DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES EN EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA FUNDACIÓN NEUMOLÓGICA COLOMBIANA

MARÍA ALEJANDRA CASTAÑO ORTEGÓN
CRISTHIAN CAMILO GARZÓN SÁNCHEZ

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
BOGOTÁ, D.C.
2015

DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES EN EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA FUNDACIÓN NEUMOLÓGICA COLOMBIANA

MARÍA ALEJANDRA CASTAÑO ORTEGÓN
CRISTHIAN CAMILO GARZÓN SÁNCHEZ

Proyecto de Grado para optar al título de Ingeniero de Sistemas

Augusto José Ángel Moreno
Director

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2015

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

Bogotá, 29 de Mayo de 2015

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE IMAGENES

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ADMINISTRACIÓN DE CRÍSIS: Proceso mediante el cual la organización administra el impacto del desastre, la cobertura adversa a medios de comunicación y mantenimiento continuo de información del avance del proceso de solución.

BISO: Business Information Security Officer (BISO) se especializa en temas de seguridad de la información relacionados con el negocio y que su objetivo es asegurar que la unidad de negocio o división entiende que la seguridad de la información es un requisito de negocio.

COBIT: guía para la administración, gestión y auditoria de los procesos de negocio relacionados con el manejo de la información. Definido por ISACA (Information Systems Audit and Control Association).

COPIA DE SEGURIDAD (BACKUP): duplicación de información en medios de almacenamiento alternos con el fin de que sea un medio de contingencia para recuperarla en caso de desastre.

DESASTRE: Un evento que afecta a un servicio o sistema de manera tal que es requerido un esfuerzo importante para restablecer el nivel original de operación y desempeño.

DRP: Proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

FACTORES DE RIESGO: es una condición del mundo real, en el cual hay una exposición a la adversidad conformada por una combinación de circunstancias del entorno donde hay posibilidad de pérdidas. Los riesgos informáticos son exposiciones tales como atentados y amenazas a los sistemas de información, la probabilidad de que una amenaza se materialice, utilizando la vulnerabilidad existente de un activo o grupos de activos, generadores pérdidas o daños.

FNC: Fundación Neumológica Colombiana

HISTORIAL: reporte del inicio y presente de un usuario especificando su movimiento en la fundación.

Noma ISO 20071: Norma internacional que se aplica específicamente a la gestión de tecnología de la información y en particular a la seguridad de la información.
PC: Procesos Críticos de los activos de la información.

PLAN DE CONTINGENCIA: es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas. El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de la Fundación, cuando alguna de sus funciones usuales se ve perjudicada por un factor interno o externo.

POLÍTICA: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

SAN: es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía.

SEGURIDAD DE LA INFORMACIÓN: Proceso continúo para salvaguardar la confidencialidad, integridad y disponibilidad de la información, al igual que las características de la información como la autenticidad.

SERVICIO: Cita programada para: neumología pediátrica, neumología adultos, estudios de sueño, los programas prestados de rehabilitación y pruebas de función pulmonar.

SISO: Strategic Information Security Officer (SISO) se especializa en la traducción de los requerimientos de negocio de alto nivel en las iniciativas de seguridad de la empresa y los programas que se deben implementar para lograr la misión, metas y objetivos de la organización.

TI: Tecnología de la Información

TISO: Technical Information Security Officer (TISO) se especializa en temas de seguridad de índole técnica, operaciones y monitoreo. La TISO también coordina y gestiona las políticas técnicas y actividades de control y evaluación.

USUARIO: Personal quien toma el servicio proporcionado por la fundación.

RESUMEN

La Fundación Neumológica Colombiana es una entidad de salud que busca ofrecer a los pacientes con enfermedades respiratorias un servicio de calidad y eficiencia, cuenta con un área de Tecnologías de la Información donde se suministran las herramientas necesarias para el buen funcionamiento del servicio prestado la paciente. En busca de mejoras continuas nace una necesidad para mantener los recursos tecnológicos protegidos ante cualquier eventualidad o desastre causado por factores externos o internos.

Se plantea el diseño del Plan de Recuperación de Desastres, el cual consta de una serie de fases basadas en el modelo internacional COBIT (Objetivos de Control para Información y Tecnologías Relacionadas), donde se describen los activos soportados por el área de Tecnologías de la Información, identificando los riesgos potenciales y las vulnerabilidades de los mismos. Posteriormente se realiza un estudio donde se evalúan los tiempos de recuperación en caso de un desastre y el impacto que genera la perdida de los servicios prestados al paciente.

Se proponen unos controles los cuales se describen por medio de las alternativas de recuperación, proponiendo diferentes escenarios para minimizar los tiempos ante una pérdida del servicio, planteados en diferentes costos donde se puede ajustar el presupuesto que disponga la Fundación Neumológica Colombiana y se ajuste a la solución adecuada. Para el estudio de levantamiento de información y el diseño del Plan se contó con permisos para el manejo de la información confidencial y procesos de la entidad, con asesoría del encargado del área de tecnología de la información y el director de proyecto de la universidad.

INTRODUCCIÓN

Actualmente en el sector Salud es imprescindible que se cuente con la capacidad para restablecer las operaciones de TI. Debido a que los riesgos asociados son muy altos y la alta dependencia en las tecnologías de información y de telecomunicaciones ha motivado la necesidad de contar con las medidas preventivas adecuadas y con un nivel de continuidad que les permita ejecutar sus procesos de negocio sin ningún tipo de pérdida o que la detención del servicio prestado sea mínima. Se torna necesario tener una prevención de las múltiples amenazas, garantizando principalmente, la preservación de tres características:

- Integridad: que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento.
- Confidencialidad: que la información sea accesible solo a las personas autorizadas.
- Disponibilidad: que los usuarios autorizados tengan acceso a la información y los recursos cuando lo necesiten.

IRAM/ISO/IEC17799 sostiene que "la seguridad de la información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al negocio y maximizar el retorno sobre las inversiones y las oportunidades", del mismo modo añade que "la seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software". Para alcanzar esto, se debe identificar los procesos y recursos críticos, entender los riesgos e impactos por interrupciones, definir estrategias y planes de recuperación, capacitar a las personas involucradas, realizar ejercicios de prueba y mantener actualizados los planes y procedimientos. [1] El plan de recuperación ante desastres es un mecanismo altamente contribuyente a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operatividad mínima luego de una contingencia, en la que se vean afectados los procesos y recursos informáticos que sostienen un negocio.

