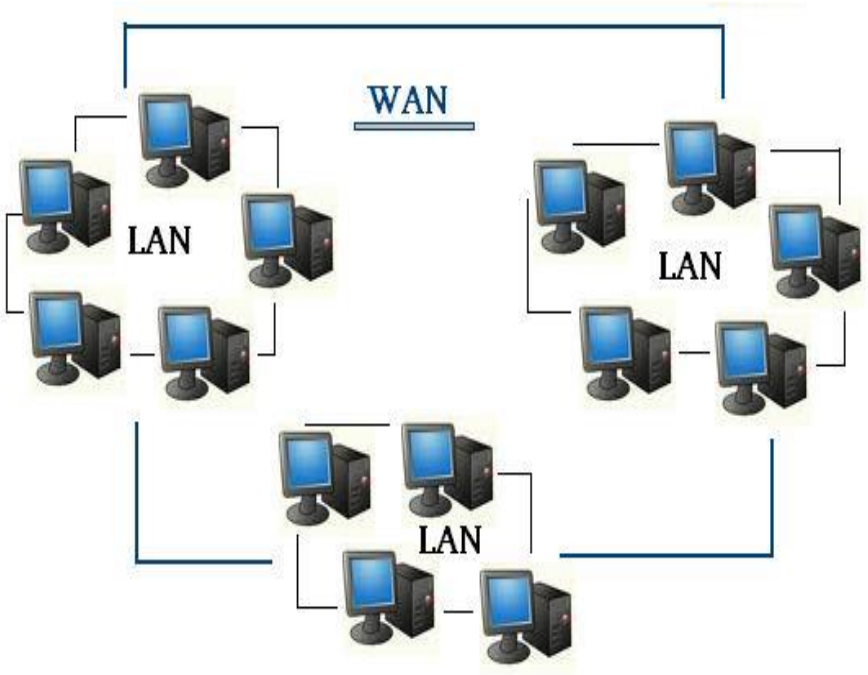


Figura 7. Red LAN y WAN

Fuente: http://danielredesit1.blogspot.com/2015/09/lan-y-wan.html

Las redes hoy son implementadas en diversas aplicaciones, clasificadas en base a la distancia o enlace, como se describe a continuación:

- Redes de Área Personal (PAN).
- Redes de Área Local (LAN).
- Redes de Área de Campus (CAN).
- Redes de Área Metropolitana (MAN).
- Redes de Área Amplia (WAN).
- Redes de Almacenamiento (SAN).
- Redes de Área Local Virtual (VLAN).

Redes de Área Local (LAN).

Las Redes de Área Local (LAN), son estaciones de trabajo conectadas a otros dispositivos localizados dentro de una misma edificación o áreas relativamente pequeñas, utilizados para conectar computadoras, estaciones de trabajo y dispositivos de acceso para compartir recursos e información.

Sin embargo, las Redes de Área Local (LAN) se limitan por:

- Tecnología de transmisión, existe el estándar IEEE 802.11, que la mayoría de los sistemas implementan, ya sea atreves de un cable o inalámbrico.
- Tamaño, permite extenderse hasta donde su medio físico lo permita.
- Velocidad de transmisión, depende del medio físico, ya sea cable o inalámbrico, dispositivo de computación y tarjeta de conexión.
- Topología, el tipo más implementado es red de bus que permite conectar todos los equipos lógicamente en una sola línea de transmisión.

Redes de Área Amplia (WAN).

Red de transmisión de datos, voz y video que se expande a un área geográfica extensa, la unión de varias redes LAN, esta ópera en los niveles más bajo del modelo OSI, es decir, capa física que describe las características eléctricas, operacional y funcional para los servicios y capa de enlace de datos.

La red capa WAN se caracterizada por:

- Dispositivos conectados a gran distancia.
- Utiliza conexiones en serie de varios tipos para facilitar el acceso a ancho de banda.

2.2.2 Cableado Estructurado de la Red[11]

En 1980, surgió una necesidad de unificar criterios, a la enorme difusión de las de datos en edificios que había en ese momento, para garantizar la compatibilidad entre sistemas y, sobre todo, flexibilizar el de este tipo de instalaciones, así nació el concepto de "cableado estructurado".

Los diferentes servicios de telecomunicaciones lo deben soportar el cableado estructurado, principalmente de voz y de datos, que se integran en un edificio. "Una instalación de cableado estructurado incluye los cables, como soporte físico para la transmisión de datos y todos los elementos (tomas, paneles, concentradores, etc.) que permiten conexionar los dispositivos de red". (Juan Carlos Martin Castillo, 2009).

Las características clave de un sistema de cableado estructurado es como voz/datos están conectadas exactamente iguales, siguiendo una topología en estrella con algún punto de distribución central, usando una combinación de medio (cableado y conectores) y hardware que puede aceptar cualquier necesidad de aplicación que pueda ocurrir a lo largo de la vida del cableado.

[11] http://www.inevid.com/2014/09/conceptos-basicos-sobre-el-cableado-estructurado.html

Las principales ventajas del cableado estructurado son las siguientes:

- Es un sistema abierto que puede recibir dispositivos de diferentes fabricantes.
- Se caracteriza ser flexible en el momento de hacer transformación o reestructuración del cableado.
- Su administración es sencilla, tanto desde el punto de vista de la instalación como de software.
- En la búsqueda de averías, se pueden retraer zonas de la instalación, dejando en funcionamiento las no afectadas.

Diseño de Cableado Estructurado

El sistema de cableado debe soportar un ambiente multi-producto y multi-marca, tomando en cuenta:

- Cableado Horizontal; cableado que se extiende desde el panel de parcheo o terminal a la conexión de cada área de trabajo, la distancia entre una terminal a otra debe tener un máximo de 90 metros para cobre y 300 metros en fibra.

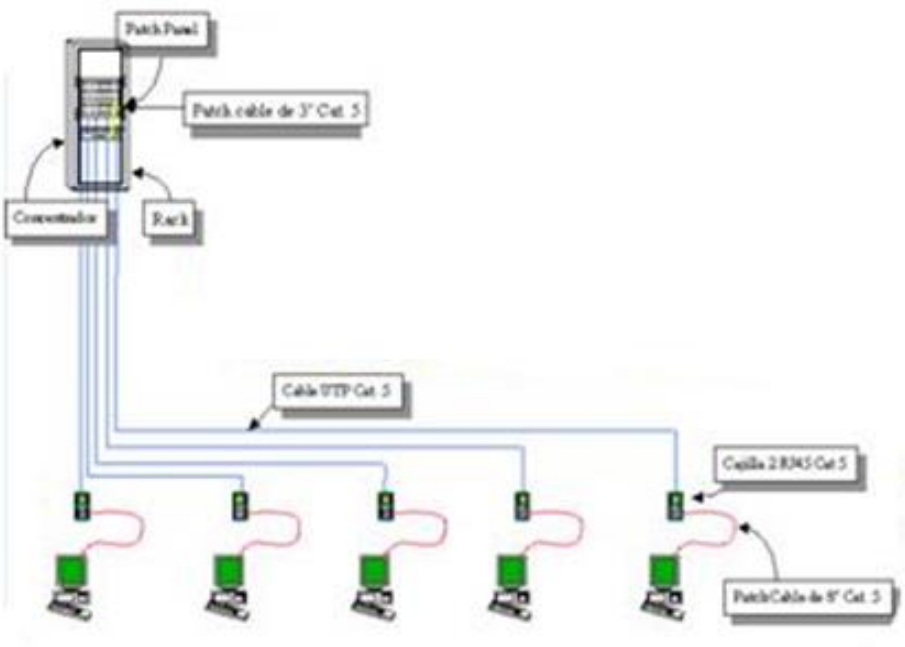


Figura 8. Diagrama cableado estructurado horizontal

Fuente: http://cableado-horizontal.blogspot.com/

- Cableado Vertical o Backbone; corresponde al cableado que une las conexiones entre las áreas, puede ser tendido de fibra óptica, coaxial o par trenzado, sin embargo, lo usual es usar cable UTP o fibra óptica.

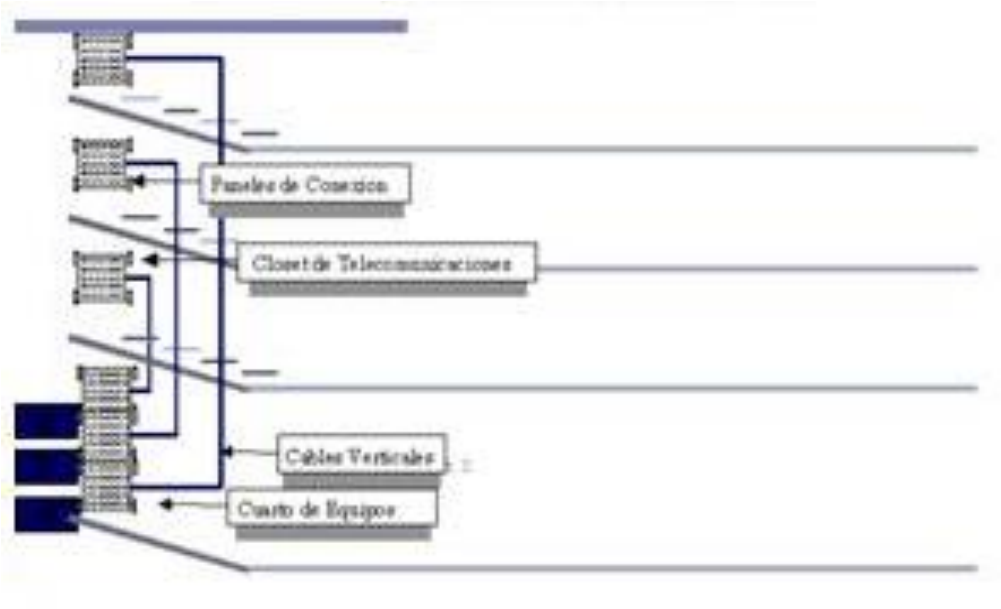


Figura 9. Diagrama cableado estructurado vertical

Fuente: http://cableado-horizontal.blogspot.com/

Categorías del Cableado

Es usual acertar con las denominaciones de categorías, ya que los cables o elementos de red están esquematizados para trabajar en una categoría determinada. Teniendo en cuenta de las categorías se pueden integrarse a una instalación normalizada de cableado estructurados.

CATEGORIA DE LOS CABLES UTP		
CATEGORIA	**DESCRIPCION**	**ANCHO DE BANDA**
Categoria 1	Actualmente no reconocida por TIA/EIA. Es utilizado para las conexiones telefónicas RBT y RDSI y cableado timbrado.	
Categoria 2	Actualmente no reconocida por TIA/EIA. Es utilizado en redes Token Ring y puede transferir datos hasta de 4Mbps.	
Categoria 3	Actualmente definido en TIA/EIA-568-B. Es utilizado para redes Ethernet a velocidades de 10Mbps. Diseñado para transmisión a frecuencia de hasta 16Mhz.	16Mhz
Categoria 4	Actualmente no reconocida por TIA/EIA. Es utilizado en redes Token Ring y puede transferir datos hasta de 16Mbps. Diseñado para transmisión a frecuencia de hasta 20Mhz.	20Mhz
Categoria 5	Actualmente definido en TIA/EIA-568-B. Es utilizado para redes Fast Ethernet para transmitir datos hasta 100Mbps y Gigabit Ethernet 1,000Mbps. Diseñado para transmisión a frecuencia de hasta 100Mhz.	100Mhz
Categoria 6	Actualmente definido en TIA/EIA-658-B. Usado en redes Gigabit Ethernet. Diseñado para transmisión a frecuencia de hasta 250Mhz.	250Mhz
Categoria 6A	Actualmente definido en IEA/EIA-568. Usado en redes de 10 Gigabit Ethernet. Diseñado para transmisión a frecuencia de hasta 500Mhz.	500Mhz
Categoria 7	Categorizado para cable de 600Mhz según la norma internacional ISO-11801. Usado en redes 10 Gigabit Ethernet y comunicaciones de alta confiabilidad.	600Mhz
Categoria 7A	Categorizado para cable de 1,000Mhz según la norma internacional ISO-11801-AD-1 de 2008. Usado en redes 10 Gigabit Ethernet y futuras comunicaciones de mayor velocidad de transmisión de datos.	1,000Mhz

Tabla 3. Categorías de los cables UTP

Fuente:https://books.google.com.do/books?id=V6IzqqDcfF8C&pg=PA85&dq=Categor%C3%ADas+del+cableado&hl=en&sa=X&ved=0ahUKEwjo3cPi1NXPAhXGHR4KHUCLAKkQ6AEIJTAB#v=onepage&q=Categor%C3%ADas%20del%20cableado&f=false

Las categorías tienen establecidos números en función de velocidad que pueden soportar en cableado. Cuanto más bajo es este número, más baja es dicha velocidad.

2.2.3 Topologías en Red

Cisco define la topología de red como la estructura de cómo encuentra establecida una red, las cuales pueden ser físicas o lógicas.

Topología Física

Se refiere a la forma que adopta el plano esquemático del cableado o estructura física de la red. Dividida en:

- Topología Bus

En esta topología se usa un solo cable backbone,[12] donde se encuentran conectados los huts. “Todos los dispositivos están conectados a un cable central llamado bus o backbone”. (Sánchez, 2013)

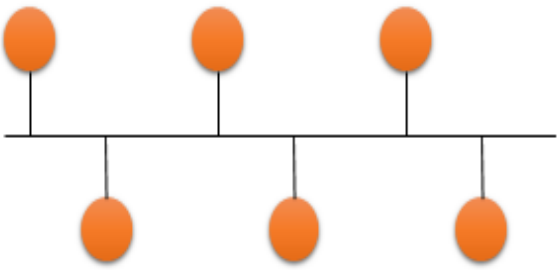


Figura 10. Topología Bus

Fuente: Los autores

[12] Backbone, se refiere al cableado troncal o subsistema vertical en una instalación de red de área local.

- Topología Anillo

En esta topología se conecta un host con el siguiente y el ultimo con el primero, creando un anillo físico de cable.

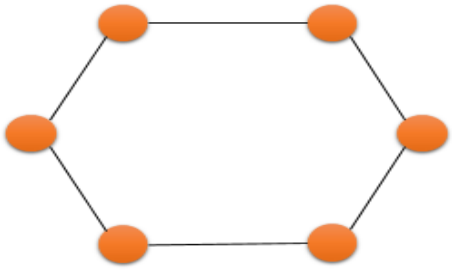


Figura 11. Topología anillo

Fuente: Los autores

Es utilizada muy frecuente en redes muy centralizadas o en sistemas de control. “Un ejemplo frecuente en redes locales, es la adaptación de una central telefónica privada con conmutación de circuitos (APBX) a la interconexión de sistemas o recursos informáticos situados en plantas o edificios contiguos” (Muñoz).

- Topología Árbol

Topología en árbol o jerárquica es similar a una topología estrella extendida, pero el sistema se conecta con un procesador principal “Es una topología híbrida. Grupos de redes en Estrella son conectados a un bus o backbone lineal” (Sánchez, 2013).

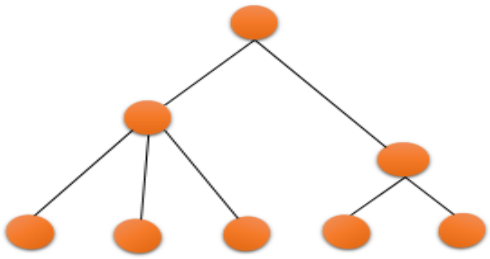


Figura 12. Topología árbol

Fuente: Los autores

- Topología Estrella

La topología en estrella conecta todos los cables con un punto central de concentración. “Todos los dispositivos están conectados a un concentrador central también llamado hubs, que es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás. Los nodos se comunican en la red a través del concentrador” (Sánchez, 2013)

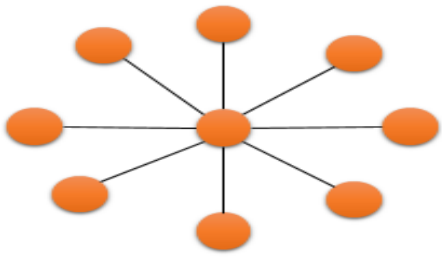


Figura 13 Topología estrella.

Fuente: Los autores

En esta topología los datos pueden transmitirse a una velocidad de 2,5 megabytes por un segundo por medio de un mismo cable, ya sea coaxial o par trenzado.

- Topología Estrella Extendida

Una topología en estrella extendida permite conectar estrellas individuales entre sí, logrando extender el alcance y cobertura de la red a través del uso de la conexión de huts.

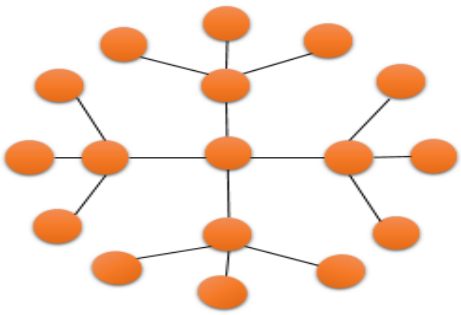


Figura 14. Topología estrella extendida

Fuente: Los autores

- Topología Malla

En esta topología proporciona mayor protección generando redundancia hacia posibles interrupciones del servicio. Las estaciones de trabajo están conectadas a diferentes interconexiones redundantes entre los nodos de la red. En esta topología podemos verificar que cada uno de los nodos se conecta con todos los nodos de la red.

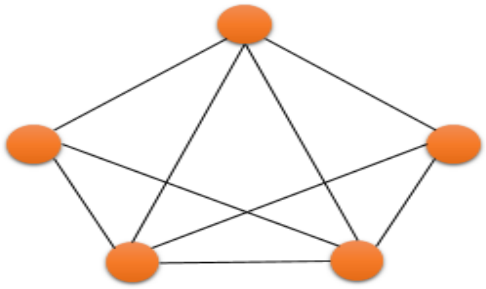


Figura 15. Topología en malla

Fuente: Los autores

Topología Lógica

Describen la forma de comunicar los hosts a través del medio físico, además de reconocer cada conexión de estación de trabajo. Las topologías lógicas son:

- Broadcast

Permite difundir simultánea paquetes a varios destinatarios. Esta disfunción puede darse en dos tipos, alto nivel y bajo nivel.

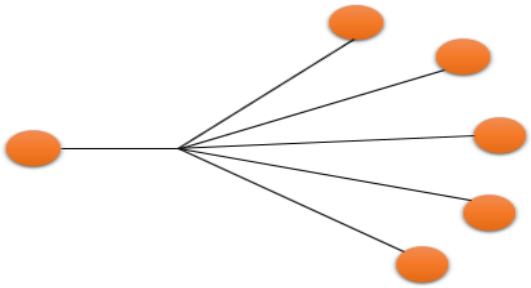


Figura 16. Broadcast

Fuente: Los autores

- Transmisión de Token

Controla el acceso a transmisión en la red mediante la transmisión de token eléctrico a cado host de manera secuencial, de tal amera que realiza un bucle entre los hosts hasta llegar al último host.

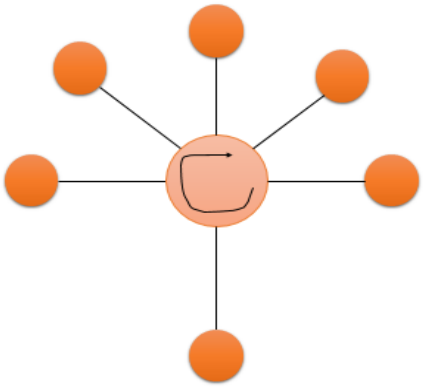


Figura 17. Transmisión de token

Fuente: Los autores

2.3 Niveles de Redundancia

Para un Datacenter estar siempre disponible es la tarea principal, sin embargo, existen fallas en el sistema que provocan permanecer un tiempo fuera de servicio, ya sea corto plazo o prolongado.

Los sistemas con alta disponibilidad cuentan con nivel integrado de redundancia, divididos en cuatro tipos:

- Redundancia Activa.
- Redundancia Pasiva.
- Redundancia Diversa.
- Redundancia Heterogénea.

2.3.1 Infraestructura de Telecomunicaciones para Datacenter TIA/EIA-94213

Los servicios son de suma importancia en un ambiente diseñado para los equipos de telecomunicaciones deben estar disponibles ininterrumpidamente para desempeñar las diversas actividades, por ende, representan la parte critica de toda la infraestructura.

El Datacenter de un espacio destinado para albergar los dispositivos necesarios para el procesamiento de información, siendo capaz de adaptarse al crecimiento y reconfiguración al mismo tiempo ser confiable y seguro.

La norma TIA-942 fue publicada por primera vez en abril del 2005 con la intensión de cubrir el diseño de la infraestructura, tomando en cuenta el espacio, cableado, consideraciones de ambiente y organización en los equipos.

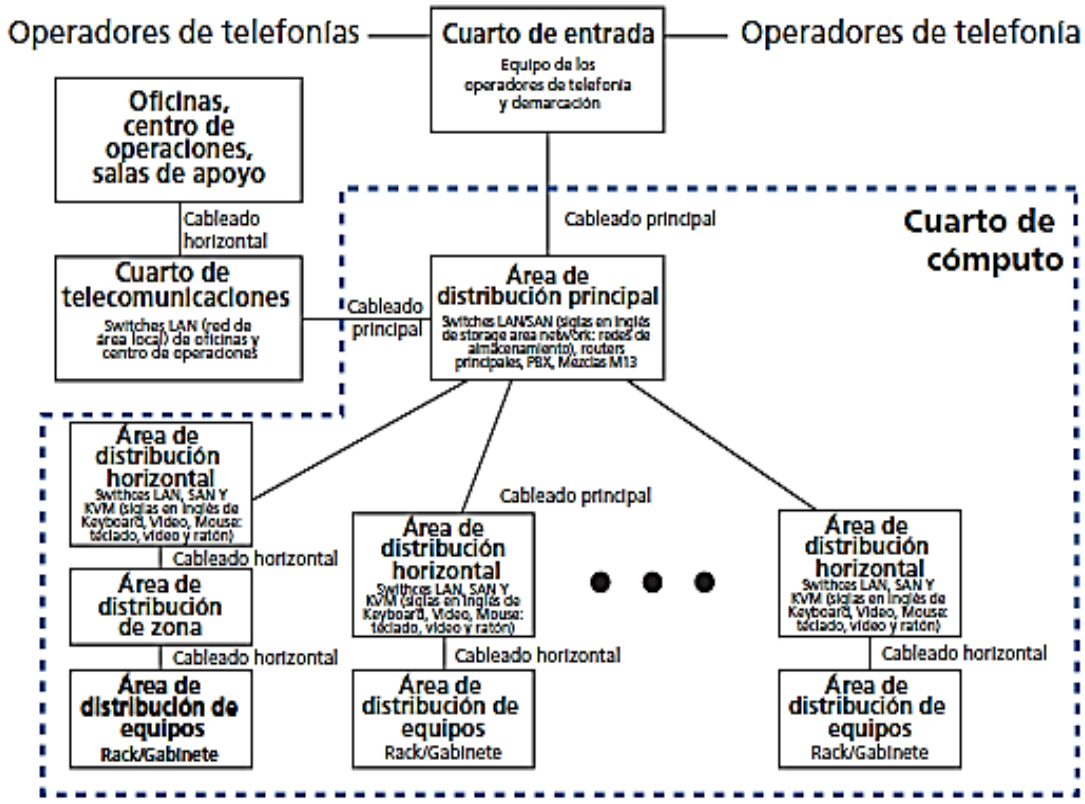


Figura 18. Descripción centro de datos que cumple norma TIA-942

Fuente: Norma ANSI

[13] Sitio de TIA-www.tiaonline.org/standars

La norma TIA-942 establece que se debe dividir en diversas áreas de la manera más óptima, las cuales son:

- Uno o más cuarto de entrada; aloja el equipo de los operadores telefónico, puede estar ubicado dentro del centro, aunque lo recomendable es que se encuentre fuera por motivos de seguridad.
- Área de distribución principal; contiene el sistema de cableado estructurado del centro de datos. La norma específica racks separados para los cables de fibra óptica, UTP y coaxial.
- Área de distribución horizontal; ubicación de las interconexiones horizontales del cableado hacia las áreas de distribución.
- Área de distribución de zona, cableado para los equipos que van desde el suelo.
- Área de distribución de equipos; correcta ubicación de los gabinetes y racks colocados “hot aisle/cold aisle” dispersados de manera eficaz.

2.3.1.1 Niveles de Redundancia (TIER)

TIER es una metodología estandarizada calcula el tiempo de disponible en el Datacenter. Para evitar estar fuera del servicio por un tiempo extenso TIA-942 consta de cuatro niveles de redundancia o TIER, así tener un Datacenter menos susceptible a interrupciones (López-Vázquez, 2012). Las características básicas de cada nivel son:

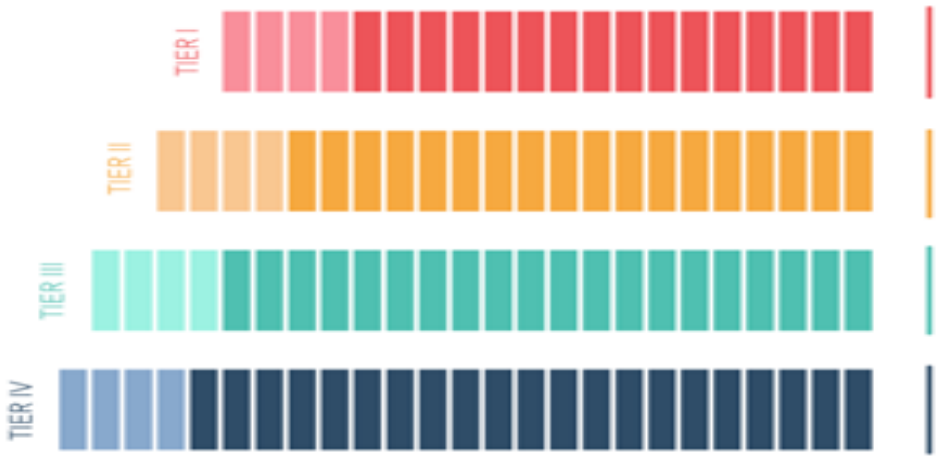


Figura 19. Niveles o TIER de redundancia

Fuente: https://ixaya.net/knowledgebase/17/Niveles-Tier.html

TIER I

TIER I es el nivel más básico, en este nivel la disponibilidad es de 99.67%. Sin embargo, no se alcanza a disponer de unidades redundante para el sistema, además de tener una sola instalación de distribución eléctrica. Puede carecer de suelo técnico. Cuenta con cierta tolerancia a fallos. Los sistemas alternos están interconectado a la instalación principal. El servicio es suspendido generalmente 29 horas anuales para ofrecer mantenimiento.

TIER II

TIER II o componentes redundantes, implica la necesidad de mayor capacidad para continuar funcionando, aunque se presenten fallas en el sistema, dispone de suelo técnico, cuenta con un segundo punto de acceso para los servicios, su disponibilidad es 99.75%. El servicio es suspendido para ofrecer mantenimiento, aproximadamente 29 horas anual.

TIER III

TIER III o mantenimiento simultaneo, permite realizar operaciones de mantenimiento sin provocar caída en el sistema con redundancia en los equipos (N+1), aunque solo dispone de una ruta activa, lo que implica que los componentes redundantes se encuentran en la ruta principal, asegurando disponibilidad temporal de 99.98%.

TIER IV

TIER IV o CPD, nivel más alto en un Datacenter, es considerado el más robusto y menos propenso a fallas. Está diseñado para mantener el servicio en los subsistemas sin que se interrumpa el servicio. Consta de múltiples rutas de circuito, red, enlace de datos, almacenamiento, energía eléctrica y refrigeración, además de tener cableado y redundancia separadas. La carga máxima admisible es del 90% y la disponibilidad es 99.99%, el cual es el índice más alto a tolerancia fallos.

Similitudes y diferencias de TIER				
Caracteristicas	**TIER I**	**TIER II**	**TIER III**	**TIER IV**
Numero de líneas de suministro	Solo 1	Solo 1	1activo 1pasivo	2 activo
Componentes redundantes	N	N	N+1	2(N+1) or S+S
Espacio de apoyo a la proporción de suelo elevado	20%	30%	80-90%	100%
Voltios iniciales/ft²	20-30	40-50	40-60	50-80
Voltios finales²	20-30	40-50	100-150	150+
Altura del piso	12"	18"	30-36"	30-36"
Libra de carga de baldosa/ft²	85	100	150	150+
Voltaje de suministro	208,480	208,480	12-15KV	12-15KV
Tiempo para poner en practica	3	3 to 6	15 to 20	15 to 20
Año desplegado por primera vez	1965	1970	1985	1995
Construcción $/ ft² piso elevado	$450	$600	$900	$1,100+
Tiempo de inactividad de TI anual	28.8hrs	22.0hrs	1.6hrs	0.4hrs
Disponibilidad del sitio	99.67%	99.75%	99.98%	100.00%

Tabla 4. Similitud y diferencia de TIER.

Fuente: Tier Classifications Define Site Infrastructure Performance, por: W. Pitt Turner IV, P.E. and Kenneth G. Brill

2.4 Seguridad de las Instalaciones de un Datacenter

En un mundo de cambios, la seguridad informática es la base de la continuidad de los servicios, donde nos encontramos expuestos a riesgos, catástrofes y contingencias que abundan impidiendo la integridad, confidencialidad y disponibilidad de los datos. En el caso de los centros de datos, la seguridad es fundamental, ya que contienen informaciones, aplicaciones y sistemas esenciales en el funcionamiento, lo que nos lleva a crear un ambiente de seguridad acorde a la importancia de la información almacenada, tomando en cuenta el impacto que producirá en caso de incidentes.

El 11 de agosto de 1999, se produjo un incendio en el Centro de Control de United Airlines, en Elk grove, Ilinois, que pospuso alrededor de 24,000 vuelos que transportaban 300,000 personas (Conroy). El impacto financiero pudo haber sido tremendo a no ser por el desarrollo e implementación de un plan de contingencia ante desastres, que incluía una instalación redundante, que en su momento costo millones de dólares, la aerolínea, hubiese tenido pérdidas significativas.

Actualmente el motor o el activo más valioso de las empresas es la información, tomando en cuenta que ahí se materializa los bienes más importantes de la compañía. Una de las funciones básicas es eliminar los riesgos potenciales. Lo ideal en los centros de datos, es mantener la disponibilidad, evitando estar el menor tiempo fuera de servicio para ello es impórtate disponer de una política de seguridad que respalde la información y el servicio en la organización. Definir una política de seguridad necesita un enfoque hacia los recursos que se desean mantener, y los cuales el sistema no puede evitar o ser expuesto tomando en cuenta:

¿Qué se está protegiendo? ¿Cuáles consideraciones deben tomarse en cuenta? ¿Qué tan expuestos nos encontramos? ¿Qué importancia representa? ¿Cuáles medidas puedo evaluar?

Una investigación de la universidad de Texas revela que de las empresas que sufren una pérdida significativa, el 43% no se recupera, el 51% lleva al cierre de la empresa en un estimado de dos años, y solo el 6% puede mantenerse activa, enfrentando las perdidas, tanto del sistema como materiales.

Cabe señalar que existen pérdidas, no solo económicas, sino también hay otros factores que interrumpen la disponibilidad, como:

- **Costo Directo**, influye en la parte financiera de la empresa, son más fáciles de identificar, por ejemplo;
  - ❖ Perdida de transacciones.
  - ❖ Perdida de operaciones.
  - ❖ Tiempo de recuperación de servicios.
  - ❖ Demandas por incumplimiento.

- **Costo Indirecto,** posibles situaciones de las cuales no tienen certeza, aunque se sabe que existen. Su impacto va:
  - ❖ Insatisfacción del usuario final.
  - ❖ Daño a la imagen de la empresa.
  - ❖ Malas relaciones públicas.

- **Costo de Oportunidad**, porcentaje de utilidades perdidas por inactividad en el servicio, o aun peor, pérdida de clientes no de la venta.

  De ahí surgen las estrategias que garanticen el funcionamiento de los procesos del sistema, proporcionando información remota, control y en caso de ser necesario emisión de alarma, segmentadas en:
  - ❖ **Seguridad Lógica,** esta contiene las herramientas necesarias para minimizar, controlar y prevenir las amenazas proporcionando la seguridad de la red.
  - ❖ **Seguridad Física,** esta protege los procedimientos de control de los recursos e información confidencial.
  - ❖ **Seguridad en la Red,** consiste en ofrecer protección en tiempo real.

A través de ello se persigue soluciones que garanticen la productividad de los equipos, definiendo la responsabilidad que requiere cada estrategia de diseño, mantenimiento el servicio tanto de los equipos e infraestructura.

En base a esto, las soluciones de seguridad abordan requisitos en el entorno de la nube, mediante perfiles dinámicos que exploran las vulnerabilidades de las aplicaciones tanto privadas como públicas, tales como:

- Sistema de detención de intrusos (IDS), brinda protección ante amenazas.
- Sistema de control de prevención de intrusos (IPS) respuesta más completa e inmediata ante amenazas.
- Seguridad en el contenido y virtualización.

Por ende, la seguridad es un factor de suma importancia, siendo necesario contar con una solución que proporcione monitoreo constante de los datos, posibles vulnerabilidades y los accesos de la base de datos a usuarios. No obstante, es natural encontrar fallas en las operaciones, es decir, posibles riesgos en los servicios. (Coloritto, Rodrigo, 2013)

2.4.1 Vulnerabilidades de los Sistemas de un Datacenter

Las amenazas y vulnerabilidades sufren constantes actualizaciones, por ende, segmentar las operaciones para obtener un ambiente protegido por un personal capacitado, amerita tiempo y dinero que resulta innecesario, cuando es posible implementar monitoreo y evaluación constante a través de un datacenter.

Las nuevas tecnologías de TI ofrecen equipos más completos y potentes fomentando una arquitectura rígida e inflexible, que permita subdividir los puntos de riesgo de la seguridad y el impacto que presenta, mitigando los riesgos que puedan presentarse.

Identificar las prioridades es vital para establecer los niveles de redundancia, logrando satisfacer las necesidades planteadas, brindando: alta disponibilidad, reducción de costos, agilidad y flexibilidad en el servicio y valor agregado a los servicios

Por su parte, debemos determinar los puntos clave de la infraestructura. Se necesita una arquitectura íntegra, sobre todo que brinde protección completa tanto el centro de datos, como la nube. Tomando en consideración que los riesgos físicos y amenazas que podría encontrarse expuesto.

Conclusión

La tecnología de la información juega un papel clave en las empresas de la actualidad, debido a la sistematización de los procesos de negocio. Los centros de datos han tomado un rol esencial debido a que son los que poseen la infraestructura tecnológica que soportan dichos procesos.

Es necesario entender que más allá de lo técnico, la administración de un datacenter se debe enfocar en el negocio. Por tal razón se debe tomar en cuenta la continuidad operativa, la disponibilidad de los servicios y la seguridad de la información. Cada uno de estos aspectos se relacionan entre si y son los que agregan valor a la empresa.

Se puede concluir que el valor estratégico de un datacenter estará directamente relacionado a la administración del mismo. Por eso se debe considerar, no solo mantener los estándares de la industria, sino acoplarse al negocio con el fin de satisfacer las necesidades de la empresa.

Capítulo III

Cloud Computing

Introducción

Las compañías a medida que escalan en el mundo empresarial, experimenta diversas evoluciones, impulsadas por los avances tecnológicos de mercado, que permiten aumentar la eficiencia en los procesos, disminuyendo los costos además de obtener mejor tiempo de respuesta, de ahí surge la necesidad del uso de cloud computing.

La computación en la nube es un paradigma relativamente nuevo, que permite acceso propagado a un conjunto de recursos informáticos configurables en la red, tales como: redes, servidores, aplicaciones y servicios, que puede ofrecer autoservicio bajo demanda, acceso a la red, expansión rápida y servicios medidos.

En este capítulo se hace mención de las principales ventajas de este servicio, generando múltiples beneficios a la vez de la combinación de servicios de diferentes proveedores en un mismo servicio, con la implementación de la computación en la nube o Cloud Computing.

3. Cloud Computing

3.1 Concepto

El término de Cloud Computing (Nube Computacional) ha sido desde sus inicios objeto de controversia y debate. La mayoría de personas puede verlo como un conjunto de tecnologías, este concepto es cierto pero la realidad Rountree & Castrillo dice, “la nube actual es un conjunto de servicios”. (The Basics of Cloud Computing, 2014)

La nube fue pensada como un conjunto de servicios, tecnología y actividades combinadas. Esto ha provocado que el concepto actual de la nube sea un poco difícil de entender, ya que lo que sucede dentro de esa combinación no es conocido por el usuario del servicio. La realidad es que la mayoría de los usuarios no le importa que sucede detrás de la nube más bien solo quieren obtener un buen servicio, solo unos pocos se interesan conocer el proceso de cómo funciona el servicio.

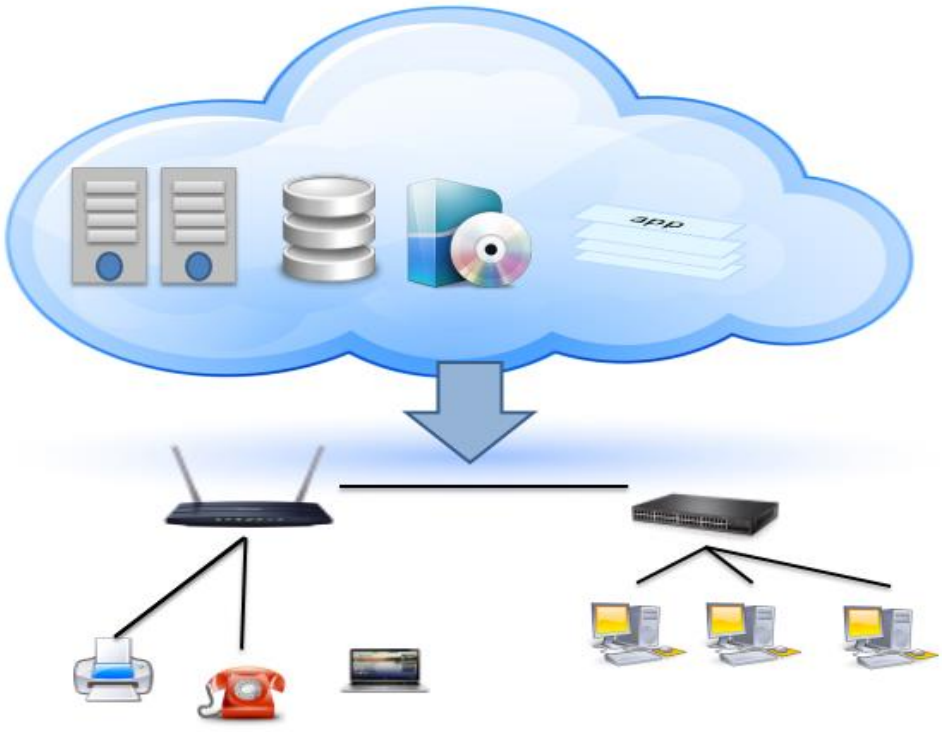


Figura 20. Cloud Computer.

Fuente: Los autores, auxiliado de NIST

El National Institute of Standards and Technology (NIST)[14] define computación en la nube como: un modelo que proporciona, mediante la red y según se requiera (en demanda), acceso a un conjunto compartido de recursos de computo configurables, e. g. redes, servidores, almacenamiento, aplicaciones y servicios ubicados en el Datacenter.

Como todo servicio, la nube y los servicios que ofrecen han ido cambiando y evolucionando a través del tiempo, buscando satisfacer a las necesidades de los usuarios. Esto también ha sido parte de la confusión del término nube, ya que cada vez que alguien viene con una buena definición, el servicio cambia.

Para poder obtener un concepto claro de la nube, se enfocará las cuatro características clave, que un servicio debe tener para considerarse una nube:

- Auto-Servicio Bajo Demanda

Esta característica es la capacidad que debe tener el servicio que permita que en cliente pueda solicitar y recibir acceso al servicio requerido sin necesidad de tener que establecer contacto con el administrador del mismo. El proceso de solicitud y entrega debe ser automatizado, lo cual brinda ventaja tanto al proveedor del servicio como al cliente.

La implementación del auto-servicio permite que el cliente pueda solicitar y acceder a los servicios que necesita en el momento que lo necesita. Por el contrario, a este modelo, en los ambientes tradicionales, las solicitudes suelen tomar días o semanas para ser atendidas y completadas.

A pesar de las dificultades que representa crear una estructura de auto-servicio bajo demanda, para cualquier proveedor de servicios de nube es la mejor opción a implementar. Este tipo de servicio suele proveerse a través de un portal de usuario, donde se realizan todas las transacciones del servicio.

[14] www.nist.gov/itl/cloud-computing

- Amplio Acceso a través de Internet

Una peculiaridad de los servicios de nube es que los mismos deben poder ser accedidos a través de una forma rápida y sencilla. Los requerimientos de conexión a los servicios de nube solo deben necesitar una conexión básica a internet. A pesar de que en los últimos tiempos el internet ha incrementado de forma exponencial su capacidad, el acceso a estos no debe requerir al usuario una gran cantidad de ancho de banda para poder utilizar el servicio.

Debe considerarse que el uso del servicio no requiera de un cliente robusto, ya que descargar un cliente robusto puede considerarse un problema para el cliente. También debe tomarse en cuenta que, sí el cliente requiere comunicación constante con el servicio, los usuarios finales podrían experimentar latencia cuando se encuentren en conectividades de internet limitado.

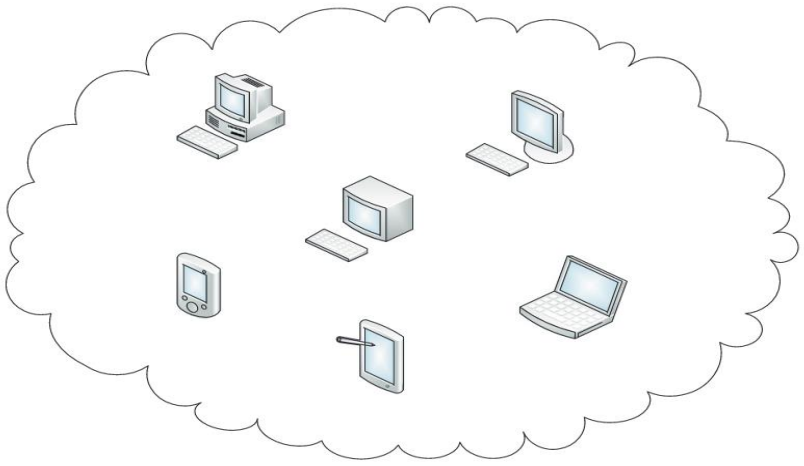


Figura 21. Acceso a través de múltiples dispositivos

Fuente: Interoute

El último punto clave de esta característica es que los servicios basados en la nube deben poder ser accedidos desde cualquier tipo de dispositivos clientes. Actualmente no solo deben incluirse las tradicionales computadoras convencionales y portátiles, ya que no son los únicos utilizados para acceder a internet. Los usuarios suelen utilizar otros dispositivos como tabletas, teléfonos inteligentes, relojes inteligentes, entre otros.

Debido a esta necesidad no se recomienda que estos servicios requieran de un cliente, ya que resulta difícil y costoso desarrollar y mantener un cliente específico para cada plataforma (Windows, Mac, IOS, Android, entre otros). Una opción es el acceso a través de un cliente web el cual es independiente al dispositivo en que sea accedido.

- Uso Compartido de Recursos

El uso compartido de recursos es lo que permite la reducción de costos y permite la flexibilidad de servicio al proveedor del mismo. Esta característica se basa en el hecho que los usuarios no siempre necesitan hacer un uso constante de todos los recursos; por lo cual los mismos en vez de estar ociosos pueden ser reutilizados por otros clientes.

Esto le brinda al proveedor la posibilidad de tener mayor cantidad de clientes que si brinda recursos dedicados a cada uno. Este modelo de negocio se logra gracias al concepto de virtualización, la cual permite incrementar la densidad de sus sistemas ya que pueden manejar múltiples sesiones virtuales en un solo sistema.

- Fácil Crecimiento

Un ambiente de servicio en la nube debe poseer la capacidad de fácil crecimiento de forma tal que pueda satisfacer las necesidades del usuario. Cada plataforma de nube debe contar con la infraestructura necesaria para poder expandir su capacidad sin afectar el servicio. Si el diseño es escalable solo necesitar añadir más recursos de computación y almacenamiento para expandir el servicio.

El punto clave para tener un crecimiento rápido es la automatización y orquestación de los recursos. Esto se logra a través de la configuración de parámetros de niveles de capacidad que desencadena la activación de procesos de expansión de capacidad. Además, se debe lograr que este proceso tenga un retorno, ya que un punto importante es que los recursos sean utilizados solo cuando sea necesario.

- Servicio Medido

Los servicios en la nube necesitan contar con la capacidad de medir el consumo realizado. El consumo puede ser medido utilizando diferentes métricas o variables, como tiempo, ancho de banda y espacio utilizado. Este servicio medido se caracteriza por permitir al usuario final pagar según su consumo.

Se debe proveer al usuario toda la información necesaria para comprender su facturación. Esto es muy relevante ya que, si no se comprende bien, el cliente puede sorprenderse con una alta facturación de su servicio.

3.1.1 Beneficios de Cloud Computer

Las principales propiedades que se derivan de la nube son:

- Flexibilidad; capacidad de aumentar la potencia en los recursos a gran escala hacia abajo o hacia arriba con rapidez y facilidad para satisfacer la demanda del servicio.
- Facturación por uso; servicio medido a través de internet sobre una base de pago por uso.
- Mejor distribución; implementación de herramientas que generan ahorro en costo e inversión.

3.1.2 Tipos de Cloud

Los tipos de nubes o cloud ofrecen distintos formatos de privacidad, donde el usuario final opta por la opción más conveniente de acuerdo a la información que maneja en los servidores, categorizados en los siguientes modelos:

3.1.2.1 Cloud Pública

El modelo más reconocible de la computación en nube para muchos consumidores es el modelo de nube pública, en las que los servicios de nube se proporcionan en un entorno virtualizado, fabricados con los recursos físicos compartidos agrupados y accesibles a través de una red pública como Internet. En cierta medida, se puede definir en contraste con las nubes privadas cuyo anillo-cerca de la piscina de los recursos informáticos subyacentes, creando una plataforma en la nube distinta a la que sólo una organización tiene acceso. Las nubes públicas, sin embargo, proporcionan servicios a varios clientes utilizando la misma infraestructura compartida.

Figura 22. Public Cloud.

Fuente: http://www.elcivismo.com.ar/notas/23959/

Los ejemplos más sobresalientes de la computación en nube tienden a caer en el modelo de nube pública, ya que son, por definición, a disposición del público. Software como Servicio (SaaS), tales como aplicaciones de oficina en línea almacenamiento en la nube y son, quizás, la infraestructura más familiar, pero ampliamente disponible como servicio (IaaS) y Plataforma como servicio (PaaS) las ofertas, incluyendo la Web basada en la nube de alojamiento y entornos de desarrollo, puede seguir el modelo también (a pesar de todo, también puede existir dentro de las nubes privadas).

Las nubes públicas se utilizan ampliamente en las ofertas para las personas físicas que son menos propensos a necesitar el nivel de infraestructura y seguridad ofrecida por las nubes privadas. Sin embargo, la empresa aún puede utilizar nubes públicas para realizar sus operaciones significativamente más eficientes, por ejemplo, con el almacenamiento de contenido que no sea sensible, la colaboración de documentos en línea y correo web. (Interoute, 2016).

El modelo público ofrece las siguientes características y beneficios:

- **Escalabilidad:** los recursos de la nube están disponibles en la demanda de vastas reservas de recursos, ya que las nubes públicas están para que las aplicaciones que se ejecutan en ellos pueden responder perfectamente a las fluctuaciones de la actividad.

- **Económico:** las nubes públicas permiten reunir a mayores niveles de recursos y así pueden beneficiarse de las mayores economías de escala. La operación centralizada y la gestión de los recursos subyacentes se comparte entre todos los subsiguientes servicios en la nube, mientras que los componentes, tales como servidores, requerir una configuración menor medida. Algunas proposiciones del mercado de masas, incluso puede ser libre para el cliente, basándose en la publicidad de sus ingresos.

- **Administración de Costos:** servicios de nube pública a menudo emplean un pay-as-you-go modelo según el cual el consumidor podrá acceder al recurso que necesitan, cuando lo necesitan, y luego sólo pagan por lo que utilizan carga; por lo tanto, evitando la capacidad desperdiciada.

- **Confiabilidad:** el gran número de servidores y redes que participan en la creación de una nube pública y las configuraciones de redundancia significa que debe un componente físico falla, el servicio en la nube todavía habría afectado ejecutar en los componentes restantes. En algunos casos, cuando las nubes dibujan los recursos de múltiples centros de datos, un centro de datos podría

estar en línea y servicios en la nube individuales sufriría ningún efecto perjudicial. No es, en otras palabras, ningún punto único de fallo que haría un servicio de nubes públicas vulnerables.

- **Flexibilidad:** existe una infinidad de IaaS, PaaS y SaaS servicios disponibles en el mercado que siguen el modelo de nube pública y que están listas para utilizarse como un servicio desde cualquier dispositivo habilitado para Internet. Estos servicios pueden satisfacer la mayoría de necesidades de computación y pueden ofrecer sus beneficios a clientes privados y empresariales por igual. Las empresas pueden incluso integrar sus servicios de nube pública con las nubes privadas, en las que necesitan para llevar a cabo las funciones confidenciales de la empresa, para crear nubes híbridas.

- **Independencia de la Ubicación;** la disponibilidad de servicios de nube pública a través de una conexión a Internet asegura que los servicios están disponibles allí donde el cliente se encuentra. Esto proporciona valiosas oportunidades a la empresa, tales como el acceso remoto a la infraestructura de TI (en caso de emergencias, etc.) o la colaboración de documentos en línea desde varias ubicaciones.

3.1.2.2 Cloud Privada

Una nube privada es un determinado modelo de computación en la nube que implica un entorno basado en la nube distinta y seguro en el que sólo el cliente especificado puede operar. Al igual que con otros modelos de nubes, nubes privadas proporciona una potencia de computación como un servicio dentro de un entorno virtualizado usando un conjunto subyacente de los recursos de computación física. Sin embargo, bajo el modelo de nube privada, la nube (el grupo de recursos) sólo se puede acceder por una sola organización que proporciona esa organización con mayor control y privacidad. (Interoute, 2016)

Los dispositivos técnicos utilizados para proporcionar los diferentes servicios que pueden ser clasificados como de los servicios de nube privada puede variar considerablemente y por lo que es difícil de definir lo que constituye una nube privada desde un punto de vista técnico. En lugar de ello estos servicios se clasifican generalmente por las características que ofrecen a sus clientes.

Los rasgos que caracterizan a las nubes privadas incluyen a la delimitación de una nube para el uso exclusivo de una organización y los niveles más altos de seguridad de la red. Puede ser definidas en contraste con una nube pública que tiene varios clientes que acceden a servicios virtualizados cual todos sacar sus recursos a partir del mismo grupo de servidores a través de redes públicas. Servicios de nube privados obtienen su recurso de un conjunto de distintos equipos físicos, pero éstos pueden ser organizados internamente o externamente y se puede acceder a través de líneas arrendadas privadas o seguras conexiones cifradas a través de redes públicas.

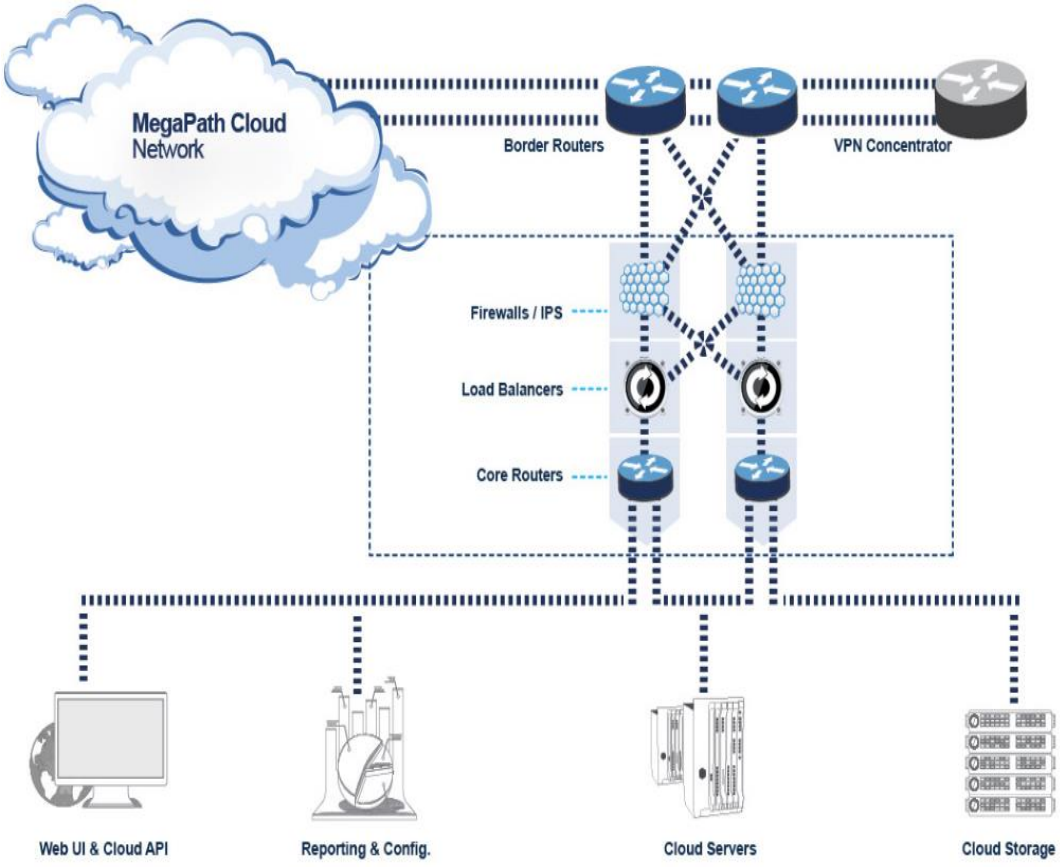


Figura 23. Private Cloud.

Fuente: http://www.gridgit.com/post_private-cloud-architecture-design-diagram_17341/

La seguridad adicional que ofrece el anillo de vallado, modelo de nube es ideal para cualquier organización, incluyendo la empresa, que necesita para almacenar y datos privados de proceso o realizar tareas delicadas. Por ejemplo, un servicio de nube privada podría ser utilizado por una empresa financiera que es requerida por la regulación para almacenar datos sensibles internamente y que todavía quieren beneficiarse de algunas de las ventajas de la computación en nube dentro de su infraestructura de negocios, tales como la asignación de recursos de la demanda.