La Fundación Neumológica Colombiana (FNC) es una institución privada sin ánimo de lucro cuyos propósitos son la atención integral, continuada, humana y multidisciplinaria del enfermo respiratorio, la investigación y la docencia en el área de la Neumología. Este documento describe la planeación y el diseño del plan de recuperación de desastre a través de la medición de los factores de riesgos en la FNC, para con ello realizar un bosquejo donde se muestren las prioridades en el momento de recuperar, prevenir y proteger los activos en el área de TI ante un desastre.

[1] PLAN, D. R. (Copyright (c) 2009 DRP.com.). DISASTER RECOVERY PLAN. Recuperado el 13 de 03 de 2015, de http://drptopicosii.site90.com/introdrp.html

1. OBJETIVOS

1.1. GENERAL

Diseñar el plan de recuperación de desastres en el área de tecnologías de la información de la Fundación Neumológica Colombiana.

1.2. ESPECÍFICOS

- Levantar la información de los factores de riesgo de los activos de la información.
- Diseñar los tiempos de respaldo.
- Diseñar el tiempo de recuperación o recovery time objective RTO.
- Diseñar el punto de recuperación o recovery point objective RPO.
- Diseñar diferentes escenarios en una posible recuperación de desastres.
- Identificar las acciones del área de tecnologías de la información para mantener vigente el plan de recuperación de desastres.

2. MARCO CONCEPTUAL

2.1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA).

Identifica los procesos de negocio críticos que más afectan a los ingresos, activos y clientes para ayudarle a asignar prioridades a las estrategias de recuperación que puedan ser necesarias durante una interrupción prolongada de la actividad. Conocer cómo funciona la empresa - qué procesos deben estar interconectados y estar permanentemente disponibles para vender, producir y asistir a los clientes - es el objetivo más importante de un análisis de impacto de negocio[2].

Este proceso es parte fundamental dentro de la elaboración de un Plan de Recuperación de Desastres DRP. De acuerdo al Business Continuity Institute[3] se tienen cuatro objetivos principales al realizar un análisis de impacto:

- Entender los procesos críticos que soportan el servicio, la prioridad de cada uno de estos servicios y los tiempos estimados de recuperación (RTO).
- Determinar los tiempos máximos tolerables de interrupción (MTD).
- Apoyar el proceso de determinar las estrategias adecuadas de recuperación.

Críticos Funciones que pueden realizarse sólo si las capacidades se reemplazan por otras idénticas. No pueden reemplazarse por métodos manuales. Muy baja tolerancia a interrupciones.

Vitales Pueden realizarse manualmente por un periodo breve. Costo de interrupción un poco más bajos, sólo si son restaurados dentro de un tiempo determinado (5 o menos días, por ejemplo).

Sensitivos Funciones que pueden realizarse manualmente por un periodo prolongado a un costo tolerable. El proceso manual puede ser complicado y requeriría de personal adicional.

No Críticos Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

El análisis de impacto sobre el negocio, está basado en escenarios catastróficos que al darse su ocurrencia impactarían la infraestructura y procesos que soporta la realización de las operaciones y servicios de, lo que requerirá que el sistema posea unas estrategias de recuperación a corto, mediano y largo plazo, que

[2] Valero, N. (2009). RECUPERACION DE DESASTRES Y CONTINUIDAD DEL NEGOCIO. Universidad Externado de Colombia.
[3] (BCI) (s.f.). *Business Continuity Institute*. Obtenido de http://www.thebci.org/

garanticen su supervivencia por el periodo que duren las consecuencias del desastre.
Se puede concluir diciendo que las actividades normalmente relacionadas al desarrollo de un análisis de impacto sobre los servicios son: Procesos críticos del sistema. Dependencias. Impacto sobre las operaciones. Determinar los tiempos de recuperación óptimos para los procesos críticos. (BCI)

2.2. PLAN DE RECUPERACIÓN DE DESASTRES DRP.

Se requiere previamente realizar un Análisis de Impacto en el negocio (BIA) por lo que se describe a grandes rasgos dichos conceptos.

El Plan de Recuperación de Desastres (DRP), por su parte, es el plan que ejecuta Tecnologías de la Información de Comunicación (TIC) para recuperar los sistemas que gestiona.

Orientado a responder a eventos importantes, usualmente catastróficos que niegan el acceso a la facilidad normal por un período extendido. Frecuentemente, el DRP se refiere a un plan enfocado en TI diseñado para restaurar la operatividad del sistema, aplicación o facilidad de cómputo objetivo en un sitio alterno después de una emergencia. El alcance de un DRP puede solaparse con el de un Plan de Contingencia de TI; sin embargo, el DRP es más amplio en alcance y no cubre interrupciones menores que no requieren reubicación. (BCI)

No se debe dejar de lado este tipo de planeación, ya que la mayoría de las veces la información controlada a través de un servidor, ya sea de aplicaciones, de base de datos o web, es vital para la continuidad de un servicio dentro de la empresa o hacia los clientes.

Ante una catástrofe de cualquier índole, seguramente se afectará de manera negativa el desarrollo de las actividades normales de la empresa o institución, un DRP va a permitir una rápida recuperación del flujo de la información y por lo tanto un menor tiempo en la interrupción de los servicios que son provistos por el equipo que ha sufrido el daño.

La diferencia entre estar protegido con un Plan de Recuperación ante Desastres y no estarlo puede ir desde recuperar el servicio en 20 minutos (o menos) en caso de estar protegido o llegar hasta varios días en caso de no haberse preparado adecuadamente.[4]

Un DRP deberá contemplar siempre la peor de las situaciones, ya que de este modo, la contingencia podrá ser solventada en el menor tiempo posible.