El modelo de nube privada está más cerca del modelo más tradicional de las redes de acceso individuales locales (LANs) utilizados en el pasado por la empresa, pero con las ventajas añadidas de la virtualización. Las características y beneficios de las nubes privadas, por tanto, son los siguientes:

- **Mayor Seguridad y Privacidad**: servicios de nubes públicas pueden poner en práctica un cierto nivel de seguridad, pero las nubes privadas - usando técnicas tales como piscinas distintas de recursos de acceso restringido a las conexiones realizadas desde detrás del firewall de una organización, líneas arrendadas dedicado y / o en el lugar de hospedaje interno - puede asegurar que las operaciones se mantienen fuera del alcance de miradas indiscretas

- **Más Control:** como una nube privada sólo se puede acceder por una sola organización, esa organización se tiene la posibilidad de configurar y gestiona en línea sus necesidades para lograr una solución de red a medida. Sin embargo, este nivel le quita elimina el control de las economías de escala generadas en nubes públicas por tener una gestión centralizada del hardware.

- **El Costo y la Eficiencia Energética:** la implementación de un modelo de nube privada puede mejorar la asignación de recursos dentro de una organización, asegurando que la disponibilidad de recursos a los departamentos / funciones de negocios individuales puede responder directamente y de manera flexible a su demanda. Por lo tanto, aunque no son tan rentables como servicios de nube pública debido a las economías más pequeñas de escala y el aumento de los costes de gestión, que no hacen un uso más eficiente del recurso informático que

las LAN tradicionales ya que minimizan la inversión en la capacidad no utilizada. Esto no sólo proporciona un ahorro de costes, pero puede reducir la huella de carbono de una organización demasiado.

- **Mejora de la Fiabilidad:** incluso en los casos (servidores, redes, etc.) están alojados internamente los recursos, la creación de ambientes operativos virtualizados significa que la red es más resistente a los fallos individuales a través de la infraestructura física. Particiones virtuales pueden, por ejemplo, tirar de sus recursos de los servidores no afectados restantes. Además, cuando la nube se encuentra alojado con un tercero, la organización todavía puede beneficiarse de la seguridad física que ofrezca a la infraestructura alojada dentro de los centros de datos.

- **Expansión Dinámica:** algunos proveedores pueden ofrecer la oportunidad de emplear la nube de ruptura, dentro de una oferta de nube privada, en el caso de picos de demanda. Este servicio permite al proveedor para cambiar ciertas funciones que no son sensibles a una nube pública para liberar más espacio en la nube privada para las funciones sensibles que lo requieran. Las nubes privadas, incluso pueden ser integrados con los servicios de nube pública para formar nubes híbridas en las funciones que no son sensibles siempre se asignan a la nube pública para maximizar las eficiencias que se ofrecen.

3.1.2.3 Cloud Híbrida

Una nube híbrida es un servicio en la nube integrado que utiliza nubes privadas y públicas para realizar funciones distintas dentro de la misma organización. Todos los servicios de cloud computing deben ofrecer ciertas eficiencias en diferentes grados, pero los servicios de nube pública es probable que sean más rentables y escalables que las nubes privadas. Por lo tanto, una organización puede maximizar su eficiencia mediante el empleo de los servicios de nube pública para todas las operaciones no sensibles, que

confía solamente en una nube privada donde lo requieran y asegurar que todas sus plataformas están perfectamente integradas.

Los modelos de nube híbridos pueden implementarse de varias maneras:

- Separada del equipo proveedores de la nube hasta proporcionar servicios tanto privados como públicos como un servicio integrado.
- Los proveedores de nubes individuales ofrecen un paquete completo híbrido.
- Las organizaciones que gestionan sus nubes privadas mismos se inscriban a un servicio en la nube pública que luego se integran en su infraestructura.

En la práctica, una empresa puede implementar nube híbrida hosting para alojar su sitio web de comercio electrónico dentro de una nube privada, donde es segura y escalable, pero su sitio sencillo en una nube pública, donde es más rentable (y la seguridad es menor de una preocupación). Como alternativa, una Infraestructura como Servicio (IaaS) ofreciendo, por ejemplo, podría seguir el modelo de nube híbrida y proporcionar una empresa financiera con el almacenamiento de datos de los clientes dentro de una nube privada, pero luego permitir la colaboración en los documentos de planificación de proyectos en la nube pública - donde que pueden ser accedidos por múltiples usuarios desde cualquier lugar conveniente.

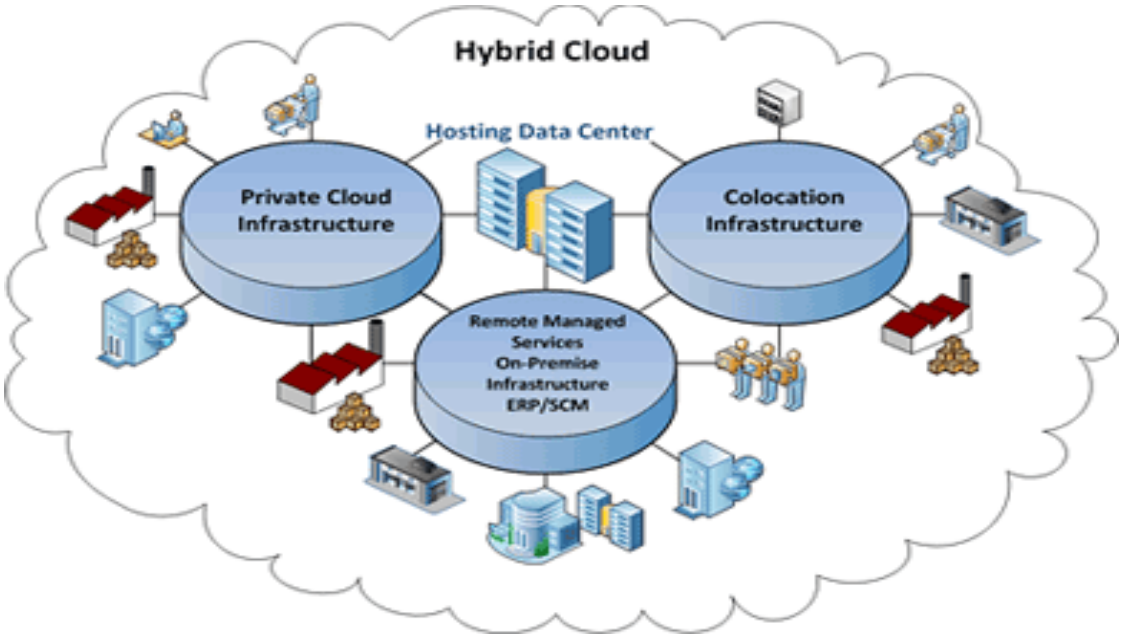


Figura 24. Hybrid Cloud.

Fuente: http://www.vmtech.net/hybrid-infrastructure.php

Una configuración de nube híbrida, tales como hospedaje híbrido, puede ofrecer a sus usuarios las siguientes características:

- **Seguridad:** el elemento de nube privada del modelo de nube híbrida no sólo proporciona la seguridad donde sea necesario para las operaciones sensibles, pero también puede satisfacer los requisitos reglamentarios para la manipulación y el almacenamiento de datos en los que es aplicable.

- **Escalabilidad:** mientras que las nubes privadas ofrecen un cierto nivel de escalabilidad en función de sus configuraciones (si están organizadas internamente o externamente, por ejemplo), los servicios de nubes públicas ofrecen escalabilidad con menos límites, porque los recursos se salen de la infraestructura de la nube más grande. Al mover la mayor cantidad de funciones que no son tan sensibles como sea posible a la nube pública que permite a una organización para beneficiarse de la escalabilidad de nube pública, mientras que la reducción de la demanda en una nube privada.

- **Las Eficiencias de Costes**: de nuevo las nubes públicas son propensos a ofrecer economías de escala más importantes (tales como la gestión centralizada), y así una mayor eficiencia de costes, que las nubes privadas. Por lo tanto, las nubes híbridas permiten a las empresas acceder a estos ahorros para el mayor número de funciones de negocio como sea posible mientras que todavía mantiene operaciones sensibles seguras.

- **Flexibilidad;** la disponibilidad de recursos tanto seguro y económico escalable recurso público eficaz puede proporcionar a las organizaciones con más oportunidades para explorar diferentes vías operacionales.

3.2 Arquitectura Orientada al Servicio (SOA)[15]

La Arquitectura orientada al servicio (SOA) es una arquitectura de acoplamiento flexible diseñada para satisfacer las necesidades de las instituciones. Anteriormente, las arquitecturas estaban basadas en tecnologías como COBRA y DCOM o enfoques basados en intercambio electrónico de datos para la integración de B2B,

La orientación a servicios (SOA) no requiere el uso de servicios web, es una manera de pensar en términos de servicios y el desarrollo basado en el servicio y los resultados de los servicios.

Un servicio:

Es una representación lógica de una actividad de negocio repetible que tiene un resultado específico (por ejemplo, verificación de crédito del cliente, proporcionar datos meteorológicos, la consolidación de los informes de perforación).

SOA se caracteriza por:

- Está auto-contenida.
- Puede estar compuesto por otros servicios.
- Su funcionamiento es oculto para los consumidores del servicio.

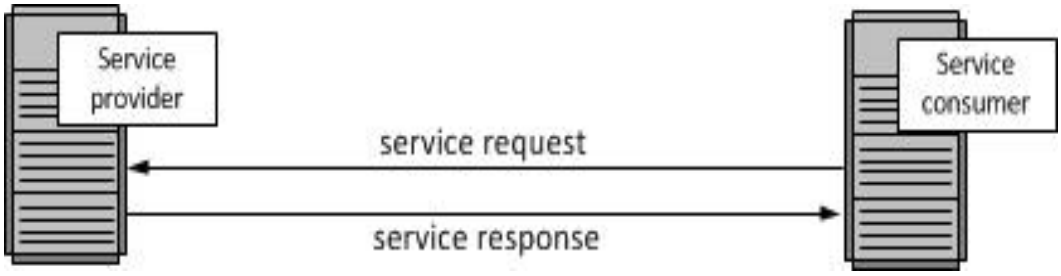


Figura 25. Arquitectura orientada al servicio (SOA).

Fuente: http://www.service-architecture.com/articles/web-services/service-oriented_architecture_soa_definition.html

[15] http://www.opengroup.org/soa/source-book/soa/soa.htm

3.3 Niveles de Servicios

3.3.1 Infraestructura como Servicio (IaaS)

La infraestructura como servicio es un nuevo modelo computacional que persigue, dejar fuera los recursos físicos que permita dejar a un lado el mantenimiento y gestión de los equipos, aprovechando los recursos disponibles y escalabilidad

Beneficios

- No es necesario invertir en el hardware.
- Infraestructura que soporta trabajos dinámicos.
- Innovador, flexible.

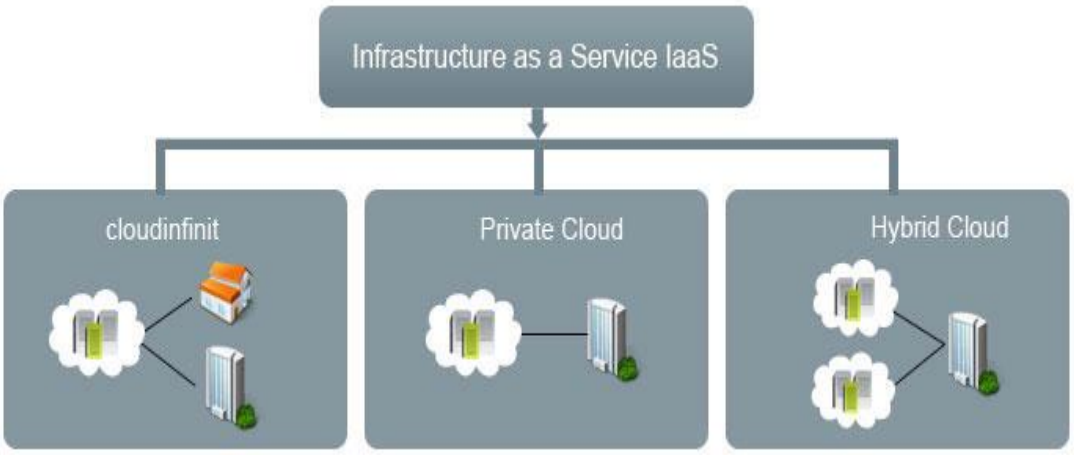


Figura 26. Infraestructura como servicio (IAAS)

Fuente: http://www.cloudinfinit.com/products/IaaS

3.3.2 Plataforma como Servicio (PaaS)

Plataforma como servicio (PaaS) trae los beneficios que posee SaaS para aplicaciones, pero enfocado al mundo de desarrollo de software. PaaS se puede definir como una plataforma de computación que permite la creación de aplicaciones web de forma rápida, sencilla y sin la complejidad de comprar y mantener el software y la infraestructura por debajo de ella.[16]

Beneficios

- Desarrollo de aplicaciones en menor tiempo para llevar al mercado.
- Implementación en minutos de nuevas aplicaciones web.
- Reducción de la complejidad con middleware como servicio.

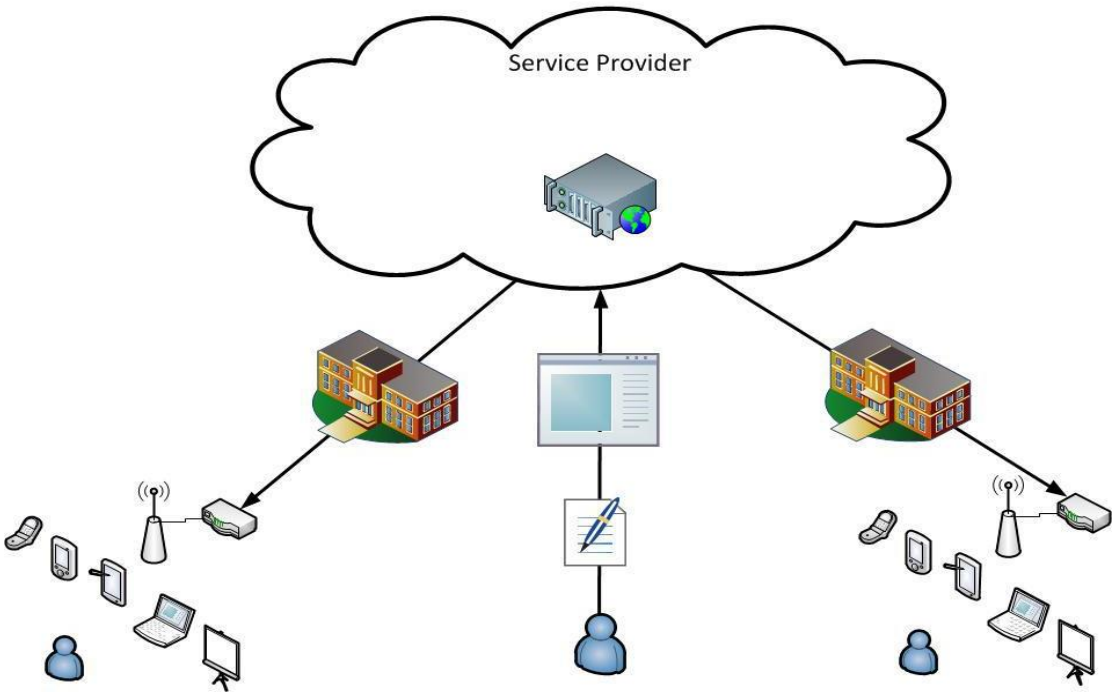


Figura 27. Plataforma como servicio (PaaS).

Fuente: https://marce44195.wordpress.com/24-2/32-2/

[16] https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/

3.3.3 Software como Servicio (SaaS)

El software como servicio, consiste en una aplicación online con las funcionalidades necesarias, básicamente se describe como el servicio que brinda a los usuarios la posibilidad de alquilar o pedir prestado software en línea en lugar de realmente comprar e instalar en sus propios ordenadores. Es la misma situación que las personas que utilizan los servicios de correo de Gmail o Yahoo, excepto que SaaS va mucho más allá. SaaS es la idea fundamental detrás de la computación centralizada: negocios enteros y miles de empleados se ejecutarán sus herramientas informáticas como productos en línea alquilados. Todo el trabajo de procesamiento y almacenamiento de archivos se realizará a través de Internet, con usuarios que accedan a las herramientas y los archivos usando un navegador web.[17]

Beneficios

- Accesibles desde cualquier equipo electrónico.
- No se pierden los datos.
- El servidor es capaz de escalar dinámicamente a las necesidades de uso.

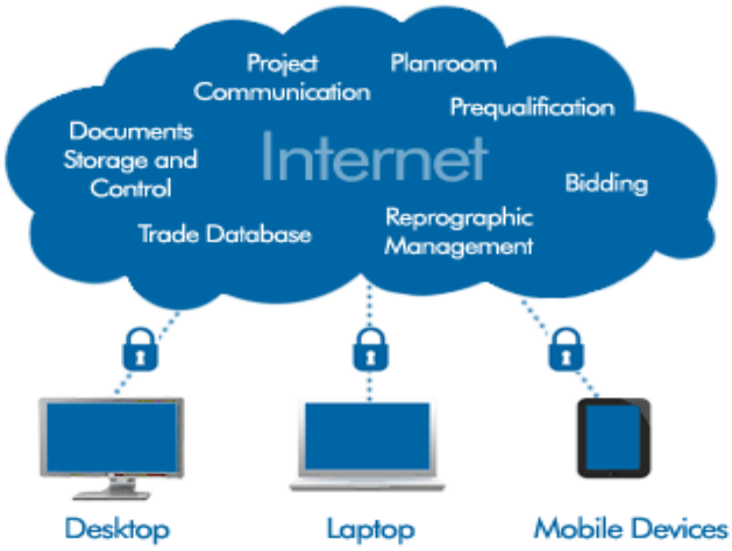


Figura 28. Software as a Service (SaaS).

Fuente: http://www.insuranceportal.tk/2015/12/software-as-servicesaas.html

[17] http://netforbeginners.about.com/od/s/f/what_is_SaaS_software_as_a_service.htm

3.4 Virtualización

La virtualización es un concepto que ha evolucionado a través de los años, dejando de ser una tecnología para uso de un público exclusivo a ser el soporte de las redes que soportan el internet que conocemos hoy en día.

La virtualización puede definirse: como un proceso en el que un equipo host, equipo físico contiene las máquinas virtuales que se almacenan en ellos en forma de archivos. Estas máquinas virtuales actúan exactamente de la forma en que los equipos físicos hacen y pueden ser mapeados con las tarjetas de red de los ordenadores host. Una vez asignados, los sistemas operativos instalados dentro de las máquinas virtuales (sistemas operativos invitados), entonces se pueden comunicar con los ordenadores principales, así como las configuraciones de red a los que los equipos host podrían estar conectados[18].

En la industria de TI, el término virtualización se utiliza con frecuencia en la actualidad. La razón detrás de esto es que, con la ayuda de las soluciones de virtualización, las organizaciones pueden reducir sus gastos notablemente, a vez de proporcionar una mejor experiencia de usuario a los usuarios finales, al mismo tiempo. Cuando la tecnología de virtualización se implementa en cualquier organización, toda la configuración y el funcionamiento de la tecnología sean totalmente transparente para los usuarios. Esto significa que, si los administradores han creado máquinas virtuales dentro de los equipos host y los han relacionado con los entornos de red físicos, los usuarios que accedan a sus datos que pueden residir dentro de las máquinas virtuales nunca se sabe si accedieran a sus datos desde las máquinas virtuales o desde el equipo host.[19]

[18] http://www.techiwarehouse.com/engine/b00fab42/Understanding-Virtualization-Concepts

[19] http://www.techiwarehouse.com/engine/b00fab42/Understanding-Virtualization-Concepts

3.4.1 Tipos de Virtualización[20]

El término virtualización, es ampliamente aplicada a una serie de conceptos que incluye:

- La Virtualización del Servidor

La virtualización de servidores es el segmento más activo de la industria de la virtualización con empresas establecidas, tales como VMware, Microsoft y Citrix. Con la virtualización del servidor una máquina física se divide muchos servidores virtuales. En el núcleo de cada una se encuentra el concepto de un hipervisor el cual es una delgada capa de software que intercepta las llamadas al sistema operativo al hardware. Los hipervisores suelen proporcionar una CPU virtualizada y la memoria de los invitados (equipos virtualizados) que se ejecutan en la parte superior de ellos. El término fue utilizado por primera vez en conjunción con el IBM PC-370.

- Virtualización de Cliente / Escritorio / Aplicación

La virtualización no sólo es una tecnología utilizada a nivel de servidores. En la actualidad se han agregado una serie de usos en el lado del cliente, tanto en el escritorio como a nivel de aplicación. Tal virtualización puede dividirse en cuatro categorías:

- ❖ La Virtualización de Aplicación Local.
- ❖ La Virtualización de Aplicaciones Alojadas.
- ❖ Alojado Virtualización de Escritorio.
- ❖ La Virtualización de Escritorio Local.
- ❖ La Virtualización de Red.

Es la mezcla de los recursos de red físicos del hardware en conjunto con los recursos de red del software en un solo elemento. La meta de la virtualización de redes es simplificar el uso de recursos compartido haciéndolo más eficaz, teniendo control y seguridad para los sistemas.

[20] https://www.infoq.com/articles/virtualization-intro

El producto final de la virtualización de redes es una red virtual. Las redes virtuales se pueden clasificar en dos grupos: externas e internas. Las redes virtuales externas son las que poseen diferentes redes locales administradas por software como una sola. Las mismas están compuestas por el hardware de conmutación y la tecnología de software VLAN. Entre los ejemplos de redes virtuales externas, se incluyen las grandes redes de corporaciones y datacenters.[21] Las redes virtuales internas y externas brindan flexibilidad a través de la segmentación de los recursos de red lo que produce una mayor eficiencia del centro de datos.

- La Virtualización de Almacenamiento

Esta se refiere al proceso de abstraer almacenamiento lógico de almacenamiento físico. Mientras el RAID en el nivel básico proporciona esta funcionalidad, la virtualización de almacenamiento a largo plazo suele incluir conceptos adicionales, tales como la migración de datos y almacenamiento en caché. La virtualización del almacenamiento es difícil de definir de manera fija debido a la variedad de formas en que la funcionalidad puede ser proporcionada.

- Servicio / Aplicación Infraestructura de Virtualización

Los proveedores de aplicaciones empresariales, también han tomado nota de los beneficios de la virtualización un empezado a ofrecer soluciones que permiten la virtualización de aplicaciones de uso común, tales como Apache, así como plataformas que permiten que el software o aplicación se desarrolle fácilmente con capacidades de virtualización que van desde el nivel más bajo hasta el más alto.

[21] https://docs.oracle.com/cd/E26921_01/html/E25833/gfkbw.html

Conclusión

El Cloud Computing o Computación en la Nube ha tenido el potencial de ser la fuerza que ha cambiado la formar de desarrollar y utilizar las diferentes tecnologías computacionales en nuestros días. Esto se debe a que la nube ha sido la evolución ya que se considera una de las tecnologías más sobrevalorado en décadas.

Por lo cual puede ser de mucho beneficio cuando se usa como parte del plan de recuperación de desastres de una organización (DR). Ahora es posible para una empresa crear un sitio de recuperación basado en la nube que se podría utilizar ante cualquier eventualidad que provoque que el centro de datos principal este fuera de servicio.

Capítulo IV

Plan de Recuperación de Desastres (DRP)

Introducción

Contar con un plan de recuperación de desastre resulta vital para las organizaciones, ya que por medio de este se puede anticipar los riesgos a los que se encuentra expuesto el sistema, garantizando la protección de los datos y equipos ante una eventualidad.

A través del Plan de Recuperación de Desastre, se puede conocer el rol que desempeña cada equipo en el sistema y los procedimientos que resultan necesarios.

Dentro del capítulo, se encuentra la estructura que debe tener un Plan de Recuperación de Desastre. Además, de los procesos necesarios para recuperar y proteger la infraestructura tecnológica de una empresa en caso de desastre puntualizando los riegos, vulnerabilidades y amenazas a las que se encuentran expuesto los datos, fases y porque resulta indispensable que las empresas cuenten con un DRP.

4.1 Conceptos de un DRP

En esta época, las instituciones cuentan con una creciente dependencia tecnología para ofrecer sus servicios, y por lo tanto, es preciso desarrollar estrategias que permitan asegurar la información crítica, implica un análisis detallado de los procesos de la organización, así como su función, dicho de otra manera implementar un plan de recuperación de desastre.

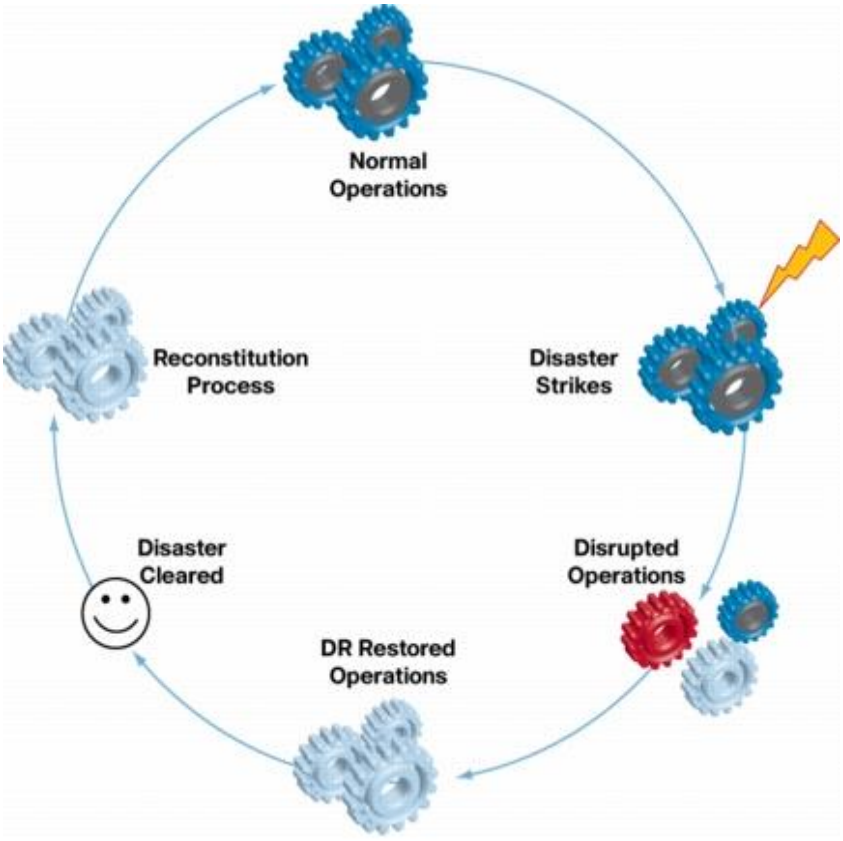


Figura 29. Ciclo de operaciones de la empresa de recuperación de desastres

Fuente: https://www.cisco.com

Un Plan de Recuperación de Desastre (DRP), es un plan centrado en el sistema para restaurar la operatividad del sistema, aplicaciones e infraestructura después de una eventualidad. Para las instituciones, un desastre significa la interrupción de la totalidad o parcialidad de las operaciones, ocasionando pérdidas.

No se puede impedir desastres naturales o provocados por el hombre, sin embargo se puede controlar el impacto. En la planificación de un plan de recuperación de desastre (DRP), se acopla el grado de complejidad del sistema, asimismo tratar de disminuir o eliminar los efectos de un desastre.

El Plan de Recuperación de Desastre forma parte de un plan sistémico llamado Plan de Continuidad de Negocio (BCP) [22]compuesto por:

- **Plan de Reanudación de Negocios (BCP),** Se centra en el mantenimiento de los procesos de la institución durante y después de una ruptura. Es usado para recuperación a largo plazo en combinación de COOP, permitiendo funciones adicionales.

- **Plan de Emergencia del Personal (OEP),** Describe los procesos de respuesta inmediata en caso de amenaza o incidente para la salud y seguridad del medio ambiente, el personal o la propiedad.

- **Plan de Continuidad de Operaciones (COOP),** Se centra en la restauración de las funciones esenciales de una organización.

- **Plan de Manejo de Incidentes (IMP),** Descripción de estrategias para prevenir incidentes, detalla como el incidente será tratado para preservar el funcionamiento y proporcionar la información.

- **Plan de Protección de Infraestructura Física (PIC),** Conjunto de políticas y procedimientos que sirven para proteger y recuperar los activos, mitigar los riesgos y vulnerabilidades.

- **Plan de Recuperación ante Desastres (DRP),** Diseñado para restaurar en funcionamiento del sistema, aplicaciones o instalación en un sitio alterno después de una emergencia.

[22] http://www.redbooks.ibm.com/redbooks/pdfs/sg246844.pdf

4.1.1 Objetivo

El objetivo principal de un Plan de Recuperación de Desastre es reducir al mínimo el tiempo de inactividad de los servicios tanto tecnológico como la perdida de datos, con el fin de obtener continuidad en el negocio. Para así satisfacer los objetivos secundarios:

- Localizar las vulnerabilidades del servicio y definir las medidas preventivas para reducir el impacto de las interrupciones.
- Analizar e identificar costos en las posibles fallas del sistema.
- Identificar las necesidades por prioridad de recuperación.
- Examinar las alternativas y métodos más eficaces.

Para cumplir los objetivos del plan de recuperación de desastre es importante conocer:

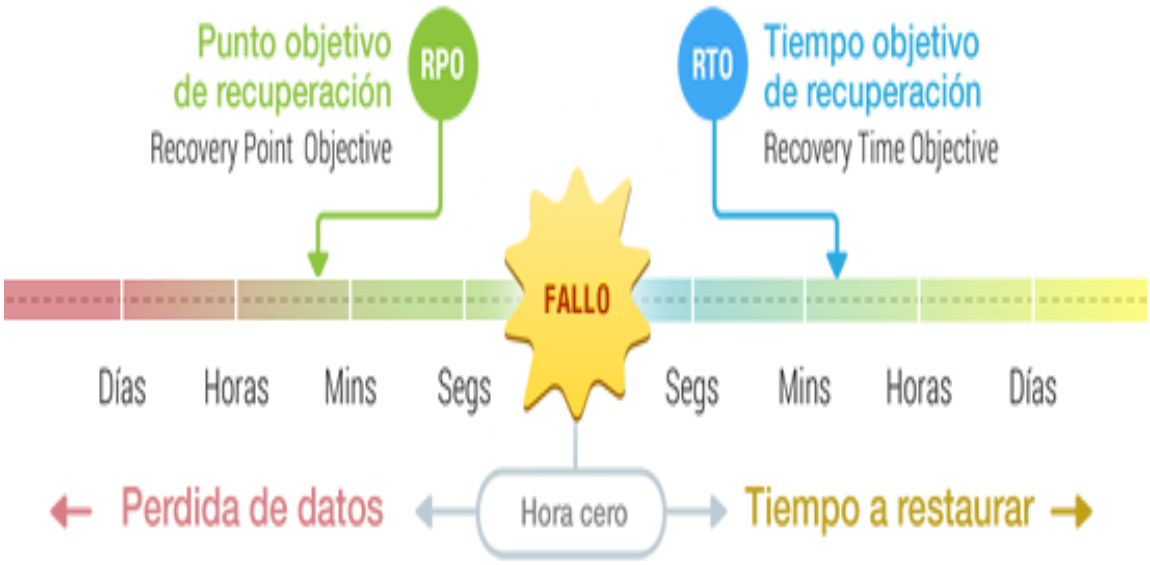


Figura 30. Recovery Point & Recovery Time.

Fuente: http://www.redsis.com/index.php/soluciones/continuidad-del-negocio/respaldo-y-recuperacion

- Objetivo del Tiempo de Recuperación (RTO, Recovery Time Objective),[23] se define como el intervalo de tiempo transcurrido entre la ocurrencia de un evento y la restauración de los servicios. RTO debe ser medido desde el momento que ocurrió la interrupción hasta reanudar el servicio, una vez se haya definido los objetivos de recuperación. Este se especifica en horas y minutos.

Con el fin de reducir el tiempo fuera de servicio se evalúa las situaciones en las diferentes áreas, tales como:

- Recuperación de la red; en este tiempo se restaura la voz o comunicación de datos.
- Recuperación de los datos; se recupera los datos de copia de seguridad, incluyendo el tiempo de carga o reinicio de aplicaciones.
- Recuperación de aplicaciones; corregir algún error en las aplicaciones después de la interrupción.
- Recuperación de la plataforma, restaurar los servicios de plataforma.
- Recuperación del servicio; representa el tiempo acumulado para restaurar el servicio tanto física como lógica, cumpliendo con las recuperaciones anteriores.

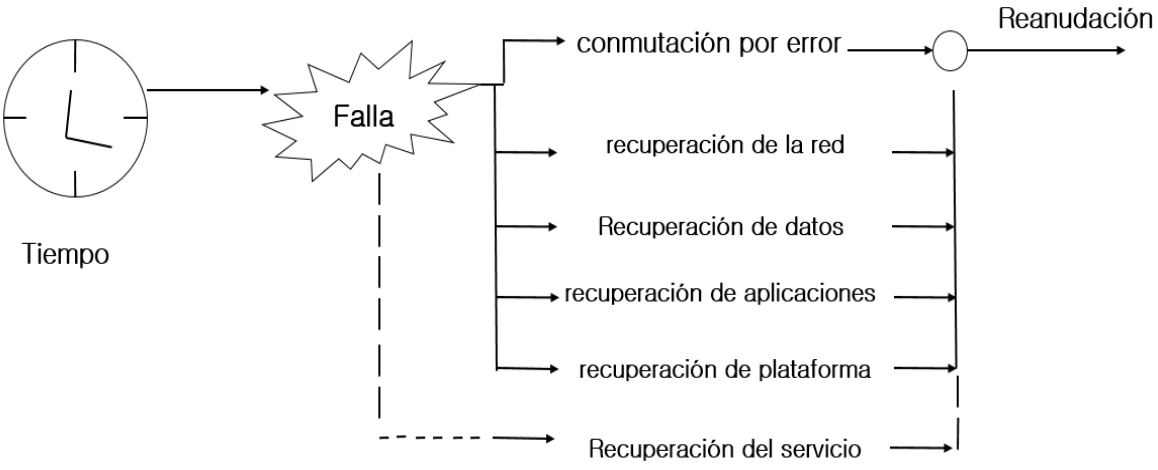


Figura 31. Actividades de recuperación

Fuente: Los autores, auxiliado de Mission Critical Network Planning, pág. 34

[23] Tomado del libro: Mission-Critical Network Planning, page 34.

- Objetivo de Punto de Recuperación (RPO, recovery point objetive[24]), se utiliza como indicador para la recuperación de datos, denominado ventana de frescura. En términos de tiempo, es el período máximo tolerable que puede pasar durante una interrupción entre la última copia de seguridad y el punto de recuperación para restablecer el funcionamiento.

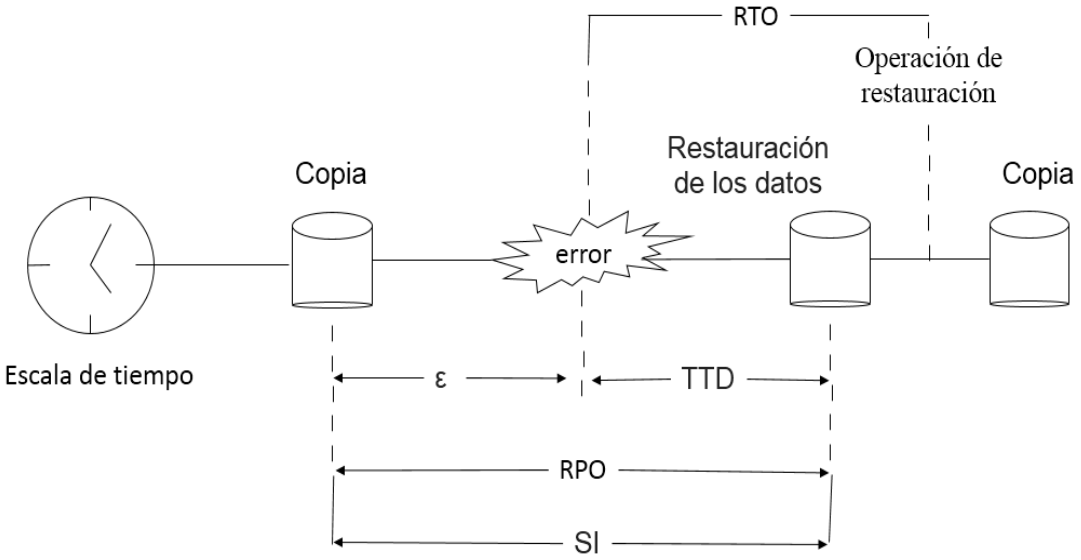


Figura 32. TTD y RPO usando una línea de tiempo.

Fuente: https://imcs.dvfu.ru/lib.int/docs/Networks/Administration/Mission-Critical%20Network%20Planning.pdf.

Las compañías que no toleran perdida de datos, la información tendría que ser restaurada instantáneamente después de un evento, implementando un sistema de copia de seguridad continua.

[24] Tomado del libro: Mission-Critical Network Planning, page 35

4.1.2 Efectos

Los diferentes eventos que puedan ocasionar daños al personal, edificio, equipos y sistemas, pueden tener los siguientes efectos en las organizaciones:

Efectos Inmediatos

- Daño directo, daño directo a los equipos, infraestructura y sistema, rindiendo procesos inhabitables y sistemas inutilizables.
- Inaccesibilidad, dependiendo el acontecimiento resulta peligro entrar, incluso para recuperar artículos o equipos.
- Servicios públicos, a causa de los incidentes los servicios eléctricos, agua y gas son interrumpidos en las zonas afectadas.

Efectos Secundarios

- Interrupción de transporte, incidentes generalizados afectan el tránsito, incluyendo autopista, carreteras principales, entre otros, por un tiempo determinado.
- Aeropuerto, las perturbaciones en los sistemas, mal tiempo, problemas de control de tráfico aéreo o mecánicos, en coacciones, logra retrasar o cancelar en casos muy necesarios por la seguridad de los terceros.
- Interrupción de las comunicaciones, las organizaciones dependen voz y comunicación en sus servicios, los cuales son interrumpidos ya sea por daños directo a la infraestructura o en el cableado.
- Evacuaciones, de acuerdo a la magnitud del desastre resulta imprescindible poner a salgo el personal, como resultado evacuaciones obligatorias de áreas o zonas.

Estos efectos logran detener las operaciones en un lapso de corta duración (horas o días) que la institución puede satisfacer la demanda de servicio al reanudar los procesos. Si los efectos de un desastre resultan más severos, en algunos casos las instituciones no logran superar la problemática y se ven en la necesidad de cesar los servicios.

4.1.3 Niveles de un DRP[25]

En 1992, IBM define un conjunto de niveles para abordar adecuadamente la necesidad de cuantificar la implementación de un DRP, proporcionando una visión general en los siete niveles, los cuales son:

TIER 0 “No hay Datos fuera del Sitio”

En este nivel no existe información, documentación o copia de seguridad almacenada. Por lo tanto, no es posible la implementación de un plan de recuperación. Un centro de datos que se encuentre en este nivel se expone a una catástrofe de la que no se podrá recuperar.

TIER 1 “Traslado Físico”

Proporciona el nivel más básico de recuperación de desastre, almacenando los datos en instalaciones fuera de la infraestructura, permitiendo recuperar y proporcionar el servicio. El nivel 1 presenta el inconveniente de no lograr restaurar el último backups.

TIER 2 “Traslado Físico a un Hotsite”

El nivel 2 se basa en un servicio de mensajería para obtener datos fuera de las instalaciones, que abarca los requerimientos del nivel uno, incluyendo la planificación de recuperación. El Hotsite tiene suficiente hardware y una infraestructura de red capaz de soportar los requerimientos críticos. En caso de desastre, se reduce el tiempo de recuperación.

[25] I.J. Modern Education and Computer Science, 2014 page. 59-60. Fuente: http://www.mecs-press.org

TIER 3 “Seguridad Electrónica”

El nivel 3 consiste en la transmisión electrónica y creación de copia de seguridad, abarca los componentes del nivel dos, permitiendo rápida recuperación, además no necesita el traslado de respaldo manualmente.

TIER 4 “Sitio Secundario Activo”

En el nivel 4 reduce el tiempo de recuperación, esto se logró a través de un procesador bidireccional, almacenando la copia de seguridad fuera de la instalación, compartiendo la carga entre la copia de seguridad y la original.

TIER 5 “Dos Sitios, Dos Fases”

El nivel de recuperación 5, abarca todos los requerimientos del nivel cuatro, además mantener actualizada la imagen local y la copia remota de la basa de datos. Requiere la sincronización de las plataformas primarias y secundarias utilizando una conexión de gran ancho de banda.

En el nivel 5 se requiere hardware parcial o total para transferir automáticamente los datos a la plataforma secundaria, logrando obtener los datos en dos localidades, en caso de desastre solo se perdería la transferencia en el momento del desastre, reduciendo el tiempo de recuperación, con una cantidad mínima de recuperar.

TIER 6 “Cero Perdida de Datos”

El nivel 6 es el último nivel de recuperación local y de copias de seguridad que utiliza almacenamiento en línea dual con una completa capacidad de conmutación de red. Ambos sistemas son avanzados, lo que proporciona transferencia automática a la plataforma secundaria o viceversa cuando sea necesario.

El nivel 6 es la solución más costosa, además de requerir de acoplamiento o aplicaciones de clúster y hardware para soportar la replicación de datos a distancia, obteniendo recuperación más rápida.

4.2 Fases de un DRP [26]

Las fases de recuperación de desastres son:

- **Fase de Activación**

  En esta fase los efectos se evalúan. Las interrupciones que afectan una determinada área, detención rápida y precisa de un evento de desastre y tener un plan de comunicación de acuerdo a los efectos de las emergencias entrante, en algunos casos se tiene el tiempo suficiente para reducir los efectos, oprimiendo el impacto. Esta fase consiste en la activación de:

  - Procedimientos de notificación, define las medidas tanto como una interrupción o una emergencia, restaurando las funciones del sistema de forma temporal.
  - Evaluación de daños, este punto es crucial para evaluar el grado de los daños del sistema. Puntualiza como se ejecutara el plan después de la interrupción, los procedimientos varían de acuerdo las emergencias, se puede considerar:
    - Origen de la interrupción.
    - Posibilidad de daños.
    - Áreas afectadas.
    - Estado de la infraestructura.
    - Estimación de recuperación de los servicios.
    - Planificación de la activación.

[26] Cisco Fuente: https://www.cisco.com

Al momento de ser detectada una falla, no es conveniente realizar interrupción en las operaciones, hasta que no se tenga certeza de daños. Resulta conveniente evaluar las áreas afectadas, por si es conveniente activar el plan de emergencia, tomando en consideración:

- Lista de servicios averiados.
- Dependencia del servicio.
- Proceso de restauración.
- Estimación de tiempo por proceso.
- Estrategias luego de restablecer el servicio.

- **Fase de Ejecución**

La operación de recuperación inicia luego de evalúan los procedimientos reales para recuperar cada entidad afectada. Las actividades de esta fase están centrada en llevar las funciones a estrategias, incluyendo el procesamiento manual, la recuperación y funcionamiento del sistema alterno.

La fase de ejecución se divide en:

- Secuencia de actividades, define las prioridades en el proceso de recuperación, cuando se producen situaciones como:
  - Acción no restablecida durante el tiempo determinado.
  - No se ha completado un proceso importante.
  - Falta de equipos para recuperar el servicio.

- Procedimiento de recuperación, el DRP debe proveer los detalles de los procedimientos al recuperar un servicio , abordando acciones como:
  - Obtener autorización de acceso a los datos.
  - Notificar a los usuarios asociados al sistema.
  - Cargar la copia de seguridad.
  - Restaurar el sistema, aplicaciones y software.
  - Restaurar la funcionalidad del sistema.

- **Fase de Reconstrucción**

En esta fase el sistema se restaura los procedimientos detenidos, retornando las operaciones a la instalación original una vez solucionadas las fallas. En caso que el sistema no pueda ser recuperado, implica la reconstrucción, por lo tanto podría durar unas semanas o incluso meses, considerando el riesgo.

Luego de restaurar el servicio y realizar las pruebas de lugar, se evalúan las siguientes actividades:

- Monitoreo continuo.
- Verificar que todos los servicios de la infraestructura están disponibles.
- Establecer la conectividad tanto interna como externa.
- Asegurar las áreas para el retorno del personal.

4.2.1 Análisis de Riesgos

Un análisis de riesgo identifica las funciones y activos importantes de la institución. Para cada proceso de la institución, es necesario determinar cada proceso crítico a los que se encuentra expuesto, evaluando:

- Escenarios naturales, desastres que posiblemente puedan ocurrir (naturales y provocados).
- Probabilidad de ocurrencia, implementando escala de altura media-baja.
- Vulnerabilidades, identificar las vulnerabilidades dentro de la institución.
- Mitigar los pasos, para cada vulnerabilidad encontrada, plantear como se puede reducir.

4.2.2 Análisis de las Amenazas

Una amenaza a diferencia de una vulnerabilidad, es un posible peligro que podría aprovechar una vulnerabilidad de violar la seguridad e integridad y por lo tanto causar posibles daños. Además, Prandini & Parello, plantea que una amenaza "requiere pensar en los posibles problemas que nos pueden afectar en un futuro cercano, por lo que plantea un posicionamiento anterior a un hecho, que representa algún grado de probabilidad de materializarse" (Magazcitum, 2013). A manera de ejemplos de amenazas reales pueden citarse los virus, los delincuentes informáticos o las intrusiones.

Otra definición, es aquella que la caracteriza como cualquier acción o acontecimiento no deseado e inesperado con la capacidad de ocasionar consecuencias adversas. En este caso, se refiere como origen de un incidente no deseado, que podría causar daños a un sistema u organización, según la define el estándar ISO/IEC-27002, si cualquiera de ellos presentara alguna debilidad o falla.[27]

4.2.3 Análisis de las Vulnerabilidades

El análisis de vulnerabilidad, también conocida como evaluación de la vulnerabilidad, es un proceso que define, identifica y clasifica los agujeros de seguridad (vulnerabilidades) tanto en una red, como en la infraestructura o equipo de comunicaciones. Además, el análisis de la vulnerabilidad puede predecir la eficacia de las medidas propuestas y evaluar su eficacia real después de su puesta en uso**.**[28]

El análisis de vulnerabilidad consiste en varios pasos:

- La definición y clasificación de la red o del sistema de recursos.
- La asignación de los niveles relativos de importancia para los recursos.
- La identificación de las amenazas potenciales a cada recurso.
- El desarrollo de una estrategia para hacer frente a los problemas más graves potenciales primera.

[27] http://www.magazcitum.com.mx/?p=2193#.WAlnnuArK00
[28] http://searchmidmarketsecurity.techtarget.com/definition/vulnerability-analysis

- Definir y aplicar medidas para reducir al mínimo las consecuencias en caso de ataque.

Podemos clasificar las amenazas en los siguientes renglones:

- Desastres Naturales
  - ❖ Sismos.
  - ❖ Huracanes.
  - ❖ Inundaciones.
  - ❖ Incendios.
  - ❖ Agua.
  - ❖ Tormentas eléctricas.

- Desastres Humanos
  - ❖ Disputas Laborales.
  - ❖ Robo.
  - ❖ Acceso no Autorizado.
  - ❖ Sabotaje.
  - ❖ Servicios.

- Desastres del Entorno
  - ❖ Falla de Energía Eléctrica.
  - ❖ Falta de Combustible.
  - ❖ Carencia de Suministro de Agua.
  - ❖ Fallo de la Telecomunicación.
  - ❖ Equipos o Sistema.
  - ❖ Fallo de Aire Acondicionado.
  - ❖ Falla de Fuente Alterna de Energía.
  - ❖ Falla Equipos Informáticos.

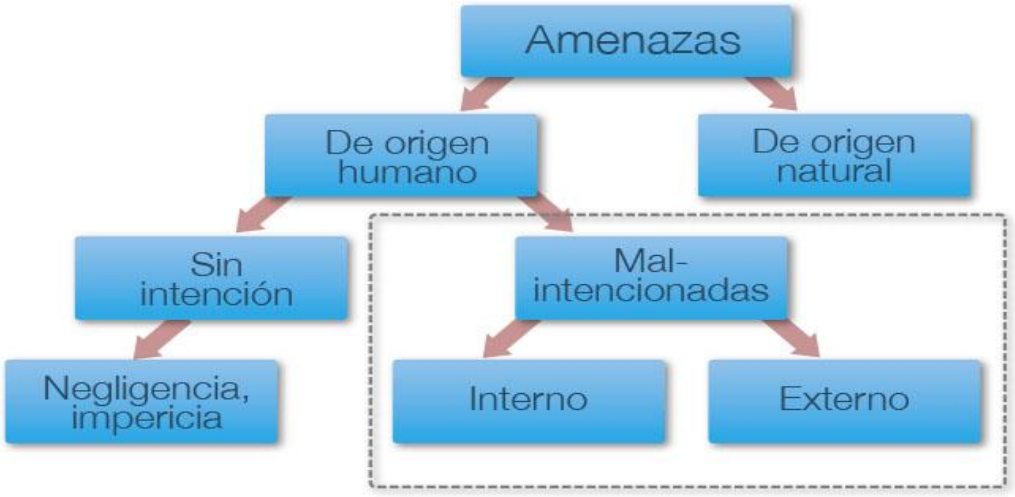


Figura 33. Desglose de causas de vulnerabilidades en el sistema

Fuente: http://www.magazcitum.com.mx/?p=2193#.WAlnnuArK00

Dichas vulnerabilidades podrían reducir o detener el desempeño en el servicio generando no solo pérdidas monetarias, sino de información, reputación y calidad. Cabe destacar que unos minutos fuera de servicios generaría un caos tanto para la compañía como para el usuario final.

En definitiva, equipos que ofrezcan múltiples capas de defensas además de explotar las vulnerabilidades encontradas, permitiendo interactuar con los servidores y monitorear cookies, accesos no permitidos, etc. logrando ofrecer confiabilidad en el desarrollo de los servicios.

4.3 Estructura de un DRP

La estructura de un plan de recuperación de desastres debe estar basada en una evaluación de riesgos y en el análisis de impacto al negocio (BIA). Según Kirvan “la evaluación de riesgos es uno de los componentes clave de la planificación de recuperación de desastres” (Computerweekly, 2011). Por lo cual para crear un plan que sea eficaz para la recuperación después de un desastre, una empresa necesita tener como prioridad cuales son los posibles desastres que pudieran ocurrir y cómo cada uno de ellos podría afectar su continuidad del negocio.

Los objetivos generales de la planificación de recuperación de desastres, que son para proporcionar estrategias y procedimientos que pueden ayudar a regresar a las operaciones de TI a un nivel aceptable de rendimiento lo más rápidamente posible después de un suceso perturbador. La velocidad a la que los activos de TI pueden ser devueltos a la ejecución normal o casi normal tendrá un impacto en la rapidez con la que la organización puede volver a la normalidad o de un estado provisional aceptable de las operaciones.

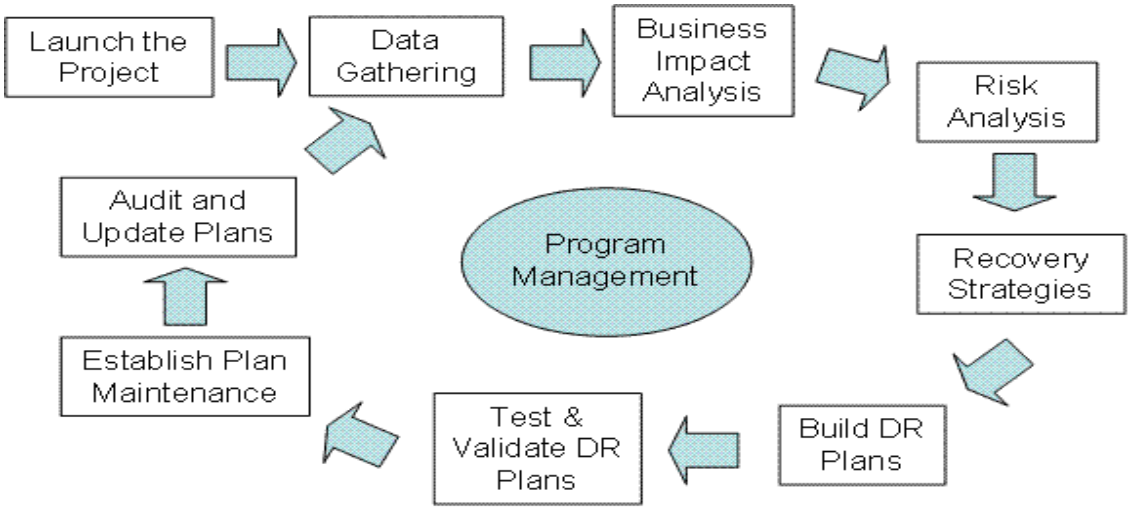


Figura 34. Círculo de desarrollo de continuidad en el negocio

Fuente: http://www.computerweekly.com/feature/Disaster-recovery-Risk-assessment-and-business-impact-analysis

4.4Necesidad de un DRP

Determinar la importancia que representa un plan de recuperación de desastres, se podría identificar con: ¿La institución cuenta con estrategias o métodos para desenvolver las funciones básicas en caso de desastre y no restaurar los datos, aplicaciones y operaciones en un plazo razonable después de un incidente? No, muchas instituciones no cuentan con un plan de recuperación ante desastre que cumpla con la protección y seguridad de los datos, por ende, no se puede recuperar lo que no se protege, lo que significa que sufrirá pérdidas significativas, que podría detener los servicios de manera parcial o total.

La recuperación de desastres es más que la definición de la estructura y la aplicación, conlleva la restauración de la infraestructura de TI en caso de incidentes. Para ello se involucra la administración de la institución y con ellos los departamentos que la integran, así obtener resultados óptimos.

Una vez esté involucrado el personal y las áreas que lo complementan se procede analizar los riesgos por área y su probabilidad. A partir del listado obtenido por área se analiza el impacto y secuelas que podrían surgir. Para la implementación de un DRP óptimo se analiza desde la pérdida total de la infraestructura, además de recuperación lenta del centro.

Posteriormente se asigna las prioridades, analizando los procesos y operaciones que se deben recuperar en el menor tiempo. Según la importancia delegada se procederá a la recuperación de la información. Dicho esto, se determinan las tácticas que serán implementados y costo asociado, considerando instalaciones de equipos, duplicación de datos en caso de no contar con una extensión, entre otros.