[4] (PLAN, Copyright (c) 2009 DRP.com.), (ISACA, 2012), (Valero, 2009)

Un sitio de respaldo es vital, sin embargo es inútil sin un plan de recuperación de desastres. Un plan de recuperación de desastres indica cada faceta del proceso de recuperación, incluyendo (pero no limitado) a:

- Los eventos que denotan posibles desastres.
- Las personas en la organización que tienen la autoridad para declarar un desastre y por ende, colocar el plan en efecto.
- La secuencia de eventos necesaria para preparar el sitio de respaldo una vez que se ha declarado un desastre.
- Los papeles y responsabilidades de todo el personal clave con respecto a llevar a cabo el plan.
- Un inventario del hardware necesario y del software requerido para restaurar la producción.
- Un plan listando el personal a cubrir el sitio de respaldo, incluyendo un horario de rotación para soportar las operaciones continuas sin quemar a los miembros del equipo de desastres.
- La secuencia de eventos necesaria para mover las operaciones desde el sitio de respaldo al nuevo/restaurado centro de datos.

Las actividades a realizar en un DRP se pueden clasificar en tres etapas:

- Actividades Previas al Desastre. Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.
- Actividades Durante el Desastre. Una vez presentada la Contingencia o Siniestro.
- Actividades Después del Desastre.

Los procedimientos de un DRP deben de ser muy entendibles y estar documentados todos los cambios, este nivel de detalle es vital porque en el evento de una emergencia, el plan quizás sea lo único que quede de su centro de datos anterior para ayudarlo a reconstruir y restaurar las operaciones, además de ofrecer la ventaja de que cualquier persona lo pueda llevar a cabo. [5]

2.3. COBIT

COBIT es un marco de referencia aceptado internacionalmente que ha sido desarrollado para la aplicación de buenas prácticas en la administración de los procesos que hacen parte del área TI. COBIT permite alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para pedir

[5] (BCI) (PLAN, Copyright (c) 2009 DRP.com.)

los logros, e identificando las responsabilidades asociadas a los encargados de los procesos de negocio de TI. [6]

Los 34 procesos de TI de COBIT se encuentran organizados en los siguientes cuatro dominios:

- Planear y Organizar (PO): Este dominio apoya la identificación de los elementos que van a permitir que TI construya con el logro de las metas de la organización, para lo cual se plantean los siguientes cuestionamientos:

    - ¿Las estrategias de TI se encuentran alineadas con las de la organización
    - ¿La empresa esta optimizando el uso de los recursos?
    - ¿Se entienden y administran los riesgos de TI?
    - ¿La calidad de los sistemas de TI es apropiada para las necesidades del negocio?

- Adquirir e Implementar (AI): Mediante la aplicación de este dominio se identifican, desarrollan o adquieren los servicios de TI requeridos por la organización: además se provee el soporte o mejoramiento de los servicios ya existentes.

- Entregar y dar soporte (DS): Este dominio cubre la entrega por aparte de TI de los servicios requeridos y la continuidad de los mismos, así como la administración de la seguridad de la información (integridad, disponibilidad y confidencialidad). Este dominio satisface los siguientes cuestionamientos:

    - ¿Los servicios se están entregando de acuerdo con las prioridades del negocio?
    - ¿Los costos de TI se están optimizando?
    - ¿La fuerza de trabajo es capaz de utilizar los sistemas de información de manera productiva y segura?
    - ¿Están estipuladas de forma adecuada la confidencialidad, integridad y disponibilidad en los servicios de TI?

- Monitorear y evaluar (ME): Los procesos de TI deben cumplir con los objetivos propuestos, para ello se establece que estos serán evaluados de forma regular. Este dominio tiene en cuenta la administración del desempeño, la monitorización del control interno, el cumplimiento regulatorio y aplicación del gobierno de TI.

[6] ISACA. (2007). International Professional Association That Deals With ir Governance COBIT 4.1. Estados Unidos.

2.4. GESTIÓN DE RIESGOS

El riesgo como “La exposición a la posibilidad de ocurrencia de ciertas cosas tales como pérdida o ganancia económica, daño físico, retrasos, daño a la salud pública, etc. que surgen como consecuencia de seguir un curso particular de acción” .El concepto de riesgo tiene dos elementos, la probabilidad de que algo ocurra y las consecuencias de si esto ocurre.

“Para efectuar una efectiva y eficiente gestión del riesgo, es necesario considerar cual es la probabilidad de que un siniestro ocurra y cuáles serían las consecuencias que se podrían generar si una o todas las cosas que podrían suceder en realidad sucedieran. Es importante considerar que los riesgos pueden surgir tanto de fuentes internas como externas”. [7]

Los profesionales en Sistemas de Información y en general todos los miembros de una entidad deben reconocer que los riesgos podrían provocar la falla de un proyecto incidiendo en la falta de satisfacción por parte del cliente, desencadenando así una mala publicidad y una imagen poco optimista de la entidad. Algunos de los riesgos que más comúnmente se presentan son: la amenaza a la salud pública, dificultades en la administración y logística, fallas en los sistemas computacionales, fraudes y deficiencias en los controles internos entre otros. Dada la naturaleza de los riesgos, resultaría imposible tener un medio ambiente completamente libre de riesgos, aunque tomando ciertas medidas de control y prevención es posible menguar, reducir, o transferir ciertos riesgos.

[7] SCRIBD. Dirección general de unidades de negocio. Bogotá: La Empresa [citado 30 marzo, 2015]. Disponible en Internet: < http://es.scribd.com/doc/7132807/Gestion-Riesgos-Tecnologicos>

3. JUSTIFICACIÓN

Resulta prioritario para cualquier empresa tanto para su funcionamiento como para su proyección, mantener su información de manera segura, estable, accesible y siempre disponible. Alienada a la visión de la empresa, el área de Tecnología de la Información es el custodio de la información así como de su estabilidad y acceso.

Uno de los pilares del área de TI es mantener un respaldo de la información, esta actividad suele posponerse y considerarse como algo secundario; de hecho, tanto se suele posponer esta tarea que si se sufre un percance, es complicado recuperar la información importante, reestablecer los servicios críticos para el negocio, ya que por falta de planes y acciones, no existe la posibilidad de volverla a obtener y restablecerla en un tiempo corto para que no se afecte el negocio o cause gran impacto en el servicio.