Unas de las funciones principales de un DRP es la restauración de la infraestructura de TI. La recuperación de desastre es un subconjunto de la estrategia de la continuidad del negocio, se concentra en los matices que no se relacionan con TI, como un aspecto esencial. El DRP debe de hacer un esfuerzo de integración entre los ejecutivos del negocio y el equipo del departamento de TI. Esto comienza con un análisis y evaluación de impacto en el negocio.

El DRP será correcto dependiendo de del sistema. Como la necesidad de almacenamiento de datos crece fuera del alcance de las instituciones, deben de considerar la externalización de esta función para centros de datos de terceros. Unas de las ventajas de los centros de datos de terceros, incluye el ahorro de costes, seguridad física avanzada y cumplimiento.

Las organizaciones de hoy en día deben de atesorar los procedimientos de comunicación interna y externa ante un desastre. “el ámbito del DRP se puede solapar con el del plan de contingencias de las TIC. Sin embargo, el DRP abarca un área más pequeña y no aborda trastornos menores que no requieren una relocalización. Dependiendo de las necesidades de la organización pueden añadirse del BCP, varios DRP como apéndices”. (Bertolin, 2008)

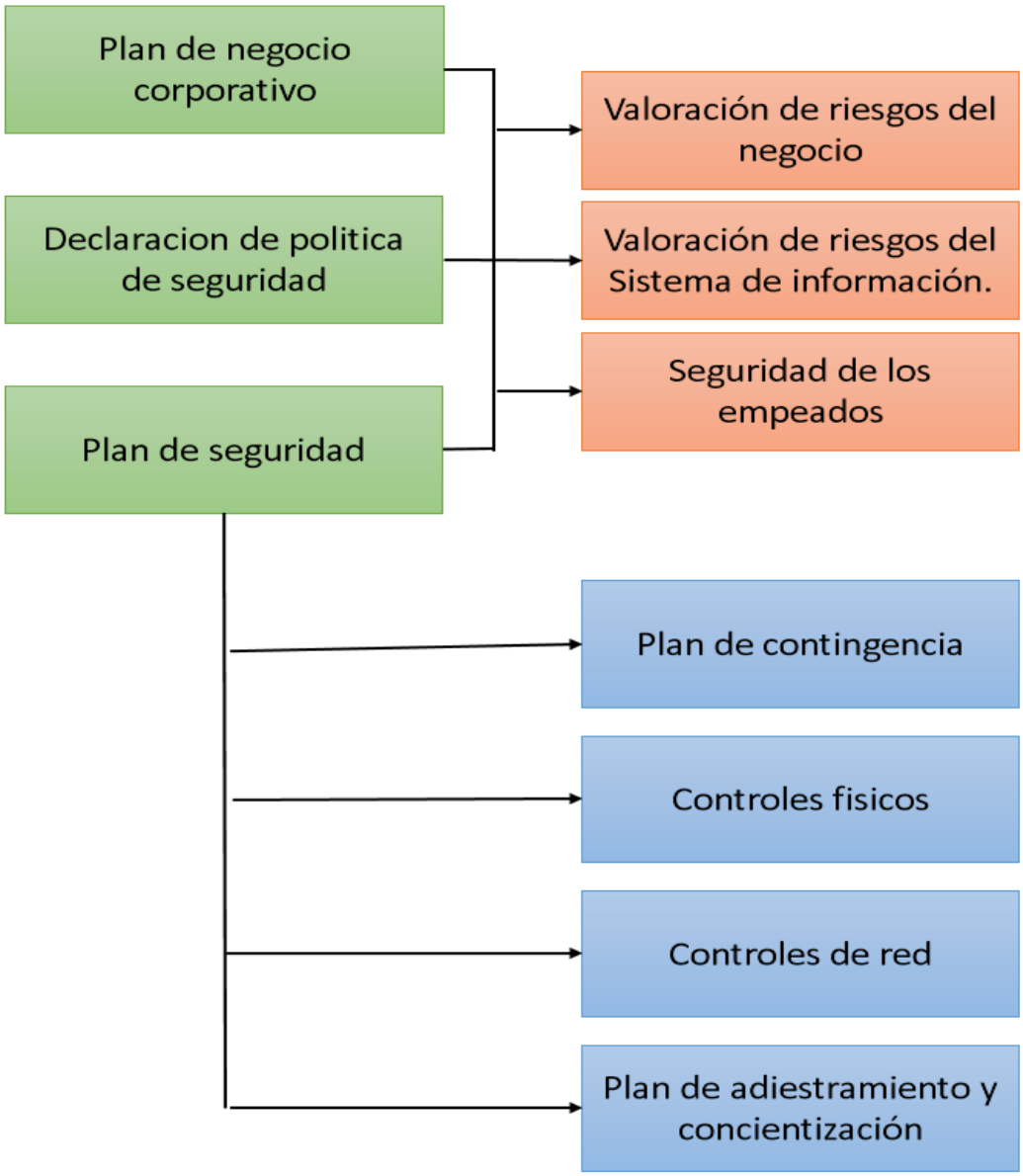


Figura 35. Elementos de un programa o plan de seguridad para un sistema de información.

Fuente: del libro Seguridad de la información, Redes, de Javier Areito Bertolin.

4.5 Recuperación de Desastres

A principio de los años 70, Norman L. Harris, Judith Robey y Edward S. tratando de descubrir un método de planificación y gestión que obstaculice la continua atención de problemas de manera fortuita. Esto dio lugar a la actividad que en sus inicios se le llamó Disaster Recovery Planning, es decir, planificación de la recuperación ante desastres.

Respaldar la información es una herramienta para duplicado de los datos más importantes que contenga la organización, esto es crucial para cuando suceda una falla electromecánica o un error en el sistema lógico, sea posible disponer de la mayor parte de la información importante para reanudar las actividades del día a día, y de esta manera evitar pérdidas de los datos. "Operaciones de recuperación es unos de los procedimientos que deben desarrollarse con anterioridad para definir las acciones que cada equipo de recuperación debe de desempeñar a continuación de las operaciones de respuesta para restaurar el nivel mínimo de actividad que se haya definido previamente"(Martinez, 2004).

Las fases para la creación de un plan de recuperación de desastre son:

- Se necesita elaborar y valorar el presupuesto de los recursos que se encuentran disponibles; infraestructura, vendedores, consultores, presupuesto de capital, etc.
- Gestionar las adquisiciones del equipamiento necesarios para la ejecución.
- Descripción de los riesgos, reconocer los activos que se encuentran en riesgo y de qué manera se pueden ver afectados, tanto como localizando los activos rehabilitados.
- Declaración del impacto del negocio, identificando las operaciones que se han paralizado, el procedimiento en que identifican la forma de restaurar las operaciones.
- Distinción para aprender de los errores y percibir el modo de intervención de los atacantes.

La recuperación de desastres es más que la definición de la estructura y la aplicación, conlleva la asignación de prioridades, que para ello se involucra los departamentos que integran la institución, así obtener resultados óptimos.

Conclusión

Un reto de gran importancia es la vulnerabilidad a la que se encuentran expuestas las organizaciones, con ellos nuevas amenazas y riesgos, que afectan tanto el prestigio de la institución como sus servicios.

El impacto de los desastres en las instituciones, no depende totalmente de la intensidad del fenómeno, está relacionado con el nivel de preparación de la empresa. Los diferentes escenarios se originan por diversas situaciones, lograr reducir el riesgo es el gran desafío. Un desafío ideal para las instituciones sería prever los riesgos que enfrentan en el día a día, al considerar proteger la infraestructura, servicios y aplicaciones. Lo cual trae como resultado la implementación de un plan de contingencia ante desastre, que permita garantizar la operación y funcionabilidad de la institución.

Un plan de contingencia ante desastre involucra procesos críticos de la institución, así como los riesgos a los que se encuentra expuesto, dichas variantes permiten evaluar la amenazas y procesos críticos a la mayor brevedad posible al momento de tener interrupciones.

Capítulo V

Propuestas de un plan de recuperación de desastre para la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

Introducción

La propuesta de un Plan de Desastres de Recuperación utilizando la Nube que se muestra a continuación es el resultado del análisis de cada uno de los servicios tecnológicos y procesos de negocio de la Oficina Presidencial de Tecnologías de la Información y Comunicación.

Se presenta una solución integrada, basada en la nube cuyo objetivo es garantizar que los servicios tecnológicos de la OPTIC puedan mantenerse disponibles ante cualquier desastre. Además, se muestra qué beneficioso resulta para la institución la implementación de este Plan de Recuperación de Desastres.

5.1 Situación Actual

La Oficina Presidencial de Tecnologías de la Información y Comunicación tiene el objetivo de proveer una infraestructura tecnológica moderna, con un elevado nivel de servicios que respondan a las necesidades tecnológicas actuales de los organismos gubernamentales y al mismo, tiempo controlar y reducir los costos de operación asociados.

A través de los servicios que proporciona el fomento de las TIC en las instituciones.

Servicios del Datacenter de la OPTIC:

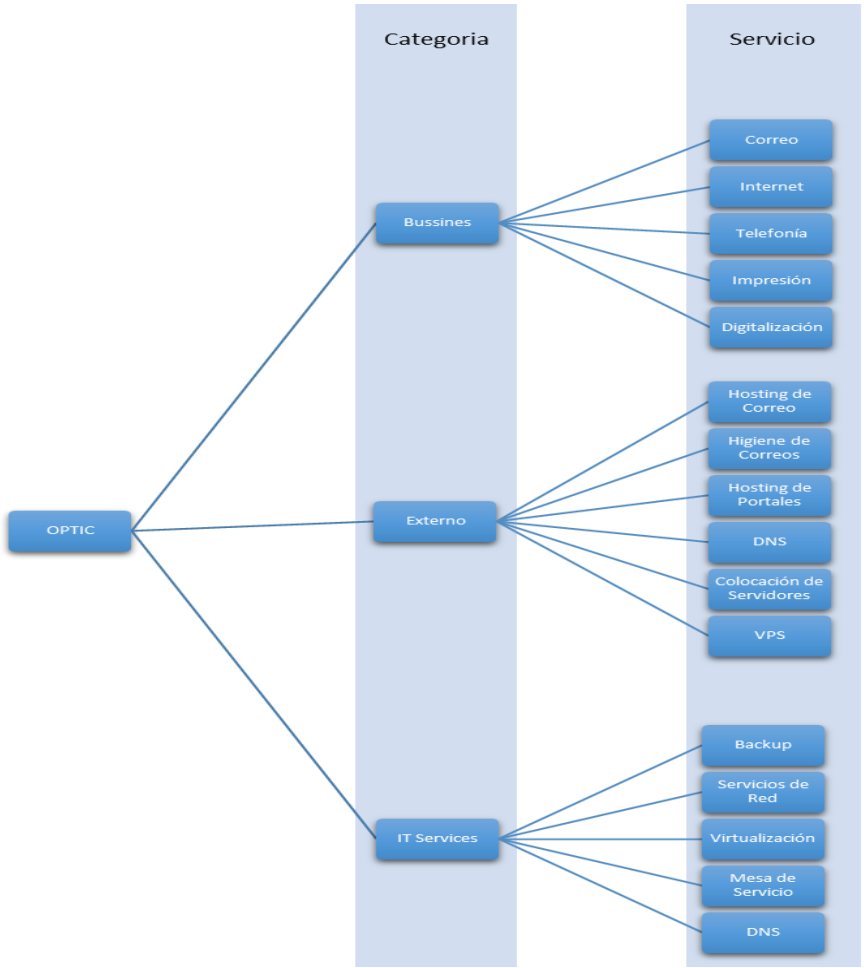


Figura 36. Servicios del Datacenter de la OPTIC.

Fuente: Los autores

En la actualidad, la OPTIC cuenta con un datacenter principal donde se alojan los servicios mencionados anteriormente. Este posee la infraestructura necesaria para garantizar la alta disponibilidad de los mismos. Además, en cuanto a capacidad posee, 160 núcleos de procesamiento, 320GB de ram y 40TB de almacenamiento; todo esto distribuido en 40 servidores físicos.

Los servicios alojados en este datacenter están bajo la certificación de ISO 20000, lo que implica que se manejan bajo un conjunto de procesos con el objetivo de garantizar la calidad y disponibilidad del servicio. Uno de los procedimientos claves para las operaciones de TI, es el de respaldo y recuperación el cual se realiza de manera off-line periódicamente según cada servicio, las copias realizadas se transfieren a cinta y se alojan en una localidad externa.

A pesar de las buenas prácticas implementadas, solo poseen contingencia en caso de eventualidades de conectividad y/o cortes de energía eléctrica de poco tiempo. En el caso de conectividad, poseen redundancia con varios proveedores, pero en su infraestructura interna no cuentan con equipos de comunicación redundantes; por lo cual, sí un equipo clave sufre una avería, se verían afectados los servicios por un tiempo prolongado. En cuanto a fallos de energía eléctrica, cuentan con UPS que pueden soportar la carga por un tiempo de 30 minutos y una planta con capacidad de brindar electricidad de forma ininterrumpida por 24 horas. Sí ocurre un desastre o evento (huracán, tormenta, terremoto, entre otros) que comprometa los equipos de infraestructura o la edificación como tal, la OPTIC interrumpiría todos sus servicios por un tiempo indeterminado en el cual puedan proceder a restaurar las copias off-line que poseen en una nueva localidad, el tiempo no se ha estimado ya que no poseen los equipos necesarios en otras localidades para realizar el proceso de recuperación.

Según las informaciones suministradas por la OPTIC, se estima que el RPO es de 24 horas, ya que el ciclo de respaldo se hace cada 24 horas. Esto se debe a que el Objetivo de Punto de Recuperación (RPO, Recovery Point Objective) de la OPTIC no se encuentra bien definido.

Otro punto importante, es el Objetivo de Tiempo Recuperación (RTO, Real Time Objetive) el cual no se ha determinado, debido a que la OPTIC es una institución gubernamental cuyo fin no es generar ingresos. El impacto no se ve reflejado solo como un costo, sino como un daño en

imagen que afecta a todo el Gobierno Dominicano ya que es la entidad que representa el Gobierno Electrónico en la República Dominicana.

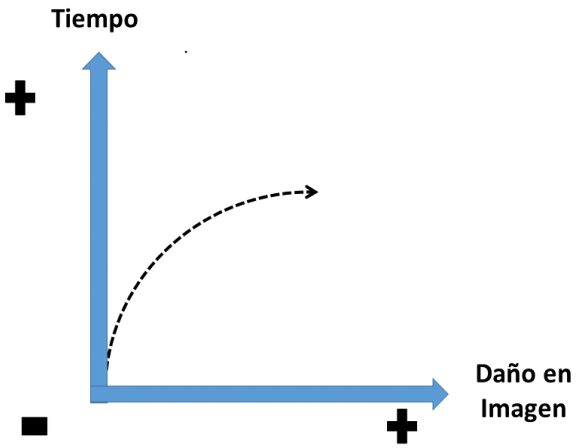


Figura 37. RPO, Recovery Point Objective & RTO, Real Time Objetive

Fuente: Los autores

5.2 FODA

Figura 38. Análisis FODA.

Fuente: Los autores, auxiliado de la OPTIC.

5.3 Diagrama Actual de la OPTIC

La Oficina Presidencia de Tecnologias de la Informacion y Comunicación posee tres localidades, las cuales se encuentran conectadas entre sí a través de enlaces de internet utilizando conexiones de redes virtuales (VPNs), como se muestra en la siguiente imagen :

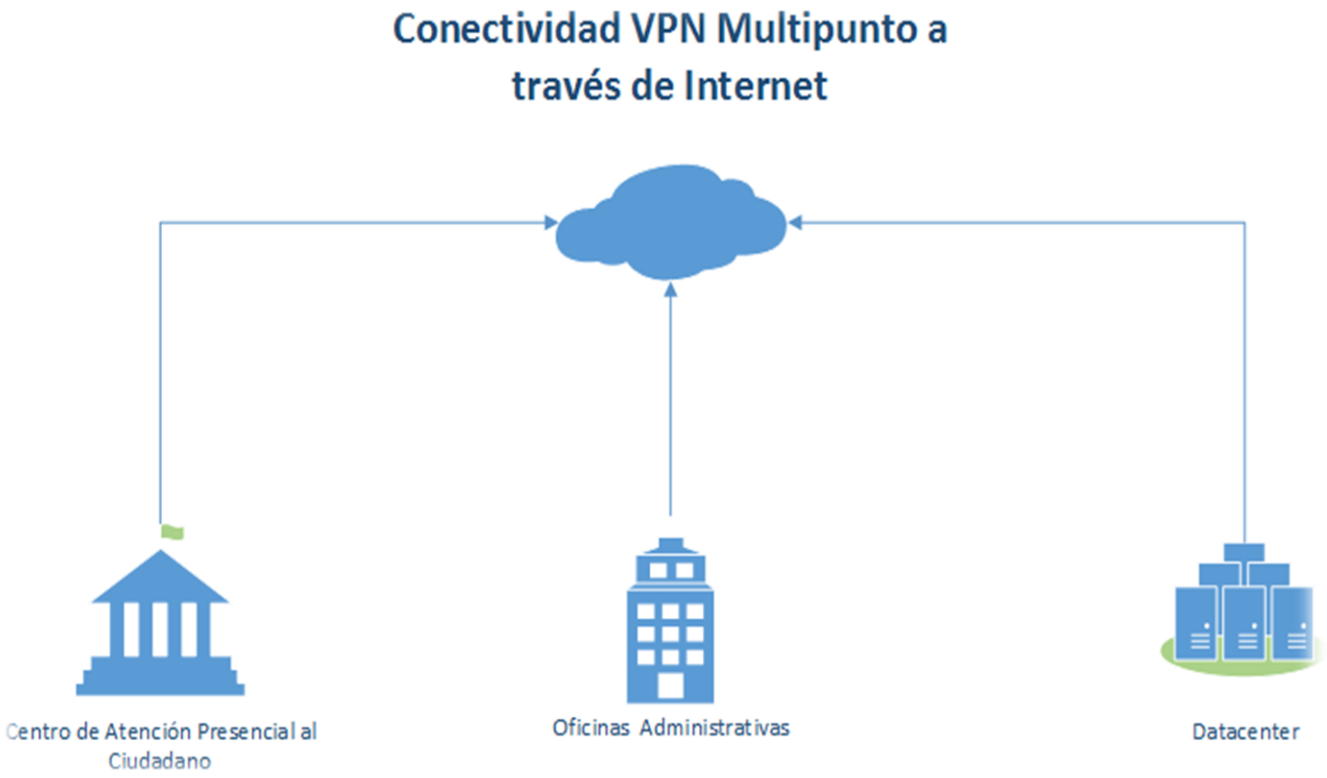


Figura 39. Diagrama Actual de la OPTIC.

Fuente: Los autores.

Los servicios son accedidos por los clientes a través de internet utilizando de tres proveedores de internet diferentes. Las diferentes localidades de la OPTIC acceden a los servicios a través de las conectividades VPN.

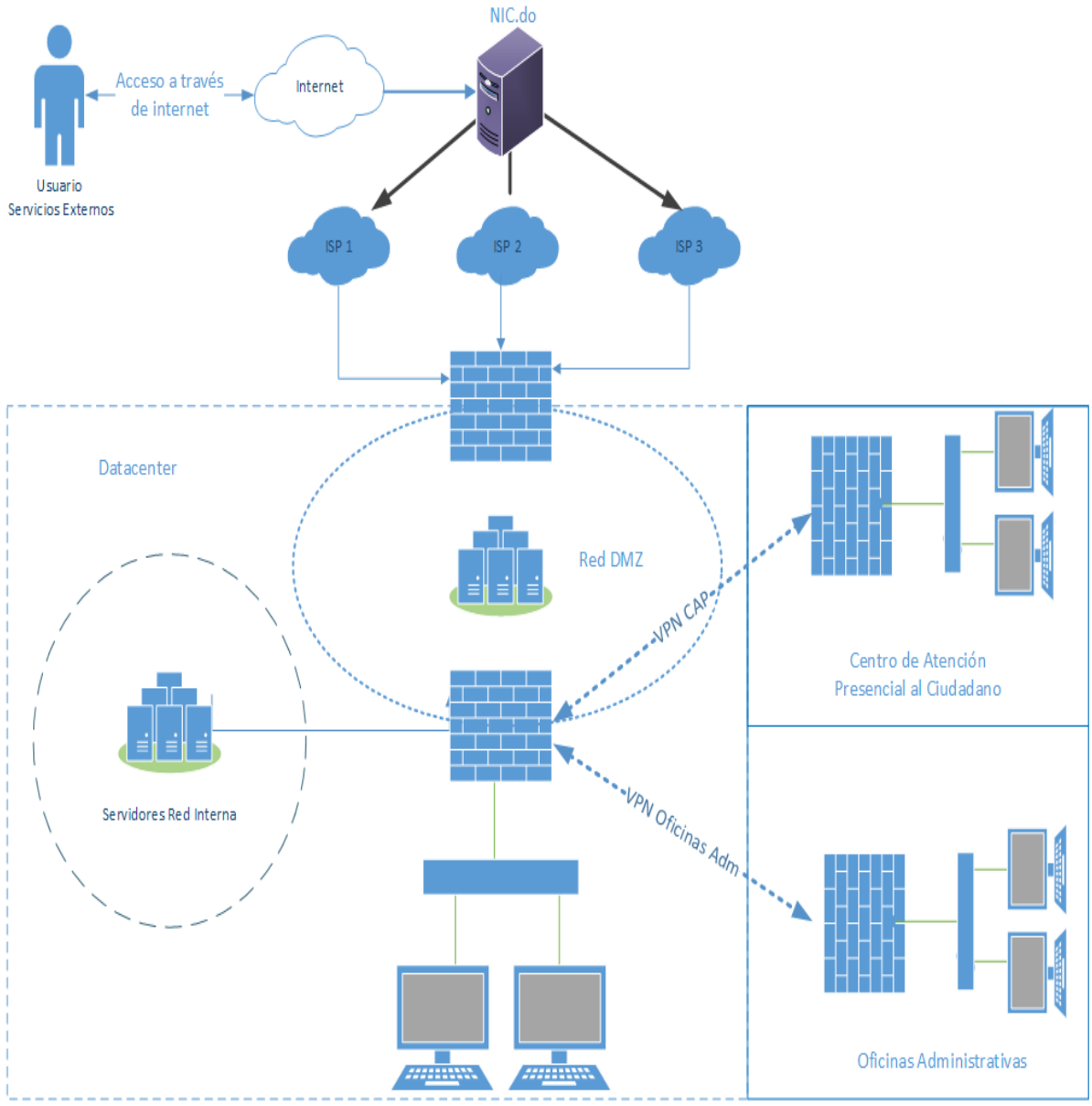


Figura 40. Diferentes localidades de la OPTIC

Fuente: Los autores

Al momento de que los usuarios acceden al servicio, las peticiones realizadas a través de internet son dirigidas a la NIC.do, la cual redirige el tráfico a los servidores DNS de la OPTIC, como se muestra a continuación:

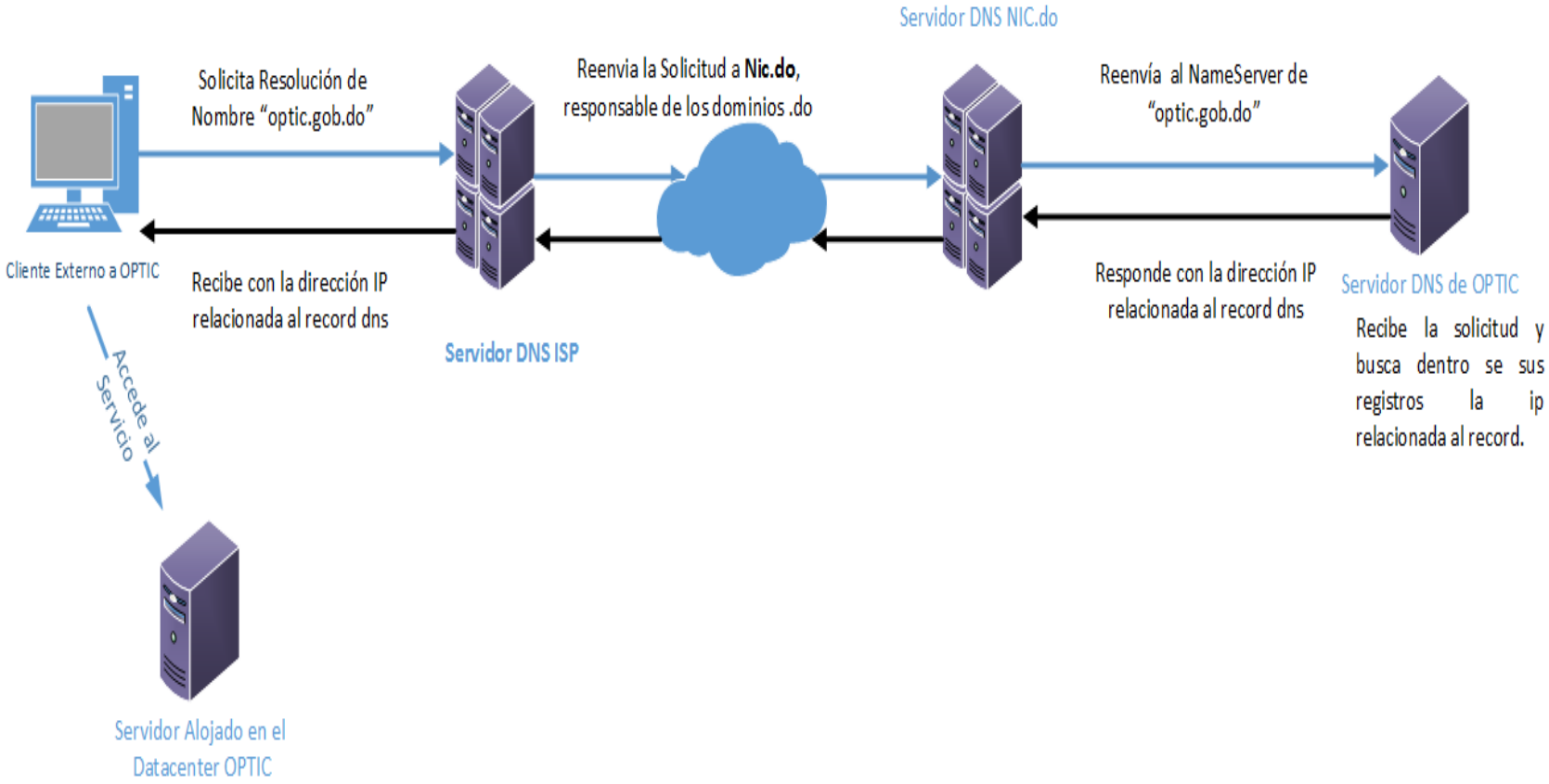


Figura 41. Trafico a los servidores DNS de la OPTIC.

Fuente: Los autores.

5.4 Propuesta Nueva para la OPTIC

5.4.1 Diagrama de Infraestructura

La propuesta del plan de recuperación de desastres para la Oficina Presidencial de Tecnologías de la Información y Comunicación, se enfoca en proponer un diseño de infraestructura y un conjunto de procesos que provean alta disponibilidad a pesar de cualquier amenaza que pueda materializarse.

Por lo cual se propone la restructuración de su topología lógica con integración de una cuarta localidad en la Nube de Microsoft Azure, la cual servirá para la realización de copias de respaldos online y como contingencia en caso de un desastre.