Para la Fundación Neumológica Colombiana son muy importantes sus activos de la información al ser esta una entidad privada, sin ánimo de lucro y ubicada en el sector salud, cuyos propósitos son la atención integral, continuada, humana y multidisciplinaria del enfermo respiratorio, la investigación y la docencia en el área de la neumología, el departamento de TI debe priorizar el respaldo de estos activos de información, identificando los activos críticos en los servicios prestados más vulnerados por diferentes factores que son inherentes al área de tecnológica, como lo son los errores humanos, los desastres naturales o interrupciones prolongadas inesperadas, para así no afectar la atención de los pacientes que son tratados en las instalaciones de la empresa así como las diferentes actividades misionales de la misma, el paciente es la prioridad y núcleo de la FNC, por esta razón el área de TI debe contar con recursos y medios necesarios para reestablecer los servicios y activos críticos.

El departamento de TI cuenta con un plan de contingencia que está pensado para solucionar problemas en caso de que se presente un desastre, el cual fue desarrollado en el año 2009 cuando el área de tecnológica estaba tomando gran importancia en la misión y visión de la FNC debido al constante crecimiento de los pacientes tratados y de los empleados, esto implica un aumento de requerimientos tecnológicos para suplir las necesidades de los usuarios, pero este plan de contingencia solo tiene en cuenta los procesos de los servicios prestados y no estaban definidos los activos críticos de la información.

Pero al pasar el tiempo este plan de contingencia se ha quedado desactualizado y sus procesos han cambiado, no tiene una información actual y no cuenta con un análisis de riesgos donde se evalúe cada uno de sus activos de la información para darles prioridad a los más críticos, de manera general como por áreas.

Por el modelo de negocio de la FNC, está claro que la prioridad de TI es mantener la información del paciente pero además de eso debe mantener toda la información administrativa y su infraestructura de sistemas, teniendo en cuenta los reglamentos legales de retención de información para el sector de salud.

Con base a lo anterior surge la necesidad de buscar una solución más eficiente que el plan de contingencia que cumpla con la necesidad de la FNC en dar un servicio óptimo en caso de que se presente un desastre, teniendo en cuenta una actualización de los activos de la información que se tiene en TI y evaluando cada uno de los mismos, para con ello evaluar la criticidad e impacto en el negocio y en los procesos de TI.

En el presente documento se plantea un diseño del plan de recuperación de desastres DRP, la cual consta de un estudio y análisis sobre los activos y procesos de TI donde se plantean diferentes esquemas para ejecutar un DRP de manera eficiente y con tiempos óptimos donde la FNC no se va a tener afectaciones en los servicios por un tiempo muy prolongado y por ende el impacto del servicio prestado al paciente va a ser mínimo.

Durante el desarrollo del DRP se identifica una serie de riesgos humanos y naturales que no se habrían identificado en el plan de contingencia actual y que afectarían a la FNC en los diferentes procesos, en los cuales el plan vigente no tiene el alcance necesario para suplir las necesidades en caso de un desastre.

El DRP ofrece varios beneficios importantes que pueden generar procesos de recuperación en los servicios afectados, minimizando las pérdidas de información, tiempos prolongados y la seguridad de los datos, sin contar en los tiempos donde no se establezca el servicio puede incurrir en gastos adicionales y pérdidas financieras. Esta solución es una inversión a favor de la FNC, por que cubre con las necesidades de prestar el servicio cuando se presente un desastre.

4. INGENIERÍA DEL PROYECTO

4.1. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

En el sector Salud se ha vuelto una prioridad asegurar que todos los procesos del negocio estén siempre disponibles para los clientes, proveedores, y otras entidades. La FNC actualmente cuenta con un área de tecnología de la información como centro de información y gestión de recursos informáticos debiendo garantizar la protección de la información ante desastres catastróficos que pueden dañar la integridad, confidencialidad y disponibilidad de la información, se construye en el año 2010 un procedimiento de contingencia, donde se especifica cada una de los recursos tecnológicos del área de sistemas, sus posibles fallas y posibles soluciones, describiendo así las herramientas necesarias ante algún daño lógico o físico.

4.2. REQUERIMIENTOS DE LA INFORMACIÓN

Con base a la situación actual en el área de TI en la FNC, nacen nuevos requerimientos para realizar mejoras y garantizar la protección de la información, descritos a continuación:

- Mantener la información asequible
- Minimizar el impacto y perdidas ante un desastre
- Documentar el proceso de recuperación ante un desastre para el área de TI
- Mantener en funcionamiento los procesos críticos de TI
- Mantener la continuidad de la información
- Tener una alternativa de recuperación de los procesos críticos de TI ante un desastre.

4.3. MODELAMIENTO DEL SISTEMA

En el desarrollo de este documento se presenta el diseño del plan de recuperación de desastres, con base al estudio realizado de los activos de la información al nivel tecnológico, y de esta forma poder establecer unos posibles escenarios de recuperación en los procesos críticos identificados en el área de TI, como guía de toma de decisiones ante una situación de desastre, donde la FNC por medio de TI pueda mitigar o minimizar perdidas en tiempo y costos debido a la falta de disponibilidad de los activos de información.

5. METODOLOGÍA

El plan de recuperación desastres DRP en la Fundación Neumológica Colombiana FNC es diseñado con el fin de mantener la disponibilidad de los activos de información críticos de la empresa evitando así la posible pérdida financiera y operativa en un evento inesperado, previendo procedimientos de recuperación efectivos.

Para desarrollar lo anteriormente descrito se plantean distintas fases donde se describe los procesos a tener en cuenta.

5.1. DESARROLLO DE POLÍTICAS DRP

El departamento de TI de la FNC será responsable del desarrollo del Plan de Contingencia, definiendo todas las políticas y acciones a llevarse a cabo durante un evento de contingencia; también será responsable de que todas las actividades se cumplan de acuerdo a lo planeado.

En el Anexo 1 se describen las políticas propuestas para la ejecución del plan de recuperación de desastres DRP, al momento de presentarse una contingencia. (Anexo1.)