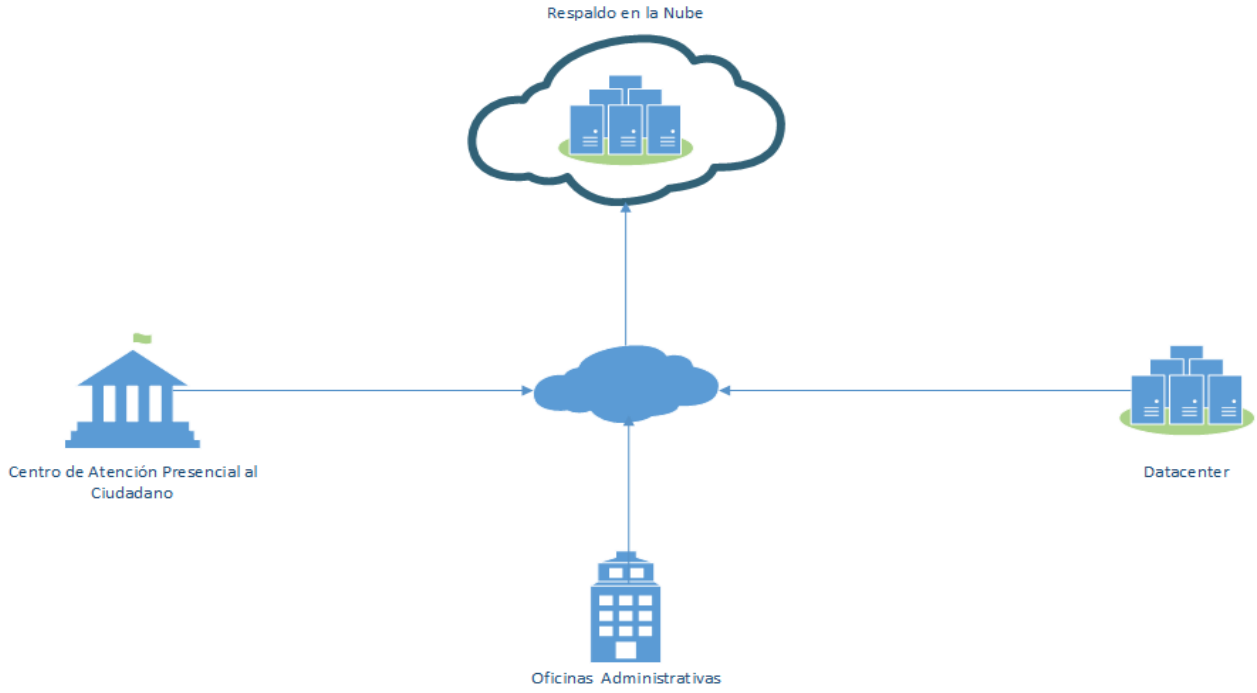


Figura 42. Diagrama de Infraestructura para la OPTIC

Fuente Los autores

5.4.2 Infraestructura Propuesta

La propuesta de infraestructura que se incluye en el plan de recuperación de desastres añade una tercera localidad, además se modifica el flujo de peticiones del cliente al servidor ya que se añade un nuevo servidor DNS el cual entrara en funcionamiento en caso de que el primero no responda en el tiempo considerado.

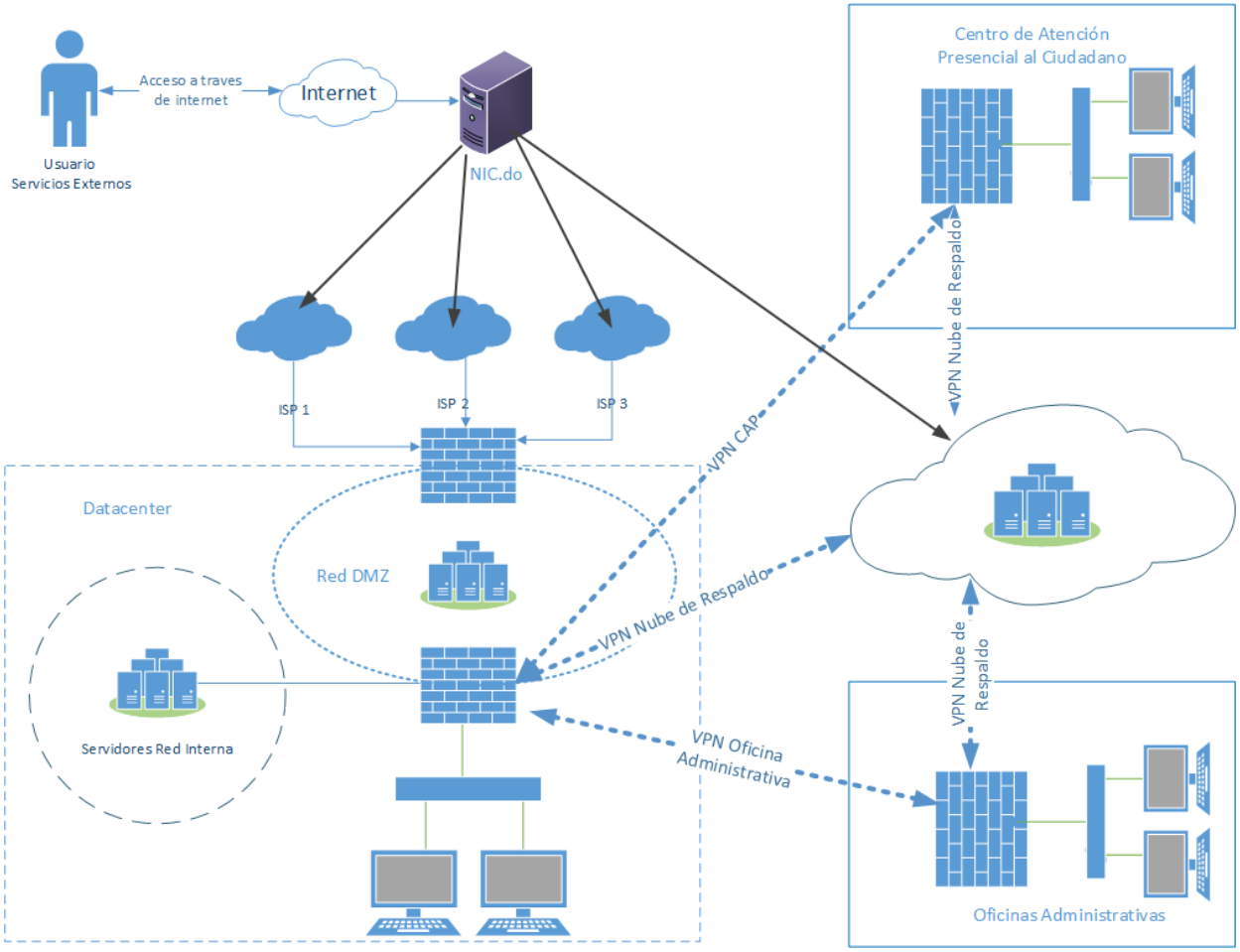


Figura 43. Infraestructura Propuesta para la OPTIC

Fuente Los autores

5.5 Flujo de Peticiones Cliente Servidor

Al momento de que los usuarios accedan al servicio, las peticiones realizadas a través de internet serán dirigidas a la NIC.do, donde a su vez se redirigirá el tráfico a los servidores DNS de la OPTIC ubicados en su datacenter local, en caso de no encontrarse disponible el mismo estará un servidor DNS Replica localizado en la nube con el fin de redirigir todo el tráfico de las solicitudes realizadas a la nube, como se muestra a continuación:

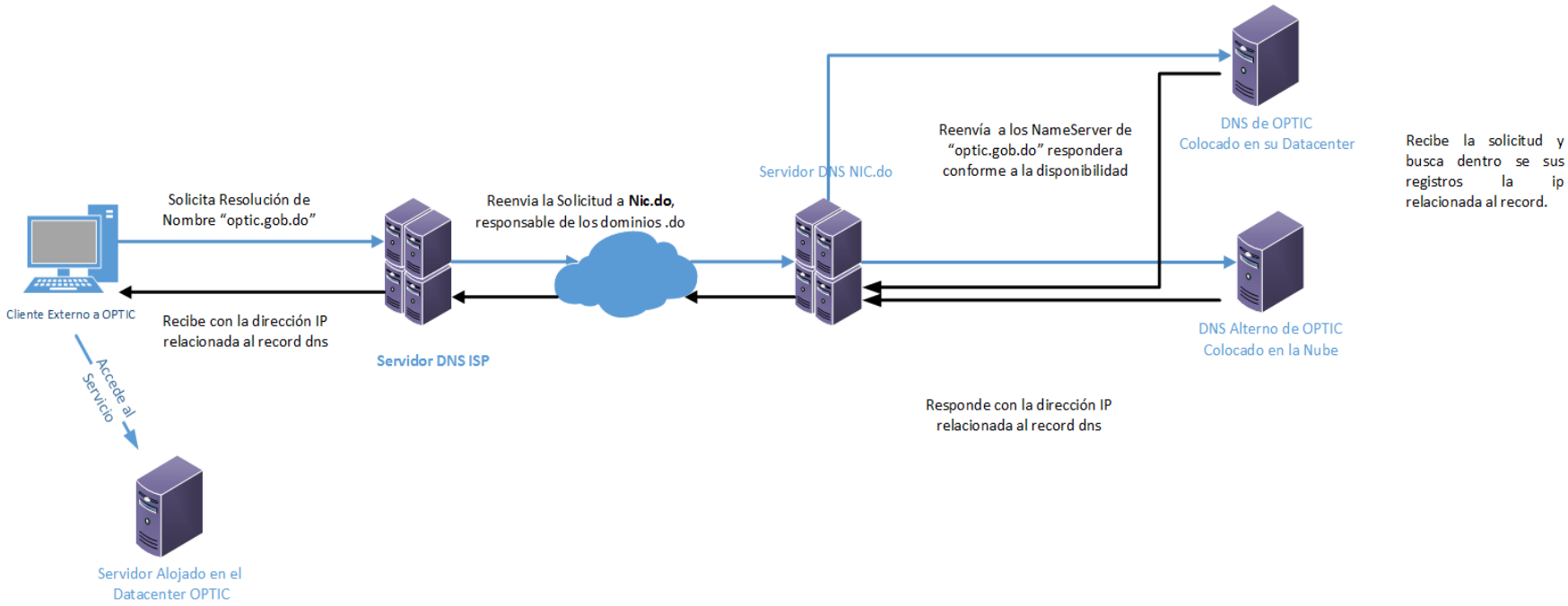


Figura 44. Flujo de Peticiones Cliente Servidor

Fuente Los autore

5.5 Alcance de los Servicios

Para proveer los servicios que necesita la Oficina Presidencial de Tecnologías de la Información y Comunicación, se utilizará la nube de Microsoft Azure, esto se debe a la flexibilidad de los costos que posee y la gran integración con la infraestructura de virtualización (Hyper -V) que tiene la OPTIC. Esto permitirá que el proceso de sincronización y respaldo online con la nube se realice de forma rápida y sencilla. Desde la nube se proveerán los siguientes servicios:

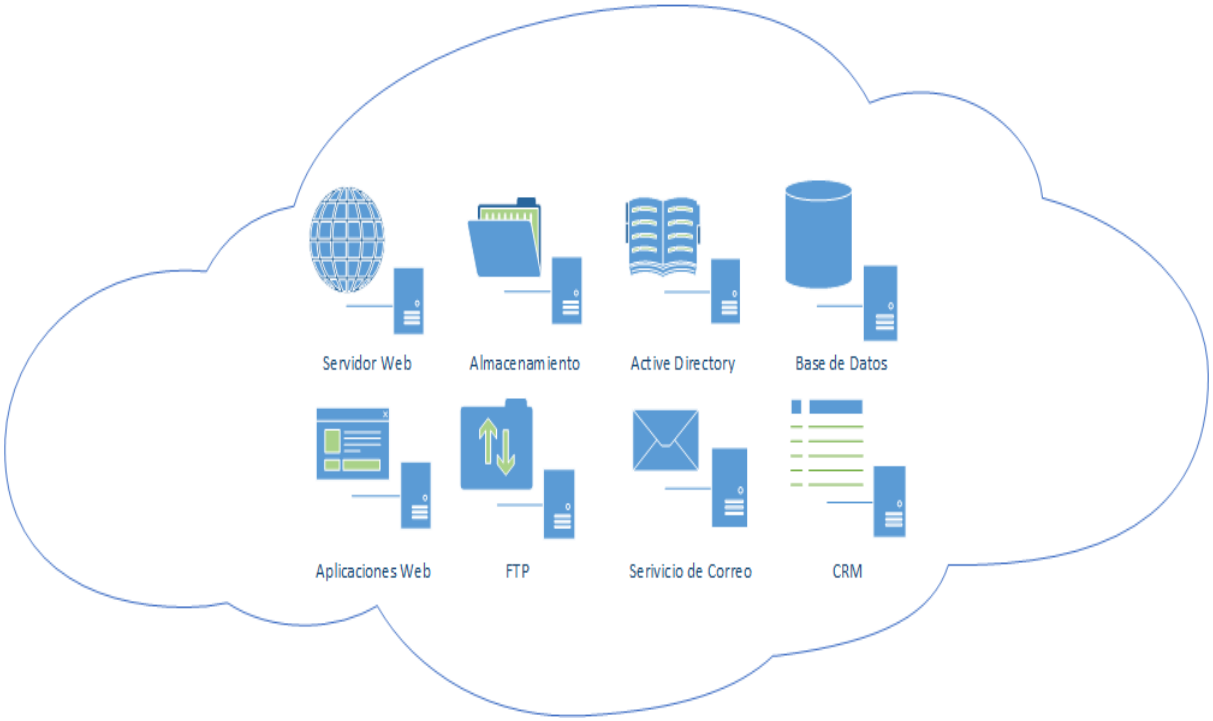


Figura 45. Alcance de los Servicios.

Fuente: Los autores.

5.6 RTO y RPO

Sistemas Critico	RTO	RPO	Amenazas	Estrategia de Prevención	Estrategia de Respuesta	Estrategia de Recuperación
Correo Interno	15 Minutos	1 Hora	Fallo en el Servidor	Backup Online en la Nube / Backup Offline On Site	Redirección DNS al Site Alterno	Se procede a restaurar las copias del respaldo de cada servicio gradualmente hasta volver al punto de operación normal
ERP/ Sistema Contable		3 Horas	Desastres Naturales			
Hosting de Correo		1 Hora	Fallas en el ISP			
Filtrado de Correo		1 Hora	Ataques DDoS			
Hosting de Portales		30 Minutos	Sabotajes			
DNS		10 Minutos				
Colocacion de Servidores		15 Minutos				
VPS		15 Minutos				

Tabla 5. RTO y RPO.

Fuente: Los autores.

5.7 Plan de Inversión

Para realizar este proyecto se utilizará el servicio de Microsoft Azure debido a la integración que tiene con los servicios de virtualización que posee la Oficina Presidencial de Tecnologías de la Información y Comunicación, en la siguiente tabla se muestran los costos de la implementación y servicio para brindar la capacidad necesaria para un plan de recuperación de desastres en la nube que soporte los servicios de la OPTIC.

Servicio	Descripción	Costo Estimado
Virtual Machines	40 Standard virtual machine(s), D12 (4 cores, 28 GB RAM, 200 GB disk, $0.652/hr) size: 1 months	$ 906,144.38
SQL Database	20 basic database(s) x 1 months, size: b	$ 4,655.80
Storage	50 TB storage Block blob type. Basic tier, LRS redundancy, 100000 x100,000 transactions	$ 73,259.67
Azure Active Directory	free tier, per-user MFA billing model, 300 MFA user(s), 50000 stored user(s), 50000 authentication(s), 0 multi-factor authentications, 25001-100000 directory objects, 1 months	$ 26,562.96
Site Recovery	0 instance(s) of Recovery to customer-owned sites, 40 instance(s) of Recovery to Azure	$ 46,700.00
Soporte	Servicio de soporte especializado por Microsoft	$ 46,700.00
Total Mensual		**$ 1,104,022.82**
Total Anual		**$13,248,273.83**

Tabla 6. Plan de Inversión.

Fuente: Los autores.

Costo de Diseño del DRP

El costo de asesoría para el Plan de Recuperación de Desastres utilizando la nube es:

- $ 750,000.00

Todos estos costos son en pesos calculados a una tasa de cambio de $45.7 pesos dominicanos por $1.00 dólar americano.

5.8 ROI

Para la puesta en marcha de este proyecto es necesario conocer la factibilidad del mismo, por lo que es necesario conocer cuál es el retorno de inversión para la OPTIC y la rentabilidad del mismo.

$$\text{ROI} = \frac{\text{Ganancia} - \text{Inversión}}{\text{Inversión}} \times 100$$

$$\text{ROI} = \frac{\$2{,}617{,}116.71 - \$\ 1{,}754{,}022.82}{\$\ 1{,}754{,}022.82} X100$$

ROI = 49%

Esto indica que por cada peso invertido se recibirá a cambio $1.49, lo cual demuestra la factibilidad económica de este proyecto.

5.9 Cronograma de Actividades para el Proyecto

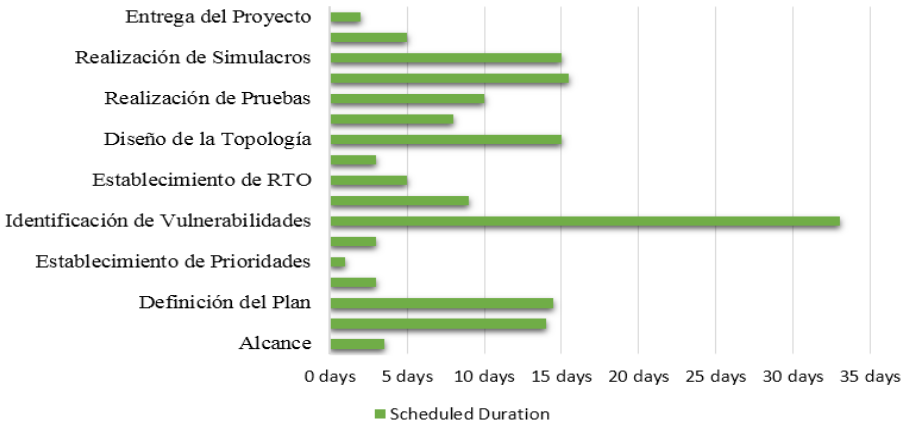


Tabla 7. Cronograma de Actividades para el Proyecto.

Fuente: Los autores

Nombre de la Tarea	Nombre de la Tarea	Nombre de la Tarea
DRP Utilizando la Nube para la OPTIC	130 days	Thu 11/10/16
Alcance	4 days	Thu 11/10/16
Recolección de la Información	14 days	Tue 11/15/16
Definición del Plan	14.5 days	Mon 12/5/16
Identificación de Servicios	3 days	Mon 12/26/16
Establecimiento de Prioridades	1 day	Thu 12/29/16
Idnetificación de Amenazas	3 days	Mon 12/26/16
Identificación de Vulnerabilidades	33 days	Thu 11/10/16
Establecimiento de RPO	9 days	Mon 12/5/16
Establecimiento de RTO	5 days	Fri 12/16/16
Selección de Estrategia de Recuperación	3 days	Fri 12/23/16
Diseño de la Topologia	15 days	Wed 12/28/16
Diseño de la Infraestructura	8 days	Wed 1/18/17
Realización de Pruebas	10 days	Mon 1/30/17
Implementación	15.5 days	Mon 2/13/17
Realización de Simulacros	15 days	Tue 4/11/17
Capacitación del Personal	5 days	Tue 5/2/17
Entrega del Proyecto	2 days	Tue 5/9/17

Tabla 8. Fase de las actividades.

Fuente: Los autores

5.10 Beneficios de la Propuesta

Luego de evaluar la propuesta es importante destacar los siguientes beneficios para la OPTIC:

- Se identifican los sistemas críticos, las amenazas existentes y cómo afecta a la empresa la interrupción de estos servicios.
- Minimiza los riesgos generados por la falla de los servicios.
- Define los nuevos objetivos de tiempo de recuperación y los objetivos de punto de recuperación lo cual es información vital para la toma de decisiones.
- Se plantea un rediseño de la topología física y lógica de la empresa, el cual añade una nueva localidad cuyo objetivo es servir de respaldo y contingencia para los servicios tecnológicos. El nuevo diseño cuenta con una topología full mesh que permite la continuidad de las operaciones de TI ante cualquier eventualidad que afecte cualquiera de las localidades, lo cual provee confianza en el servicio.
- Se establecen los procesos necesarios y los responsables para mantener un plan de recuperación de desastres. Además, se definen los pasos a seguir antes las diferentes eventualidades que se presenten para mantener el servicio.
- Contar con una solución de respaldo en la nube es el primer paso para crear la base y la estructura necesaria que permita en mediano plazo poder migrar de forma completa todos los servicios a la nube, con el fin de seguir aumentando la disponibilidad, mejorar la confiabilidad y reducir los costos operativos de la organización.
- La solución de infraestructura en la nube siempre es tecnología actualizada, que no se desvalúa en el tiempo a diferencia de la infraestructura local.
- Limita la pérdida de ingresos y los gastos excesivos en medio de un evento o desastres inesperados que afecte a la empresa.

CONCLUSIÓN

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) es la responsable de la implementación del Gobierno Electrónico en el país a través del uso de las Tecnologías de la Información y Comunicación (TIC). Además, brinda múltiples servicios de forma interna a sus usuarios, también de forma externa a diferentes instituciones del estado como también a los ciudadanos. Dentro de los servicios que ofrece se encuentra alojamiento de correos, alojamiento de páginas web, alojamiento de aplicaciones, atención ciudadana vía telefónica, entre otros.

Según el primer objetivo, se identificó la incidencia y la relevancia de la infraestructura de TI para la OPTIC, se pudo evidenciar a través de la identificación de los servicios y sistemas críticos de la organización que la infraestructura de TI tiene un papel fundamental en las operaciones de organización, esto se debe a que la OPTIC es la representación del Gobierno Electrónico en todo el estado Dominicano, por lo cual una interrupción en sus servicios a las demás institución y/o al ciudadano representa un gran daño a la imagen de la institución.

Para el segundo objetivo, se determinó cuáles procedimientos posee la OPTIC para prevenir y responder a los diferentes eventos inesperados que pueden presentarse. Además, se identificó tanto al personal responsable de cada una de las áreas y procesos, así como también, la documentación clave para llevar a cabo cada uno de dichos procesos.

Según el tercer objetivo, se identificó las posibles causas que pueden interrumpir las operaciones, se establecieron las amenazas, lo cual a su vez permite la delimitación del alcance que debe tener el plan de recuperación de desastres.

En el cuarto objetivo, se analizó las diferentes vulnerabilidades que pueden afectar a los sistemas de la OPTIC. También se evaluó los riesgos de dichas vulnerabilidades con el fin de determinar cómo puede afectar los mismos a la organización.

Luego de obtener estas conclusiones, es importante que la OPTIC, como organización que representa el Gobierno Electrónico y como portavoz de las buenas prácticas de tecnología, examine las recomendaciones expresadas a continuación.

RECOMENDACIONES

Luego de observar los procesos y actividades de la OPTIC, donde se obtuvo la oportunidad de ingresar y evaluar las características y condiciones a las que se encuentra expuesta, se procede a recomendar:

1. Definir cada proceso y flujo crítico que resguardan las operaciones de TI, ya que esto permitirá conocer de forma clara cuales son las posibles amenazas y vulnerabilidades que pueden afectar
2. Se recomienda capacitar el personal responsable de velar por el cumplimiento de los procesos que garantice el funcionamiento óptimo del DataCenter.
3. Identificar e implementar controles con el fin de prevenir o disminuir las interrupciones en los servicios, y así mantener los niveles de la disponibilidad prometida y a su vez, reducir los costos de una posible recuperación.
4. Elaborar un conjunto de estrategias de recuperación, esto con el objetivo de garantizar la recuperación de los servicios de manera rápida y efectiva después de una interrupción.
5. Definir el Tiempo de Recuperación y el Punto de Recuperación, determinando la prioridad en caso de ocurrir incidentes y cuales procesos resultan críticos e imprescindibles para el funcionamiento de las actividades.
6. Se recomienda la evaluación del Plan de Recuperación de Desastres actual, donde se exhorta a realizar los cambios pertinentes que permita la continuidad de los servicios ante cualquier eventualidad que afecte las operaciones de TI identificadas en el último capítulo.
7. Rediseñar su Plan de Recuperación de Desastres utilizando la nube de forma tal que puedan tener disponible un respaldo adicional de sus sistemas off-site (fuera de sitio) con el fin de poder recuperar y reactivar los servicios en un tiempo mínimo.
8. Se recomienda empezar a evaluar la posibilidad de migrar de forma mediano o a corto plazo, toda su infraestructura de tecnología a la nube con el objetivo de seguir aumentando los niveles de disponibilidad de cada servicio.

BIBLIOGRAFIA

Libros

Arias, Á. (2015). *Computación en la Nube: 2ª Edición.* IT Campus Academy.

Carpenter, T. (2011). *Microsoft Windows Server Administration Essentials.* John Wiley & Sons.

Coloritto, Rodrigo. (2013). Seguridad & Datacenter *Logicalis Now*, 12.

Ferrill, P., & Ferrill, T. (2014). *Exam Ref 70-413 Designing and Implementing a Server Infrastructure.* Microsoft Press.

Guise, P. d. (2008). *Enterprise Systems Backup and Recovery: A Corporate Insurance Policy.* Florida: CRC Press.

Hidalgo, J. R., & Campins Eritja, M. (2000). *De las catástrofes ambientales a la cotidianidad urbana: la gestión de la seguridad y el riesgo.* Barcelona: Edicions Universitat.

IBM. (18 de 11 de 2015). IBM abre Centro de Continuidad de Negocios en la Nube. México, México

López-Vázquez, M. A.-P. (2012). *Fundamentos de las Infraestructuras de Datos Espaciales (IDE)* (Vol. 1ª edición). (U. Press, Ed.) Madrid.: UPM Press. Obtenido de www.upmpress.es / upmpress@fgupm.es.

Pablo Gil Vázquez, J. P. (2010). *Redes y Transmisión de Datos.* (U. D. PUBLICACIONES, Ed.) Universidad de Alicante. Obtenido de https://books.google.com.do/books?id=On6y2SEaWyMC&printsec=frontcover#v=onepage&q&f=false

Southwick, P., Marschke, D., & Reynolds, H. (2011). *Junos Enterprise Routing: A Practical Guide to Junos Routing and Certification.* "O'Reilly Media, Inc.".

Viñals, J. T. (2011). *Empresas en la Nube.* Libros de Cabecera.

Revistas y Articulos

Buyya, R., Yeo, S. C., & Venugopal, S. (2008). *Market-Oriented Cloud Computing:Vision, Hype, and Reality for Delivering IT Services as Computing Utilities.* Obtenido de http://www.buyya.com/papers/hpcc2008_keynote_cloudcomputing.pdf

Conroy, M. (s.f.). Protegiendo la TI. *nfpa Latinoamericano*. Obtenido de http://www.nfpajla.org/archivos/edicion-impresa/alarma-deteccion-senalizacion/628-protegiendo-la-ti

Fernandez, A. (13 de 12 de 2011). *Expansion* . Obtenido de Expansion.com: http://www.expansion.com/accesible/2011/12/13/empresas/1323804371.html

Gómez, J. A. (2011). *Redes Locales.* Editex.