5.2. IMPACTO DE ANÁLISIS DEL SERVICIO BIA

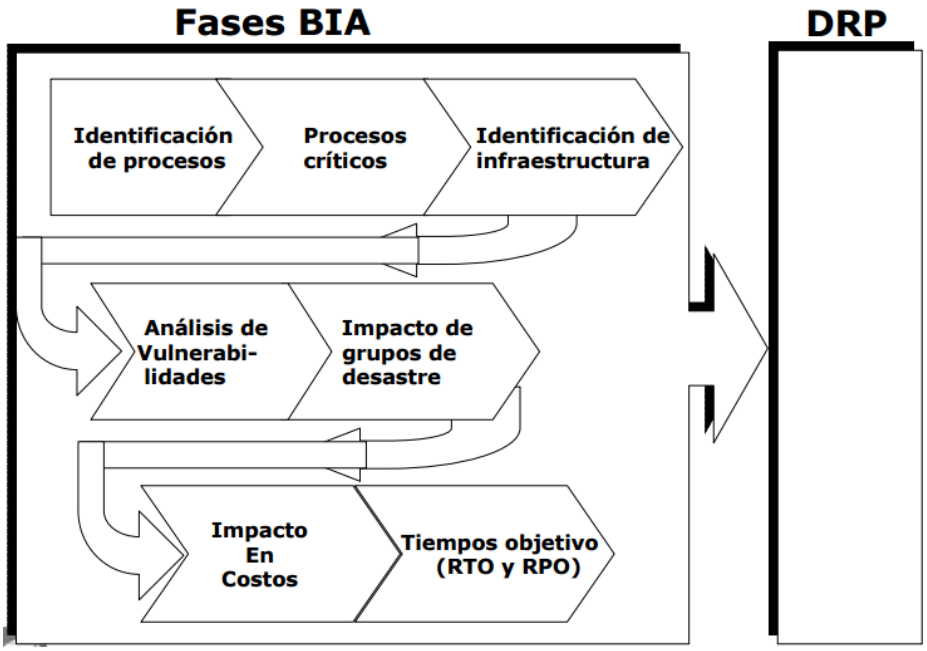
El Análisis de Impacto del Servicio BIA es una de las partes fundamentales en el plan de recuperación de desastres la cual permite identificar las áreas que sufrirán las pérdidas financieras y operacionales más grandes en caso de un desastre, la cual se identificaran a través de los procesos críticos.

Bajo la metodología COBIT el análisis BIA tiene una serie de fases que permiten identificar de manera clara y concisa los procesos críticos, los riesgos, las vulnerabilidades, el impacto y el tiempo estimado en que la FNC puede tolerar en caso de un desastre[8].

En la siguiente imagen, se ilustra las fases del análisis BIA que según COBIT se deben contemplar para el levantamiento de información correcto y con ello obtener los factores de riesgo e identificar los impactos los tiempos e impactos para el diseño del DRP:

[8] ISACA. (2007). International Professional Association That Deals With ir Governance COBIT 5. Estados Unidos.

Imagen 1. Fases de Análisis de Impacto al Negocio



Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

5.2.1. Identificación de Procesos

Durante la primera fase del BIA se identifican los procesos y herramientas por cada una de las áreas funcionales que comprende la FNC que son soportadas por el área de TI, se desglosa el proceso por hardware, software y también se tienen en cuenta que los procesos o actividades realizadas por cada una de las áreas tienen distintos pesos o valores para las mimas.

Al finalizar la elaboración del levantamiento e identificación de información se obtiene un total de 119 activos dentro de la FNC describiendo su función e importancia en cada una de las áreas. Para conocer detenidamente dichos activos se anexa el archivo Identificación de Procesos – Descripción del Activo en cada Proceso (Inventario de Activos) (Anexo 2).

En la FNC Las áreas funcionales se identifican por centros de costos y para identificarlos dentro de la identificación de procesos es necesario dar a conocer la denominación de cada uno. En la siguiente tabla se describe los centros de costos actuales para el año 2015:

Tabla 1. Áreas Funcionales por Centro de Costo

Centro de Costo	Área Funcional
ATPA	Atención al Paciente
COME	Comercial
COAD	Consulta Externa Adultos
COPE	Consulta Externa Pediatría
DIAD	Dirección Administrativa y Financiera
DIGE	Dirección General
DIME	Dirección medica
EDDO	Educación y docencia
INVE	Investigación
PRFP	Pruebas de función pulmonar
SUEÑ	Sueño
TEIN	Tecnologías de la Información
TERA	Terapia Respiratoria

Fuente: Fundación Neumológica Colombiana FNC. Centros de Costos FNC. 2015

5.2.2. Procesos Críticos.

Con base a la evaluación anteriormente descrita, se procede a realizar un estudio para identificar los procesos críticos de los 119 activos de la información de acuerdo a la confidencialidad, integridad y disponibilidad cuyos volares e impactos sean altos. Identificación de Procesos – Descripción del Activo en cada Proceso (Matriz de Riesgos PC) (Anexo 3).

Áreas con procesos más críticos dentro de la FNC:

- Dirección Medica
- Dirección Administrativa
- Educación y Docencia
- Investigación
- Tecnologías de la información
- Facturación
- Atención al Paciente

5.2.3. Identificación de Infraestructura.

Dentro la infraestructura tecnológica de la FNC existen diferentes herramientas para el funcionamiento de los procesos ejecutados dentro de cada una de las áreas. Los siguientes sistemas de información serán incluidos en el proceso de implementación DRP, Esquema de Red e Infraestructura FNC (Anexo 4).[9]

- Servinte Clinical Suite
- Alejus
- Gmail
- Novasoft
- SQL Server 2005
- SQL Server 2014
- Digiturno IT
- FoxPro
- G3
- Alice
- Somnomedics
- VMax
- Medgraphics
- NDD
- Medicap
- Documentos de cálculo con bases de datos y estadísticas.

El departamento de TI soporta los siguientes sistemas operativos:

- Windows 2003 Server
- Windows XP
- Windows 7
- Windows 8
- Windows 2008 Server
- Windows 2012 Server
- Linux Smoothwall
- VMWare ESXi 5.1
- Avaya

La red de datos de la Fundación Neumológica Colombiana está compuesta por:

- 59 Computadores de escritorio
- 18 Laptops
- 75 Clientes Livianos
- 77 Teléfonos IP

[9] Tomado del área de TI de la Fundación Neumológica Colombiana FNC

- 30 Impresoras
- 9 VMax (Equipo PFP)
- 18 Alice (Equipo Sueño)
- 13 Cámaras
- 8 Access Point
- 6 Servidores Físicos
  - 2 ESXI
  - 2 Terminal Server
  - 1 Firewall
  - 1 VCenter
- 1 SAN
- 1 Robot de cintas
- 12 Servidores Lógicos
  - 4 Bases de datos
  - 1 Desarrollo
  - 1 Aplicativo Historias Clínicas
  - 2 Terminal Server
  - 2 Controladores Dominio
  - 1 Aplicaciones Anti virus / Consola Avaya / Digiturno
  - 1 Servidor DFS e Impresión
- 11 Switches
  - 2 Core
  - 7 Acceso
  - 2 Cluster servidores ESXI
- 2 Modem ADSL
- 1 Planta telefónica
- 321 Puntos de red
  - 225 Datos
  - 96 Voz
- 2 UPS

5.2.4. Análisis de Vulnerabilidades.

A través del Análisis de Vulnerabilidades se realiza un estudio de acuerdo a la descripción de cada activo y la importancia del proceso detectando las principales vulnerabilidades de la Infraestructura donde intervienen la Tecnología de Información clasificadas de acuerdo al riesgo que representa.

Posteriormente se identifican las vulnerabilidades y se realiza un análisis para identificar la probabilidad y el impacto de posibles amenazas. En la siguiente tabla se describe los valores considerados para evaluar la Probabilidad de Amenaza que puede tener cada activo.

Tabla 2. Valores de Probabilidad de Amenaza

PROBABILIDAD		
NIVEL	RANGO	DESCRIPCIÓN
5	Probable	Puede que suceda en todas las circunstancias
4	Muy probable	Puede suceder en la mayoría de veces
3	Moderada	Puede ocurrir
2	Improbable	Puede ocurrir algunas veces
1	Rara	Puede pasar bajo características especificas

Fuente: Identificación de Procesos – Descripción del Activo en cada Proceso (Referencias de Datos). 2015.

En la tabla siguiente se describe los valores considerados para identificar el Impacto de Amenaza que puede tener cada activo.

Tabla 3. Valores de Impacto de Amenaza

IMPACTO		
NIVEL	RANGO	DESCRIPCIÓN
5	Catastrófico	Perdidas Enormes
4	Mayor	Perdidas mayores
3	Moderado	Perdidas medias
2	Menor	Perdidas bajas
1	Insignificante	Perdidas mínimas

Fuente: Identificación de Procesos – Descripción del Activo en cada Proceso (Vulnerabilidades PC) (Anexo 3).

5.2.5. Tiempos Objetivo (RTO y RPO)

El Tiempo de recuperación de las actividades que se han identificado bajo unas condiciones mínimas aceptables para el funcionamiento de los activos en la FNC. Para el punto objetivo de recuperación RPO, la FNC cuenta con diferentes métodos de backup que se realizan a los activos de la información a nivel de hardware y software:

- Bakups de Software: Este se ejecuta en horas de la noche según la tarea programada, la información es extraída de los discos duros de la SAN y es llevada a las cintas de almacenamiento para ser organizada por el robot de cintas dispuesto para este fin.

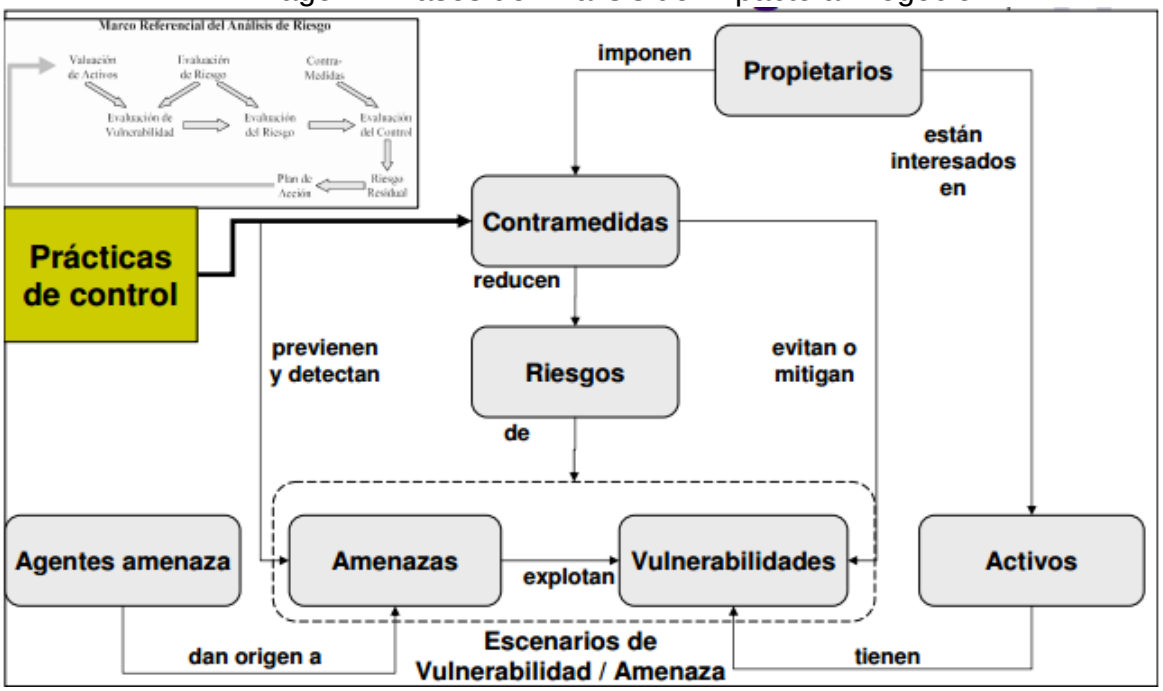
- Backups de Hardware: Para toda la parte de hardware se tiene como respaldo los acuerdos de nivel de servicio que la FNC tiene con los proveedores.