Interoute. (16 de Enero de 2016). Obtenido de http://www.interoute.com/cloud-article/what-hybrid-cloud

José Carlos Gallego . (2015). *Instalación y Mantenimiento de Redes para Transmision de Datos.*

Juan Carlos Martin Castillo. (2009). *Instalaciones de Telecomunicaciones.*

Kirvan, P. (Mayo de 2011). *Computerweekly*. Obtenido de http://www.computerweekly.com/feature/Disaster-recovery-Risk-assessment-and-business-impact-analysis

Martinez, J. G. (2004). *Planes de Contigencia: la Continuidad del Negocio en las Organizaciones.*

Martínez, J. G. (2004). *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones.* Madrid: Diaz de Santos, S. A.

Muñoz, A. A. (s.f.). *Teleinformática y Redes de Computadores.*

RedUsers. (2010). *Redes Cisco. Instalación y Administracion de Hardware y Software.*

Río, M. D. (2014). *Tecnologías de Virtualización.* IT Campus Academy.

Rivas, A. (7 de Enero de 2013). *Definición de un Sistema de Cableado Estructurado.* Obtenido de Next Solutions:

http://www.nexxtsolutions.com/co/blog/2013/01/definicion-de-un-sistema-de-cableado-estructurado

Rouse, M. (June de 2014). *whatis.techtarget.com*. Obtenido de http://whatis.techtarget.com/definition/server

Schlez, M. (Marzo de 2012). Hacia una Intraestructura de Data Canter unificada. *Logicalis, 17*, 45. Obtenido de https://issuu.com/logicalislatam/docs/logicalisnow17

GLOSARIO

- **Automatización:** Sistema de transmisión de tareas de producción, habitualmente realizadas por operadores humanos a un grupo de elementos tecnológicos.
- **Cloud Computing:** Conocida como computación en la nube, brinda servicios a través del internet. Se puede acceder a las informaciones, sin poseer una gran infraestructura.
- **Confiabilidad:** Un sistema es más confiable si es tolerante a errores. Si el sistema presenta un error en un solo elemento, el elemento redundante asumirá su función sin que produzca un tiempo de inactividad considerable.
- **Datacenter:** Centros seguros donde se concentra las instalaciones de servidores y diversos recursos tecnológicos, para el procesamiento de las informaciones de una institución.
- **DCOM:** (Distributed Component Object Model) Esta tecnología desarrolla componentes de software ordenados sobre varias computadoras y que se comunica entre sí.
- **DRP:** Plan de recuperación de desastres es más que la definición de la estructura y la aplicación, conlleva la restauración de la infraestructura de TI en caso de incidentes.
- **Escalabilidad:** Es la característica de aumentar la capacidad de trabajo o tamaño del sistema sin comprometer su funcionamiento y calidad de este.
- **Estandarización:** Es el proceso de unificación de una serie de características en servicios, procedimientos y normas. Su finalidad es la reducción de costos de la empresa.
- **IaaS:** (Infrastruture as a Service) Es uno de los tres modelos importantes en el campo del cloud computing, este proporciona acceso a recursos informáticos situados en un entorno virtualizado.
- **IEEE 802.11:** Es un estándar conocido como Instituto de Ingenieros Eléctricos y Electrónicos. En el 2009 con la aparición del estándar 802.11 n, supera los 100Mbps.

- **Infraestructura Tecnológica:** Es el conjunto de hardware y software que sustenta los diferentes servicios de una institución para el funcionamiento de todas sus actividades.
- **Internet:** Es una agrupación de redes interconectadas a nivel mundial con la característica de que cada una de ellas es independiente y autónoma.
- **Ipv4:** Es la versión 4 del protocolo de internet, que se limita a 4.3 mil millones de direcciones, utiliza direcciones de 32 bits. Se centra en estándares de interconexión de redes basados en internet.
- **Ipv6:** Es la versión 6 del protocolo de internet, se apoya de 128 bits. Si lo elevamos a la 128va potencia recibiremos el total de direcciones IPv6 totales.
- **NIST:** (The National Institute of Standars and Technology), responsable del desarrollo de normas y directrices, proporcionando seguridad de la información adecuada para todas las operaciones de la agencia y activos.
- **PaaS:** (Platform as a Service) Esta Categoria de los servicios en la nubes proporciona un entorno donde los desarrolladores pueden crear aplicaciones y servicios que funcionen a través de internet.
- **Protocolo IP:** (Internet Protocol) proporciona servicios de distribución de paquetes de información. Es utilizada por el protocolo de transporte.
- **RAID**: (Redundant Array of Inexpensive Disk) Redundante de discos independientes, es un Sistema de almacenamiento de datos en tiempo real que utiliza unidades de almacenamiento de datos.
- **Red LAN**: Es una red de área local, esta permite la interconexión de dispositivos en área reducidas.
- **Red Wan:** Es una red amplia, que nos permite interconectarnos a larga distancia.
- **Redundancia:** Son las repeticiones de la información contenida en un mensaje, que proporciona, a pesar la perdida de una parte de este.
- **Routers:** Es un dispositivo que tiene como función administrar el tráfico de información que circula por una red de computadoras.
- **RPO:** (Recovery Point Objetive), Indicador del tiempo tolerable para la recuoeracion de datos durante una interrupcion.
- **RTO:** (Recovery Time Objective), Intervalo de tiempo entre la caida y la restauracion de los servicios, especificado en HH/MM/SS.

- **SAAS:** (Software as a Service), apliacion online de prestacion de software online en lugar de comprar e instalar.
- **SOA:** (Service Oriented Architecture) Es un concepto de arquitectura orientada a servicios para dar soporte a los requisitos que solicita el negocio.
- **Switches:** Dispositivo digital lógico que permite la interconexión de equipos que ejecutan en la capa de enlace de datos del modelo OSI.
- **TIA/EIA-568:** Este estándar hace referencia al cableado de telecomunicaciones para edificios comerciales. Este estándar tiene como objetivo ser universal, tanto en servicios soportados como en fabricantes compatibles.
- **TIA/EIA-942:** (Telecommunications Indutry Association) Es un estándar que proporciona una serie de recomendaciones y normas para la instalación de centros de datos.
- **TIC:** Las Tecnología de la Información y la Comunicación, es la agrupación de tecnologías desarrolladas para gestionar información.
- **TIER:** Metodologia que permite calcular el tiempo de disponibilidad en los centros de datos.
- **Topología de Red:** Son las configuraciones que acogen las interconexiones entre los equipos.
- **Virtualización:** Es una solución viable que hoy en día utilizamos para reducir los costes relacionados con los sistemas informáticos.
- **Vulnerabilidades:** Es la debilidad de cualquier tipo que arriesga la seguridad de un sistema informático.

ANEXOS

Tabla de Anexos

Anexo 1. Entrevista realizada al Ing. Charli Polanco, Director de Tecnología de la Información

1. ¿Qué rol desempeña el departamento de Tecnologías de la Información para la OPTIC?

   El departamento de TI tiene un papel clave para la OPTIC ya que es el que soporta las operaciones para poder brindar los servicios a sus diferentes clientes.

2. ¿Cuántas localidades poseen?

   Actualmente contamos con tres localidades, las oficinas administrativas, nuestro centro de atención presencial al ciudadano y nuestra localidad operativa donde se encuentra nuestro datacenter.

3. ¿Poseen equipos de seguridad perimetral?

   Si, contamos con una gran infraestructura de seguridad la cual nos permite asegurar nuestra información

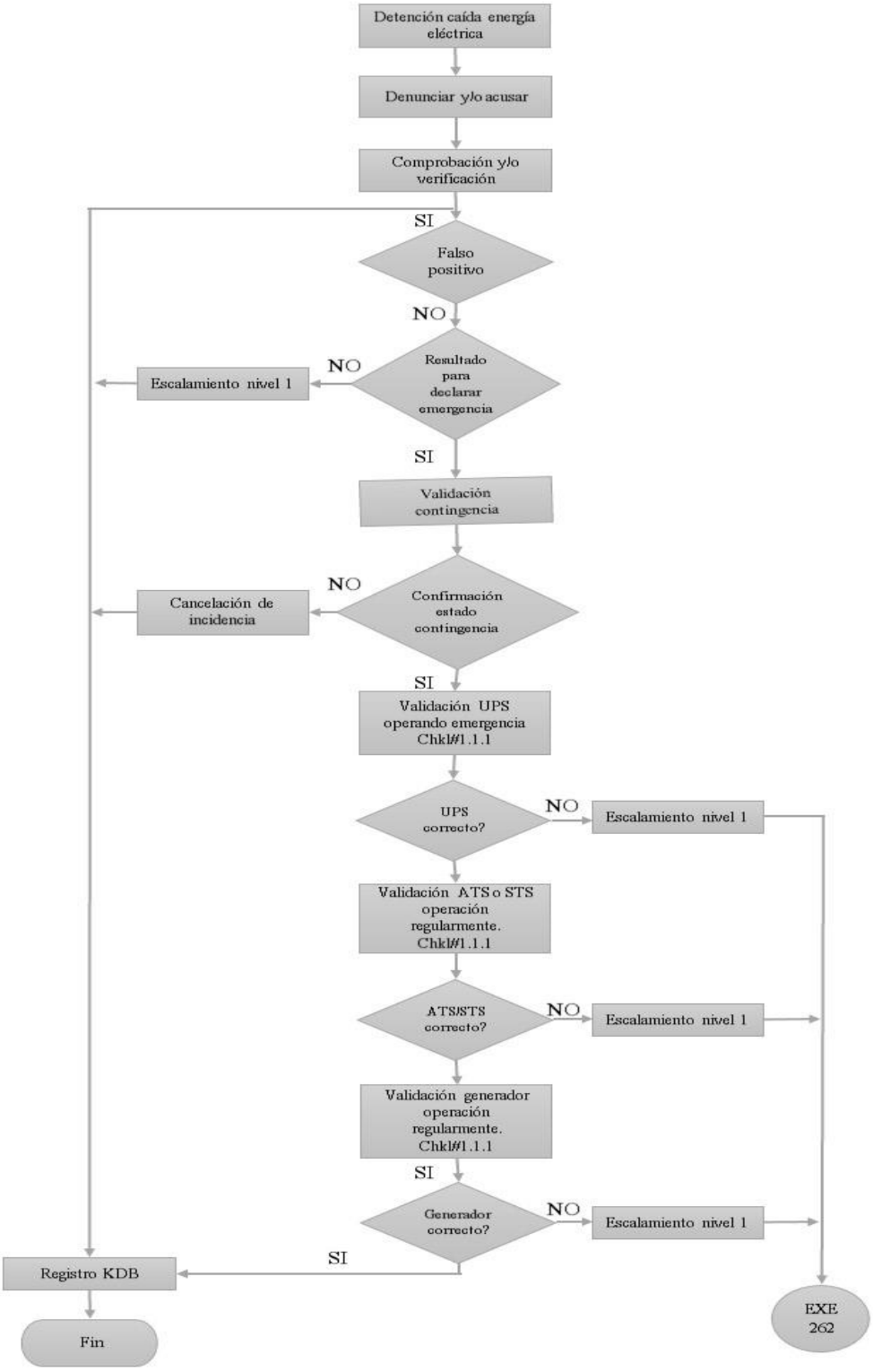
4. ¿Han tenido alguna eventualidad que haya provocado la salida de sus servicios?

   En los últimos 4 años solo hemos tenido una sola salida de servicio, el mismo se debió a la mudanza o traslado de localidad de nuestro datacenter. El mismo fue un evento programado y coordinado con nuestros clientes y que solo nos llevó 12 horas de salida en el servicio

5. ¿Cuentan con un Plan de Recuperación de Desastres que permita la recuperación en un tiempo mínimo?

   Si la OPTIC cuenta con un plan de recuperación de desastres que permite tener un respaldo offline de todos sus sistemas, lo que actualmente no es posible lograr la recuperación en corto tiempo ya que debido al tamaño de nuestra infraestructura necesitaríamos contar con una réplica casi exacta de los mismo para que la recuperación sea en corto tiempo.

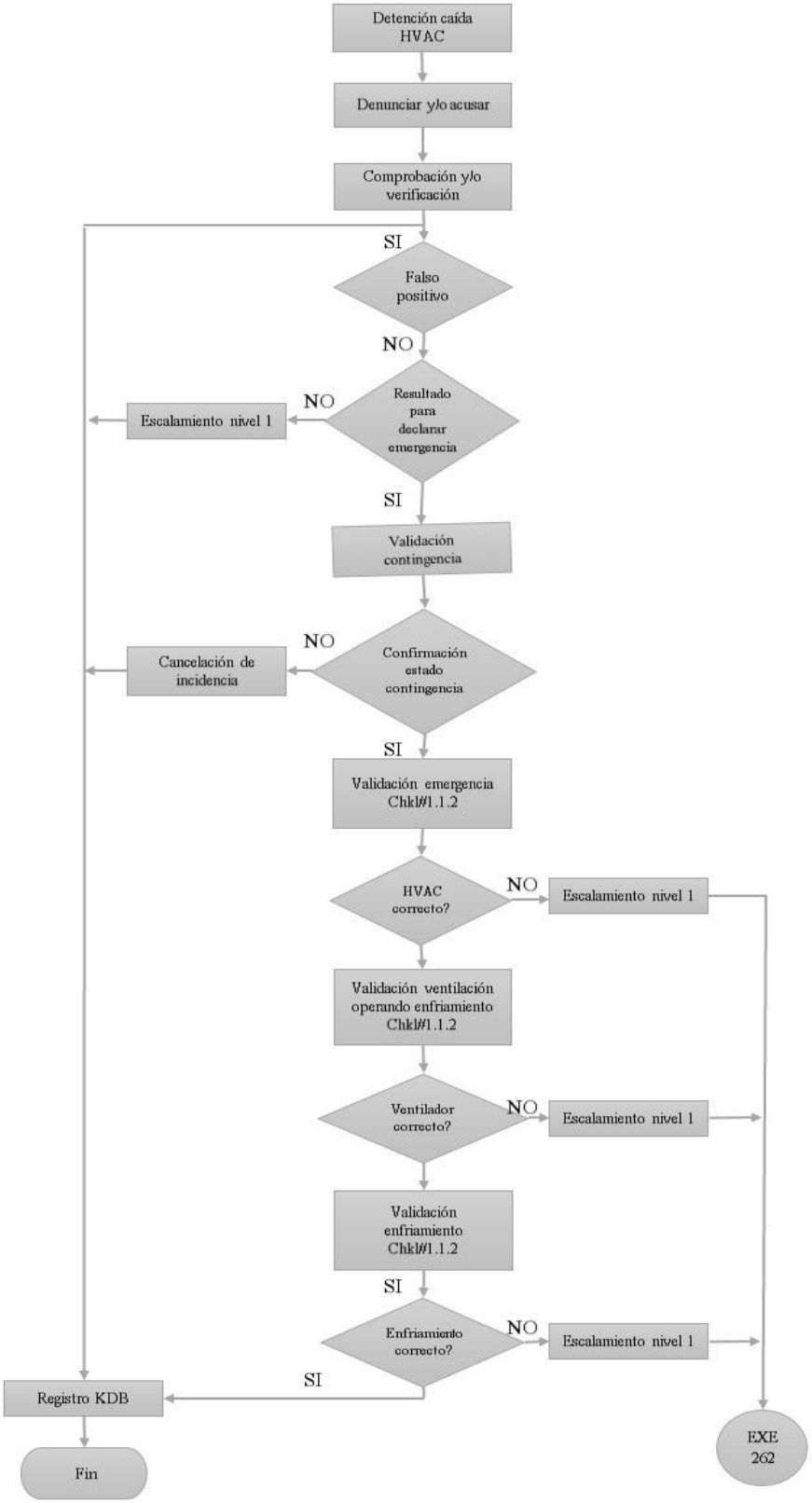
Anexo 2. Procedimiento de la OPTIC Caída Energía Eléctrica



Anexo 2. Caída de energía eléctrica.

Fuente los autores

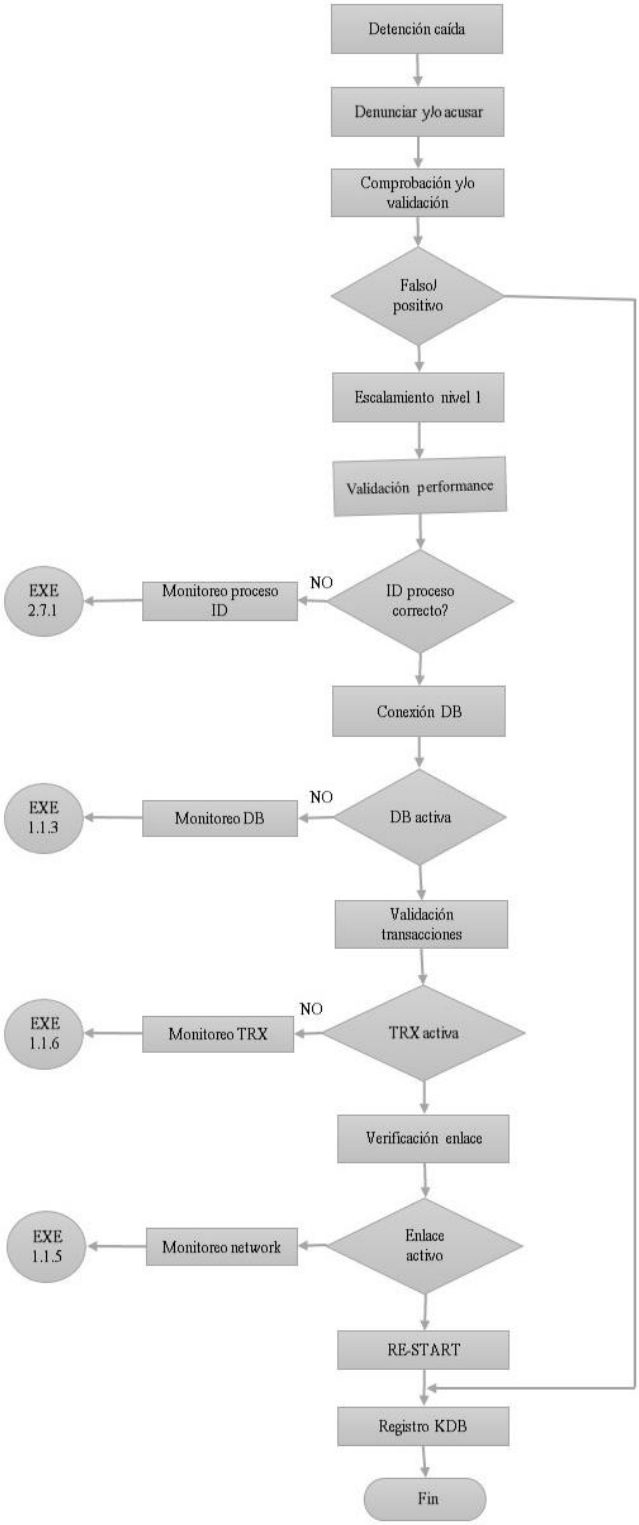
Anexo 3. Procedimiento de la OPTIC Caída HVAC (Climatización)



Anexo 3. Detención caída HVAC

Fuente los autores

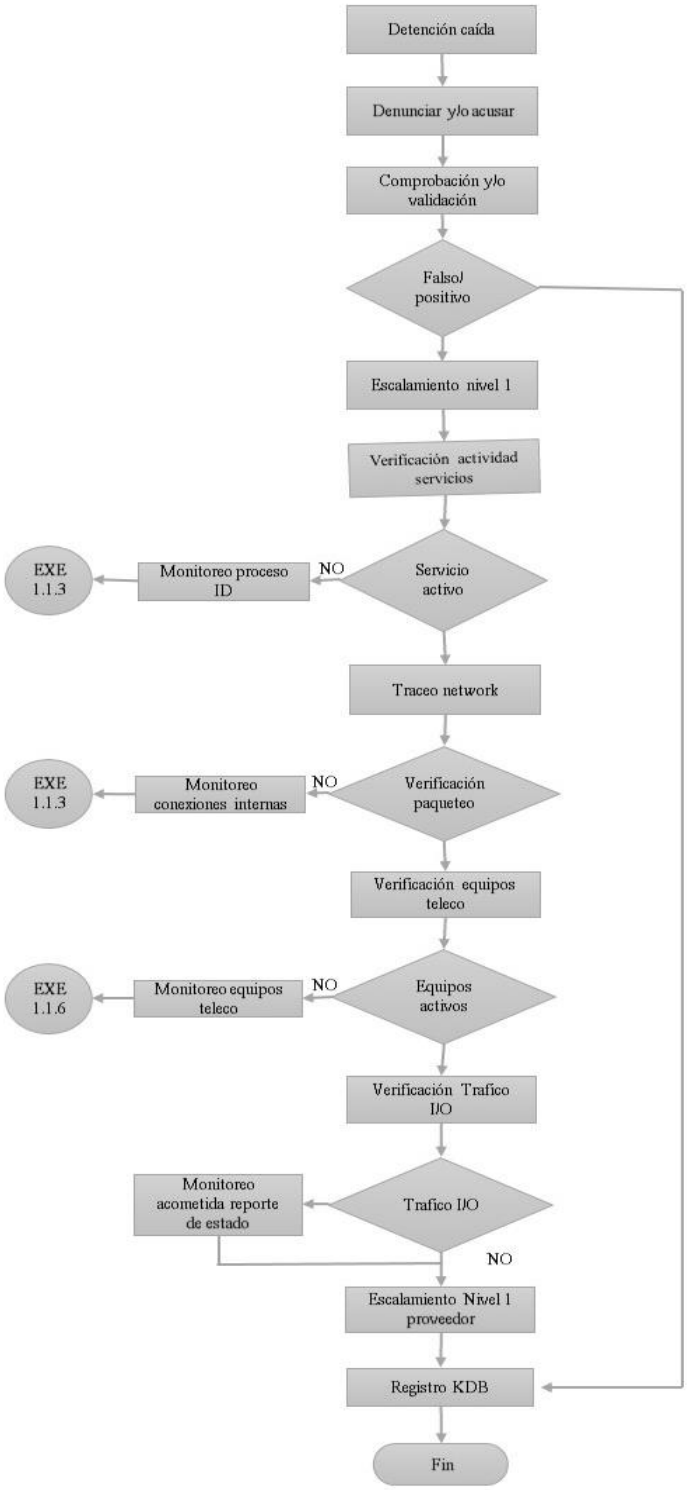
Anexo 4. Procedimiento de la OPTIC Caída Energía Eléctrica



Anexo 4. Detención de caída eléctrica

Fuente los autores

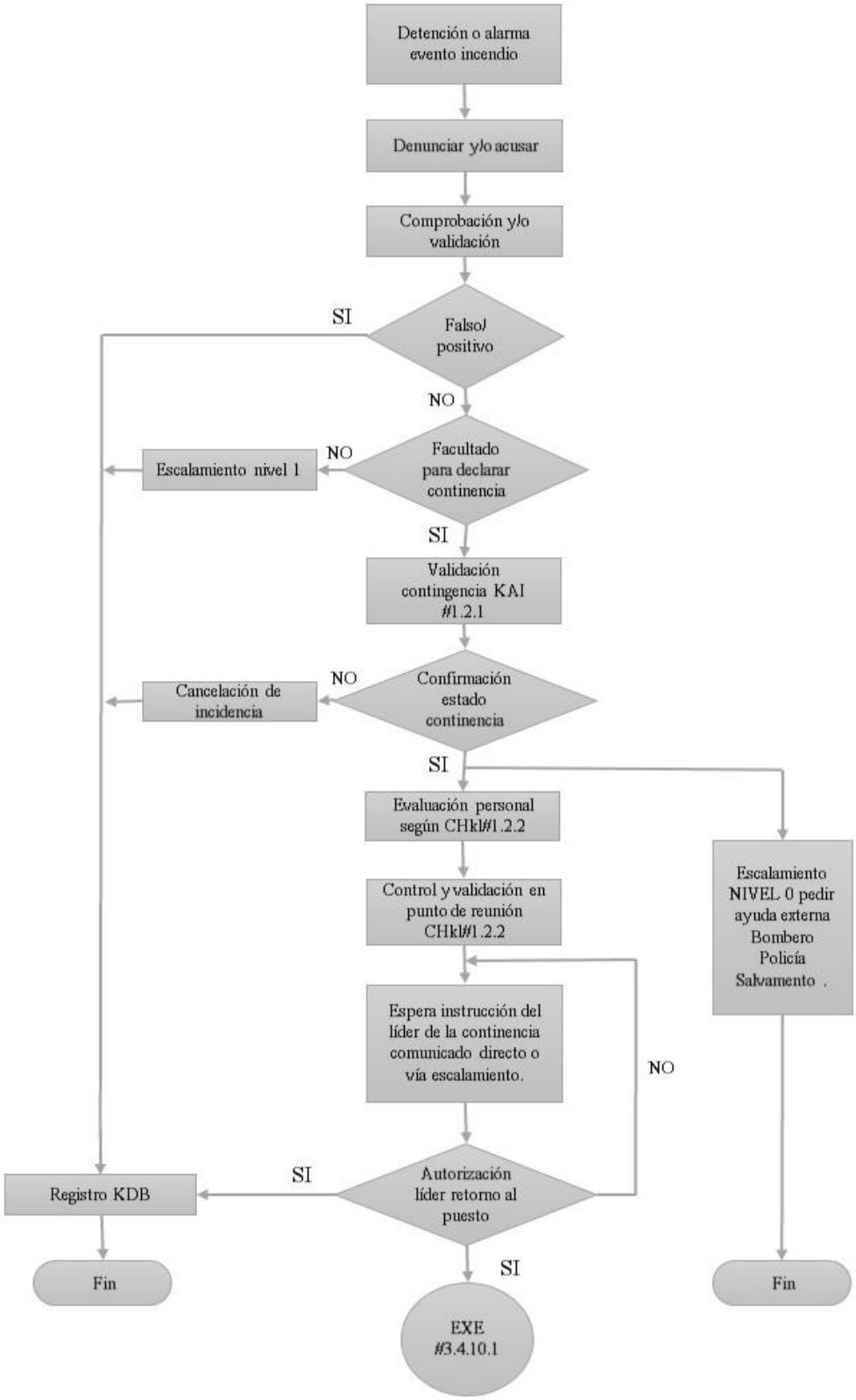
Anexo 5. Procedimiento de la OPTIC Caída de Red



Anexo 5. Caída de la red

Fuente los autores

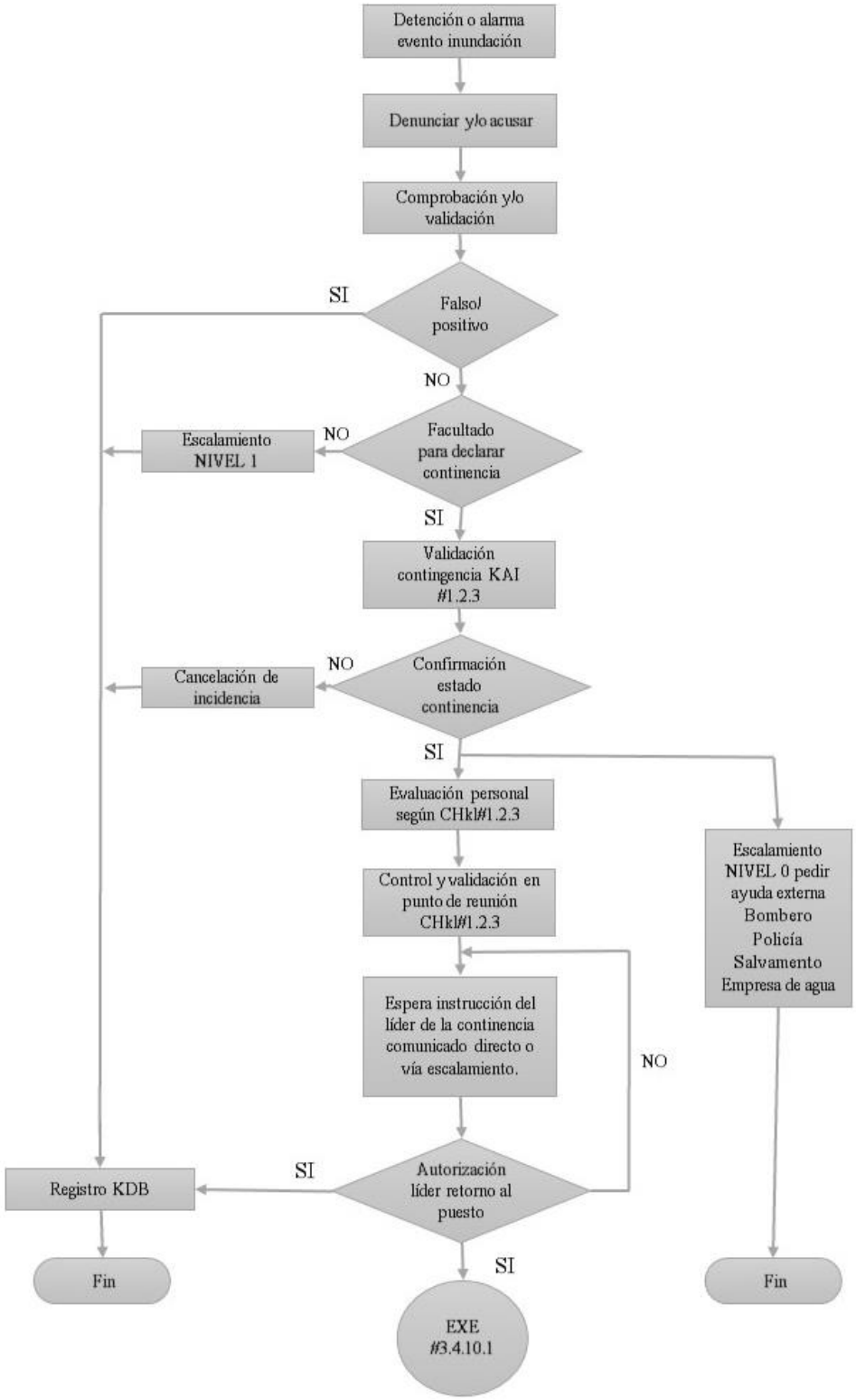
Anexo 6. Procedimiento de la OPTIC Detección de Incendio



Anexo 6. Detención de incendio

Fuente los autores

Anexo 7. Procedimiento de la OPTIC Detección de Inundación



Anexo 7. Detención de inundación

Fuente los autores

Anexo 8. Anteproyecto análisis e implementación de un sistema de recuperación de desastre para la oficina presidencial de tecnologías de la información y comunicación (OPTIC) utilizando el cloud computing (nube), en la ciudad de santo domingo durante el periodo septiembre diciembre del 2016.