El estudio realizado se muestra detalladamente en el archivo de Identificación de Procesos – Descripción del Activo en cada Proceso (RPO y RTO PC) (Anexo 5).

5.3. EVALUACIÓN DE RIESGOS

En la evaluación de riesgos se identifican los elementos que integran los subprocesos de cada uno de los activos críticos identificados en el BIA, como se ilustra en la Imagen 2 se puede observar las fases y el proceso como modelo:

Imagen 2. Fases de Análisis de Impacto al Negocio



Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

5.3.1. Riesgos Potenciales

Dentro de la FNC se identificaron diferentes riesgos potenciales clasificados en los diferentes recursos de los activo identificados en el BIA. En la Matriz de Análisis de Riesgo desarrollada se miden los riesgos con las posibles amenazas y la probabilidad de ocurrencia

En la Tabla 4 se describen los riesgos encontrados y su calificación:

Tabla 4. Riesgos Potenciales – Identificación de Procesos – Descripción de los Activos en cada Proceso *(FNC)*

Actos originados por la criminalidad común y motivación política	**Sucesos de origen físico y Naturales**	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**
Allanamiento (ilegal, legal)	Incendio	Falta de inducción, capacitación y sensibilización sobre riesgos
Sabotaje (ataque físico y electrónico)	Inundación / deslave	Mal manejo de sistemas y herramientas
Daños por vandalismo	Sismo	Utilización de programas no autorizados / software 'pirateado'
Fraude / Estafa	Polvo	Falta de pruebas de software nuevo con datos productivos
Robo / Hurto (físico)	Falta de ventilación	Perdida de datos
Robo / Hurto de información electrónica	Electromagnetismo	Infección de sistemas a través de unidades portables sin escaneo
Intrusión a Red interna	Sobrecarga eléctrica	Transmisión no cifrada de datos críticos
Infiltración	Falla de corriente (apagones)	Manejo inadecuado de contraseñas (inseguras, no cambiar, BD centralizada, compartidas, acceso a terceros)
Virus / Ejecución no autorizado de programas	Falla de sistema / Daño disco duro	Exposición o extravío de equipo, unidades de almacenamiento, etc
Violación a derechos de autor		Sobrepasar autoridades

Tabla 4. Continuación

Actos originados por la criminalidad común y motivación política	Sucesos de origen físico y Naturales	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
		Falta de mantenimiento físico (proceso, repuestos e insumos)
		Falta de actualización de software (proceso y recursos)
		Fallas en permisos de usuarios (acceso a archivos)
		Acceso electrónico no autorizado a sistemas externos
		Acceso electrónico no autorizado a sistemas internos
		Red cableada expuesta para el acceso no autorizado
		Red inalámbrica expuesta al acceso no autorizado
		Dependencia a servicio técnico externo
		Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos y las políticas de seguridad descritas por TI)
		Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control (descritos por TI)
		Ausencia de documentación

Fuente: Identificación de Procesos – Descripción del Activo en cada Proceso (Matriz Riesgos PC). 2015.

En cada uno de los riesgos que se evaluaron según su clasificación y peso se dieron unos valores para la calificación de los umbrales de riesgo como se muestra en la Tabla 5.

Tabla 5. Cuantificación de los Riesgos – Identificación de Procesos – Descripción de los Activos en cada Proceso (FNC)

Umbral Bajo Riesgo	Umbral Medio Riesgo	Umbral Alto Riesgo
	10	20
x	y	y
1.0	11.0	21.0
2.0	12.0	22.0
3.0	13.0	23.0
4.0	14.0	24.0
5.0	15.0	25.0
6.0	16.0	
7.0	17.0	
8.0	18.0	
9.0	19.0	
10.0		

Fuente: Identificación de Procesos – Descripción del Activo en cada Proceso (Referencias de Datos). 2015.

5.3.2. Amenazas, Vulnerabilidades y Controles.

Una vez identificadas las amenazas y vulnerabilidades se procede a generar los controles donde se puede evaluar si se pueden eliminar, mitigar o aceptar estas amenazas y vulnerabilidades; estos posibles controles se describen bajo el análisis TISO/BISO que se realizó a cada uno de los 119 activos de la información en el archivo Identificación de Procesos – Descripción del Activo en cada Proceso (Inventario de Activos) (Anexo 2).

5.3.3. Elementos de Continuidad y Contingencia

Los elementos de contingencia están descritos en la actualización y restructuración que se realizó a partir de los activos de la información críticos que se encontraron en el archivo de Procedimientos de contingencia v4 (Anexo 6) (FNC).

5.4. DESARROLLO DE ESTRATEGIAS DE RECUPERACIÓN

Existen diferentes alternativas de recuperación donde la estrategia apropiada es la que tiene un costo para un tiempo aceptable de recuperación que también es

razonable con el impacto y la probabilidad de ocurrencia. Las acciones más efectivas serían:

- Eliminar la amenaza completamente.
- Minimizar la probabilidad y el efecto de la ocurrencia.

Una estrategia de recuperación es una combinación de medidas preventivas, detectivas y correctivas. La selección de una estrategia de recuperación depende de:

- La criticidad del proceso del negocio y las aplicaciones que soportan los procesos.
- Costo.
- El tiempo requerido para recuperarse.
- Seguridad.

En general, cada plataforma TI en la que corra una aplicación que soporte una función crítica del negocio necesitará una estrategia de recuperación.

5.4.1. Alternativas de Recuperación

Las interrupciones más prolongadas y más costosas, en particular los desastres que afectan la instalación física primaria de la FNC, requieren alternativas de recuperación en un sitio distinto a la ubicación primaria (offsite). Los tipos de instalaciones de respaldo de hardware en sitio alternativo que existen son[10]:

Mirror sites: es un sitio alterno que contiene una réplica exacta de otro. Estas réplicas u espejos se suelen crear para facilitar descargas grandes y facilitar el acceso a la información aun cuando haya fallos en el servicio del servidor principal.

Los espejos suelen sincronizarse periódicamente con el servidor principal para mantener la integridad de la información. En el caso de las redes, mirror también hace referencia al modo en el que trabaja un switch, al hacer réplica de todos los paquetes que este conmuta direccionados a un solo puerto a través del cual, con un analizador de tráfico, se puede observar todo el tráfico de la red.