DECANATO DE INGENIERIAS E INFORMATICA

Anteproyecto de Tesis

Tema:

Análisis e implementación de un sistema de recuperación de desastre para la oficina presidencial de tecnologías de la información y comunicación (OPTIC) utilizando el cloud computing (nube), en la ciudad de santo domingo durante el periodo septiembre diciembre del 2016.

Sustentantes:

Yaritza Pamela Moreta Rodriguez 2012-2259

Ledy Gissel Gómez Rodríguez 2011-1929

Edwin Alexander Sánchez Vásquez 2013-1827

Asesor

Freddy Jiménez

Fecha

30 de Junio de 2016

Santo Domingo, Rep. Dom.

Índice

Tema

Análisis e implementación de un sistema de recuperación de desastre para la oficina presidencial de tecnologías de la información y comunicación (OPTIC) utilizando el Cloud Computing (Nube) en la ciudad de santo domingo durante el periodo Septiembre Diciembre del 2016.

Introducción

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) es la responsable de planificar, dirigir y ejecutar las acciones necesarias para implementar el Gobierno Electrónico en el país mediante la difusión y uso de las Tecnologías de la Información y Comunicación (TIC).

La información se ha convertido en el activo más importante de las organizaciones de hoy en día, por lo cual es necesario asegurar la integridad, confidencialidad y disponibilidad de la misma. Por lo cual se hace necesario el uso de las TIC con el objetivo de poder administrar de forma correcta la información.

Actualmente la OPTIC brinda múltiples servicios de forma interna a sus usuarios, también de forma externa a diferentes instituciones del estado como también a los ciudadanos. Dentro de los servicios que ofrece se encuentra alojamiento de correos, alojamiento de páginas web, alojamiento de aplicaciones, atención ciudadana vía telefónica, entre otros.

La OPTIC no posee actualmente un plan de recuperación de desastres que permita mantener sus servicios activos ante una eventualidad. Un plan de recuperación de desastres es un conjunto de procesos y mecanismos que permiten mantener la disponibilidad de los servicios ante cualquier desastre que se presente.

Esta investigación se plantea buscar la solución al problema planteado con el fin de que la OPTIC pueda obtener un mayor nivel de garantía de sus servicios. Además, se busca disminuir el tiempo de recuperación de las operaciones ante cualquier eventualidad.

Justificación e Importancia

República Dominica es un país que posee 48311 kilómetros cuadrados de la Isla la Española. Como parte de una isla se encuentra vulnerable ante eventos naturales que pueden presentarse de forma inesperada, como pueden ser Huracanes, Tormentas, Maremotos, entre otros.

Además de los riesgos propios de una isla se la añade el hecho de que se encuentra ubicada sobre varias fallas geológicas activas que han provocado y pueden provocar movimientos sísmicos causando a su vez temblores de tierra.

Existen antecedentes de este tipo de desastres que han provocado grandes danos de infraestructura a la nación, como el terremoto ocurrido en 1946 el cual tuvo una magnitud de 8.0 en la escala de Richter, otro caso fue el huracán David de categoría 5 que causo danos en alrededor de 1540 millones de dólares.

Un hecho reciente ocurrido en enero de 2010, fue el terremoto ocurrido en la vecina República de Haití. Todo el registro civil e inmobiliario desapareció durante el sismo perdiendo la información de toda la nación, debido a que no contaban con un plan de recuperación de desastres.

Delimitación del problema

La actividad fundamental en la OPTIC es la implementación del gobierno electrónico en la Republica Dominicana, con el fin de fomentar el crecimiento tanto económico como tecnológico, a través de lineamientos, políticas y estrategias que permiten promover y desarrollar nuevas tecnologías, para determinar el diseño y la planificación de las acciones y sustentar la forma más práctica y de menor costo.

Como institución del estado se procederá a definir las variables y relevancia del problema de estudio, dividido de la siguiente manera:

Marco espacial

El planteamiento del problema y la investigación, se realizará en base a la Oficina Presidencial de Tecnologías de la Información y Comunicación en su localidad principal de Santo Domingo, Distrito Nacional.

Marco temporal

Esta investigación se delimita al periodo Agosto – Diciembre del 2016.

Marco poblacional

Para llevar a cabo el objetivo de la investigación sobre la OPTIC, se seleccionó la muestra no probabilística. Las personas seleccionadas procederán al proceso de entrevista, encuesta y observación, así lograr documentar las expectativas.

Planteamiento del Problema

Las organizaciones de hoy día buscan adaptarse al contexto actual, donde productividad, la competencia continua y la globalización han provocado una dependencia completa de las tecnologías de la información para sus operaciones cotidianas.

Por lo cual se hace vital contar con un plan de recuperación de desastres que permita no solo mantener la disponibilidad de la información, sino que además brinde continuidad de operaciones ante posibles situaciones críticas.

Este plan debe ser desarrollado acorde a los lineamientos estratégicos de la empresa con el fin de poder cumplir con los objetivos necesarios para mantener el funcionamiento de la misma.

La siguiente investigación busca indagar los riesgos de los sistemas, servicios, equipos de redes y aplicaciones. Para asegurarnos de cómo se ejecutaría el plan de recuperación de desastre, si se percibe una falla.

Descripción del Problema

Formulación del problema

¿Cuál es la razón por la que la Oficina Presidencial de Tecnologías de la Información y Comunicación no cuenta con un plan de recuperación de desastres que permita la continuidad tecnológica del negocio ante un desastre natural?

Sistematización del problema

¿Qué garantía tiene la OPTIC para mantener sus operaciones ante un evento inesperado?

¿Por qué necesita la OPTIC tener un plan de recuperación de desastres?

¿Cuál sería el impacto de no tener un plan de recuperación de desastres para la OPTIC, si sucede un evento que afecte sus operaciones?

Objetivos

Objetivos Generales

Analizar el plan de recuperación ante desastres de la Oficina Presidencial de Tecnologías de la Información y Comunicación(OPTIC), determinar e identificar las necesidades específicas con el fin de poder tomar las mejores medidas y prácticas que garantice la mejora continua de los procesos en el diseño y elaboración, así lograr minimizar el impacto.

Objetivos Específicos

1. Determinar las incidencias en el departamento de TI en la OPTIC.
2. Conocer la funcionalidad del plan de recuperación, personal involucrado, equipos alternativos, configuraciones y documentación existente.
3. Identificar las causas de interrupción de las operaciones de la institución.
4. Evaluar las vulnerabilidades existentes y determinar el riesgo e integridad de las informaciones de la empresa.

Marco de referencia

Marco teórico

Debido a la necesidad de mantener la continuidad en las operaciones, resulta primordial diseñar estrategias y políticas que permitan proteger y recuperar en el menor tiempo las operaciones ante desastres ya sean naturales o provocados por terceros, logrando poner en peligro los datos, el ciclo comercial o la reputación de la misma.

Un desastre puede definirse como: "cualquier causa que afecte la infraestructura ya sea natural, involuntaria, intencional e impida la continuidad del negocio" (Martínez, 2004) el cual limita el desarrollo de las operaciones a la vez de poner en riesgo los datos.

Unos minutos sin servicio, lograría no solo perdida de datos, sino que trae consigo mala reputación como en el caso de la empresa electrónica Japonesa Sony por la inundación que se produjo en Tailandia en noviembre de 2011 interrumpió la producción especialmente de las cámaras, lo cual implico la caída en los precios de los equipos en Estados Unidos y Europa con una perdida aproximada de 1,100 millones de dólares, reduciendo las ganancias en un 9% a 20 millones de aparatos, estimado a cuatro años de pérdidas. No obstante, dicho acontecimiento se situaba en la octava pérdida del mismo año, llevando a recortar el 90% de ganancia operativa. (Fernández, 2011).

Debido a la catástrofe y no disponer de un correcto y completo plan de recuperación de desastres con la capacidad de minimizar el impacto en las operaciones interrumpidas, intensificado pérdidas de clientes, operativa y monetaria donde solo se logró obtener 10% de las ganancias operativas en ese periodo.

Un desastre puede definirse como: "cualquier causa que afecte la infraestructura ya sea natural, involuntaria, intencional e impida la continuidad del negocio" (Martínez, 2004) el cual limita el desarrollo de las operaciones a la vez de poner en riesgo los datos, es decir, unos minutos de inactividad, lograría no solo perdida de datos, sino que trae consigo mala reputación como en el caso de la empresa electrónica Japonesa Sony que la inundación que se produjo en Tailandia en noviembre del 2011 interrumpió la

producción especialmente de las cámaras, lo cual implico la caída en los precios de los equipos en Estados Unidos y Europa con una perdida aproximada de 1,100 millones de dólares, reduciendo las ganancias en un 9% a 20 millones de aparatos, estimado a cuatro años de pérdidas. No obstante, dicho acontecimiento se situaba en la octava pérdida del mismo año, llevando a recortar el 90% de ganancia operativa. (Fernández, 2011). Debido a la catástrofe y no disponer de un correcto y completo plan de recuperación de desastres con la capacidad de minimizar el impacto en las operaciones interrumpidas, intensificado pérdidas de clientes, operativa y monetaria solo se logró obtener 10% de las ganancias operativas en ese periodo.

Un análisis más profundo aportado por IBM sobre el impacto económico de riesgos de TI en noviembre de 2015 "Una interrupción de 20 minutos pude costar a una organización de mediano tamaño más de un millón de dólares. Una interrupción importante, que dure en promedio siete horas, puede implicar costo por encima de los 14.2 millones" (IBM, 2015).

Actualmente las empresas se mantienen en constante cambios en la medida que la tecnología escala, mientras que la seguridad de los datos se encuentra más propensas amenazas, para ello las empresas se ven en la necesidad de invertir con el fin de mantener disponibilidad en el sistema, datos y aplicaciones, haciendo uso herramientas de análisis y automatización que asegure la continuidad en el funcionamiento del sistema mientras ocurre el incidente.

Ahora bien, ¿Qué plataforma seria vital para la recuperación ante desastres? La nube se posiciona como la ideal herramienta para almacenar los archivos e informaciones sin la necesidad de disponer de gran capacidad de almacenamiento, además de ofrecer las informaciones almacenadas en tiempo real, es decir, acceso cuando y donde quiera con un simple acceso a internet, quedando la responsabilidad para los proveedores de mantener la infraestructura.

El Cloud ha logrado en los últimos años convertirse en el negocio más productivo e importante para proporcionar servicios, como en el caso de Joyent el proveedor líder de servicios en la nube pública y privada, creada en el 2004, adquirida por la empresa surcoreana Samsung, líder en el mercado de Smartphone y dispositivos inteligentes. Con la alta tecnología de nube de Joyent, Samsung ahora tendrá acceso a su propia

plataforma en la nube capaz de dar soporte a la creciente línea de móviles, internet de las cosas, software y servicios basados en la nube" (Samsungs, 2016).

Por otro lado, Amazon Web Services (AWS) creada en el 2006, líder global en el comercio electrónico, ofreciendo gran variedad de artículos, a través de la plataforma comercial. AWS brinda la agilización de los servicios, permitiendo llegar y escalar de manera sostenible en el mercado, además de reducir los costos. La nube es el nuevo estándar para muchas empresas; es el nuevo “normal o común” en arquitecturas de cómputo. Oponerse al cloud computing es como luchar contra la ley de gravedad. (Carlson, 2016).

Lo anterior impone la búsqueda y aplicación de estándares y prácticas para un diseño estratégico focalizado en los puntos críticos para la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) que englobe la planificación, implementación y ejecución de paramentos que permitir recuperar y proteger la infraestructura tecnológica ante un eventual desastre.

Innovación

La OPTIC integrara una revaluación del plan de recuperación de desastres, además de puntualizar los riesgos en el servicio, equipos, aplicaciones y sistemas que al momento de ser afectados se logre obtener recuperación ágil, disminuir costos y satisfacer las necesidades de los clientes. Cabe destacar que posee el servicio de almacenamiento cloud lo que facilita la protección de servicios y tecnologías establecidas

Origen Histórico

Oficina Presidencial de Tecnologías de la Información y Comunicación: Origen e Historia.

En el año 2004, buscando modernizar el Estado, aumentar la competitividad del sector productivo y socializar el acceso a la información, el Gobierno Dominicano identificó la necesidad de contar con un organismo de alto nivel gubernamental, articulando iniciativas sectoriales en el sentido de manifestar en el país el uso de las tecnologías de la información y comunicación (TIC). Siendo de interés muy particular fomentar, desarrollar y diseñar proyectos, políticas y estrategias que tiendan a democratizar el uso, acceso y aplicación de las tecnologías de la información y comunicación (TIC), y reducir la brecha digital, el cual consiste en la diferencia de acceso al conocimiento, a la información y a las tecnologías de la información y comunicación (TIC) entre personas con mayores y menores recursos para subsistir.

En base a esto, se creó un organismo encargado de coordinar las iniciativas y proyectos de desarrollo, apoyándose en las tecnologías de información y comunicación (TIC) de manera armónica y articulada acorde a los planes generales y estratégicos trazados por el Poder Ejecutivo, de crear el ambiente necesario para la competitividad, eficientizar y transparentar el desempeño de la Administración Pública, así como de invertir en las áreas que propicien la participación de toda la ciudadanía. Sumado al interés como país de cumplir con los acuerdos suscritos con las Naciones Unidas para alcanzar los Objetivos del Milenio y erradicar la pobreza, y dar cumplimiento a acuerdos tales como la Declaración de Bávaro, la Declaración de Principios y el Plan de Acción de la Cumbre Mundial para la Sociedad de la Información en su primera fase, en Ginebra, diciembre 2003, y en su segunda fase el Compromiso y Programa de Acción celebrado en Túnez, noviembre 2005.

Estas necesidades motivaron que el día 3 de septiembre de 2004, mediante Decreto No. 1090-04, fuera creada la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), con dependencia directa del Poder Ejecutivo, autonomía financiera, estructural y funcional.

En el mismo orden este decreto adhiere a la OPTIC, las funciones del instituto Audiovisual de Informática (IADI), en la actualidad denominado Centro de Estudios de Tecnologías de la Información y Comunicación (CETIC) y de la Comisión Nacional de Informática (CNI), con la finalidad de integrar bajo un mismo seno las iniciativas de Tecnologías de la Información y Comunicación (TIC) y Gobierno Electrónico.

Además, mediante Decreto No. 212-05, se crea la Comisión Nacional de la Sociedad de la Información y Conocimiento (CNSIC), con la responsabilidad de elaborar, desarrollar y evaluar la Estrategia Nacional de la Sociedad de la Información, la formulación de políticas derivadas de dicha estrategia y la definición de iniciativas, programas y proyectos para su realización.

Otros Decretos han sido emitidos, No. 228-07 y No. 229-07, en miras de institucionalizar el desarrollo e implementación de la Agenda Nacional de Gobierno Electrónico. Estos Decretos establecen el Centro de Contacto Gubernamental y el instructivo de aplicación de Gobierno Electrónico respectivamente.

Visión

Ser la institución que impulse la transformación, el fortalecimiento institucional y la eficiencia del Estado, propiciando el desarrollo de la ciudadanía y del sector empresarial mediante el uso de las TIC.

Misión

Formular e implementar políticas, estrategias y controles que garanticen la mejora continua de los procesos, a través de las TIC en la administración pública, facilitando el acceso de los ciudadanos a los servicios del Estado.

Valores

- Transparencia
- Integridad
- Ética
- Compromiso
- Innovación
- Trabajo en Equipo
- Excelencia

Política Integrada de Gestión

Nos comprometemos a satisfacer las necesidades de nuestros clientes, mediante el cumplimiento de los requisitos legales y normativos aplicables, la mejora continua de nuestros procesos y servicios, con el fin de asegurar y mantener los sistemas de gestión de acuerdo a los estándares de calidad, seguridad de la información y los servicios de TI y así contribuir con la transformación del Estado Dominicano.

Nos proponemos garantizar a nuestros clientes, servicios:

- De excelencia
- Profesionales
- Eficientes
- Disponibles
- Seguros

Marco conceptual

- **Fenómeno Natural:** Hace referencia a los riesgos en sí mismos, como huracanes, maremotos, terremotos, sequias, ciclones, etc. (Hidalgo & Campins Eritja, 2000, p. 73)
- **Desastre Natural:** Hace referencia a las consecuencias o el impacto de este fenómeno sobre una comunidad dada, tanto en pérdidas de vidas humanas, como materiales, económicas y sociales. (Hidalgo & Campins Eritja, 2000, p. 73).
- **Nube Computacional:** La computación en nube es un sistema de computación paralela y distribuida que consiste en una colección de ordenadores interconectados y virtualizados que se aprovisionan de forma dinámica y se presenta como uno o más recursos de computación unificada basada en acuerdos de nivel de servicio (SLA) establecidos a través de la negociación entre el proveedor de servicios y consumidores. (Buyya, Yeo, & Venugopal, 2008, p. 2).
- **Respaldo:** Es una copia de seguridad es una copia de todos los datos que se pueden utilizar para restaurar los datos como y cuando sea necesario a su forma original. Es decir, una copia de seguridad es una copia válida de datos, archivos, aplicaciones o sistemas operativos que pueden ser utilizados para los fines de recuperación. (Guise, 2008, p. 2)
- **Conmutador (Switch):** Es un dispositivo que interconecta redes LAN con los mismos protocolos de nivel físico y de enlace del modelo OSI. Se utiliza para segmentar redes y aumentar sus prestaciones. Evita que colapse la red y por ello ha sustituido al hub, aunque no se use para crear subredes. Al ser un equipo activo, envía los paquetes al equipo destino concreto, ofreciéndole todo el ancho de banda en esas fracciones de segundos. (Gómez, 2011, p. 72) **.**
- **Cableado Estructurado:** Es tender cables de señal en un edificio de manera tal que cualquier servicio de voz, datos, vídeo, audio, tráfico de Internet, seguridad, control y monitoreo esté disponible desde y hacia cualquier roseta de conexión del edificio. Esto es posible distribuyendo cada servicio a través del edificio por medio de un cableado estructurado estándar con cables de cobre o fibra óptica.

Esta infraestructura es diseñada, o estructurada para maximizar la velocidad, eficiencia y seguridad de la red. (Rivas, 2013).

- **Enrutador (Router):** Estos dispositivos operan en la Capa 3 del modelo OSI y conectan subredes IP de la otra. Los routers se mueven paquetes a través de una red en un salto por salto a través de los diferentes dispositivos. (Southwick, Marschke, & Reynolds, 2011, p. 17).
- **Ethernet:** Estos dominios de difusión se conectan varios equipos host juntos en una infraestructura común. Hosts se comunican entre sí utilizando direcciones de Capa 2 medios de control de acceso (MAC). (Southwick, Marschke, & Reynolds, 2011, p. 17)
- **Servidor:** En la tecnología de la información, un servidor es un programa informático que proporciona servicios a otros programas de ordenador (y sus usuarios) en la misma u otras computadoras. (Rouse, 2014).
- **Virtualización:** es una tecnología de software que permite ejecutar varias máquinas virtuales en una única maquina física, compartiendo los recursos de ese ordenador único entre varios entornos. (Río, 2014)

Tipo de Investigación

Aspectos metodológicos de la investigación

En función de la naturaleza del problema en general se implementará el tipo de investigación explicativo, el cual consiente en conducir los criterios seleccionados en una sola dirección, ya sea físicos o sociales. La investigación explicativa conlleva de una amplia investigación de la mano de análisis e interpretación. Además de obtener nuevos resultados y elemento que pueden conducir a formular soluciones factibles, a través de las informaciones obtenidas.

Además de capturar los datos mediante los métodos metodológicos cuantitativos, ofrecerá una respuesta exhaustiva y concreta de los estudios realizados, mientras el

cualitativos, nos permitirá identificar los hechos y sucesos estadísticos ofreciendo una perspectiva holística, validando las investigaciones a través de los resultados obtenidos, generando teorías e hipótesis.

Para poder abarcar la investigación y lograr clasificar de acuerdo al grado de importancia que presente, así poder trabajar en las posibles soluciones, tomando en cuenta:

Población, empleados que conforman la empresa.

Muestra, selección de los empleados que permita realizar análisis y experimentación para determinar las características en general.

Tamaño de la muestra: para la construcción del estudio se tomará en cuenta 250 empleados.

Método de investigación

La recopilación de información se implementará técnicas e instrumento que faciliten la deducción de los resultados, tales como:

Entrevista: se realizará entrevista al personal de la OPTIC para obtener detalles más completos de las funciones y métodos implementados dentro de la institución.

Observación: se observará el desenvolvimiento del sistema de la OPTIC, capacitación de los empleados, con la idea de encontrar las soluciones factibles para suplir las necesidades.

Bibliografía

Arias, Á. (2015). *Computación en la Nube: 2ª Edición.* IT Campus Academy.

Buyya, R., Yeo, S. C., & Venugopal, S. (2008). *Market-Oriented Cloud Computing:Vision, Hype, and Reality for Delivering IT Services as Computing Utilities.* Obtenido de http://www.buyya.com/papers/hpcc2008_keynote_cloudcomputing.pdf

Carpenter, T. (2011). *Microsoft Windows Server Administration Essentials.* John Wiley & Sons.

Fernandez, A. (13 de 12 de 2011). *Expansion* . Obtenido de Expansion.com: http://www.expansion.com/accesible/2011/12/13/empresas/1323804371.html

Ferrill, P., & Ferrill, T. (2014). *Exam Ref 70-413 Designing and Implementing a Server Infrastructure.* Microsoft Press.

Gómez, J. A. (2011). *Redes Locales.* Editex.

Guise, P. d. (2008). *Enterprise Systems Backup and Recovery: A Corporate Insurance Policy.* Florida: CRC Press.

Hidalgo, J. R., & Campins Eritja, M. (2000). *De las catástrofes ambientales a la cotidianidad urbana: la gestión de la seguridad y el riesgo.* Barcelona: Edicions Universitat.

IBM. (18 de 11 de 2015). IBM abre Centro de Continuidad de Negocios en la Nube. MÉXICO , MÉXICO .

Martínez, J. G. (2004). *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones.* Madrid: Diaz de Santos, S. A.

Río, M. D. (2014). *Tecnologías de Virtualización.* IT Campus Academy.

Rivas, A. (7 de Enero de 2013). *Definición de un Sistema de Cableado Estructurado.* Obtenido de Next Solutions: http://www.nexxtsolutions.com/co/blog/2013/01/definicion-de-un-sistema-de-cableado-estructurado

Rouse, M. (June de 2014). *whatis.techtarget.com*. Obtenido de http://whatis.techtarget.com/definition/server

Southwick, P., Marschke, D., & Reynolds, H. (2011). *Junos Enterprise Routing: A Practical Guide to Junos Routing and Certification.* "O'Reilly Media, Inc.".

Viñals, J. T. (2011). *Empresas en la nube.* Libros de Cabecera.

Esquema preliminar de contenido de Trabajo de Grado

DEDICATORIAS

AGRADECIMIENTOS

INTRODUCCIÓN

RESUMEN

ASPECTOS METODOLÓGICOS

ÍNDICE DE FIGURASI

ÍNDICE DE TABLAS

Capítulo I

Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

Introducción

1.2 Valores

1.3 Política Integrada de Gestión

1.4 Organigrama

1.5 Descripción de Puestos

1.6 Servicios

1.7 Uso e implementación del Gobierno Electrónico

Conclusión

Capítulo II

Datacenter

Introducción

2.1 Concepto de Datacenter

2.2 Redes de Conexión Local

2.2.1 Redes LAN y WAN

2.2.2 Cableado Estructurado de la Red

2.2.3 Topologías en Red

2.3 Niveles de Redundancia

2.3.1 Infraestructura de Telecomunicaciones para Datacenter TIA/EIA-942

2.3.1.1 Niveles de Redundancia (TIER)

Capítulo V

Propuestas de un plan de recuperación de desastre para la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

Introducción

5.1 Situación Actual

5.2 FODA

5.3 Diagrama Actual de la OPTIC

5.4 Propuesta Nueva para la OPTIC

5.4.1 Diagrama de Infraestructura

5.8 Plan de Inversión

5.9 ROI

5.10 Cronograma de Actividades para el Proyecto

5.11 Beneficios de la Propuesta

CONCLUSIÓN

RECOMENDACIONES

BIBLIOGRAFIA

GLOSARIO

ANEXOS