Hot Sites: Se configuran totalmente y están listos para operar dentro de varias horas. El equipo, red y software del sistema deben ser compatibles con la instalación que está siendo respaldada. Las únicas necesidades adicionales son personal, programas, archivos de datos y documentación.

[10] (PLAN, Copyright (c) 2009 DRP.com.), (ISACA, 2012), (Valero, 2009)

Los costos asociados con el uso de un hot site de terceros por lo general son elevados, pero más bajos que crear un sitio redundante y con frecuencia son costos justificables para aplicaciones críticas. El hot site está destinado para operaciones de emergencia durante un período limitado de tiempo y no para uso prolongado.

Warm sites: Están en parte configurados, por lo general con conexiones de red y equipo periférico seleccionado, como por ejemplo, unidades de discos y otros controladores, pero sin la computadora principal. Algunas veces un warm site está equipado con una CPU menos potente que la que se usa generalmente. El supuesto detrás del concepto warm site es que la computadora puede por lo general obtenerse rápidamente para una instalación de emergencia y como la computadora es la unidad más cara, dicho acuerdo es menos costoso que un hot site.

Cold sites: Es el menos costoso de sitio de copia de seguridad de una organización para operar. No incluye la respaldada copia de los datos y la información de la ubicación original de la organización, ni tampoco incluye hardware ya configurado. La falta de hardware aprovisionado contribuye a los costos mínimos de puesta en marcha del cold sites, pero requiere tiempo adicional tras el desastre de tener la operación funcionando a una capacidad cercana a los que antes de la catástrofe. En algunos casos, cold sites puede tener equipo disponible, pero no es operacional.

Acuerdos interinstitucionales: Este es un método es poco frecuente, ya que consiste en que entre dos o más organizaciones cuenten con equipos o aplicaciones similares para que en el momento de un desastre se pueda subir los servicios. Bajo el acuerdo típico, los participantes prometen proveerse mutuamente tiempos de computadoras cuando surja una emergencia.

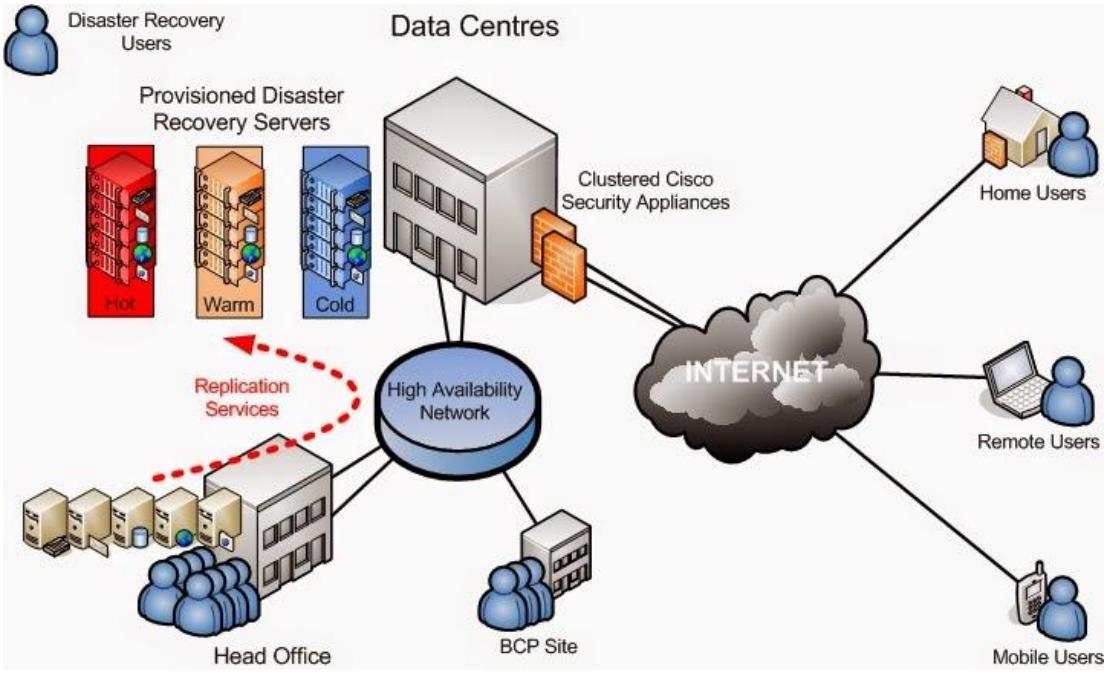
Este sitio alterno debe ubicarse lejanamente de la instalación del sistema principal y evitar que ambos fallen por estar en el mismo sector, ya sea por apagón, terremoto, ataque violento o vía Internet, entre otras.

El hardware y el software deben ser absolutamente compatibles para subir los servicios para el adecuado funcionamiento. Los recursos en ambas instalaciones deben ser iguales por lo que las revisiones periódicas y pruebas periódicas son básicas. [11]

En la siguiente imagen se ilustra un esquema de cómo debería estar la alternativa de recuperación que se elija para el DRP.

[11] Fuentes: (PLAN, Copyright (c) 2009 DRP.com.), (ISACA, 2012), (Valero, 2009)

Imagen 3. Infraestructura de Red – Alternativas de Recuperación [COBIT]



Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

5.4.2. Estrategia Recuperación vs Tiempo

Según los requerimientos analizados en RTO/RPO de los procesos de cada activo, se deberá contar con una alternativa de recuperación oportuna sobre los procesos críticos. La estrategia de recuperación debe respetar las medidas de seguridad. Contar con un contrato claro con los proveedores de servicio de almacenamiento y verificar los requerimientos de ancho de banda para asegurar todos los datos críticos pueden respaldarse según las escalas de tiempo RTO/RPO,

Con base a lo anterior se realiza un estudio donde se evalúan las estrategias de recuperación, basados en el tiempo en que se tardan cada una de ella en recuperar la funcionalidad mínima para garantizar la operación tras un desastre y en el costo que genere su aplicabilidad a la FNC.

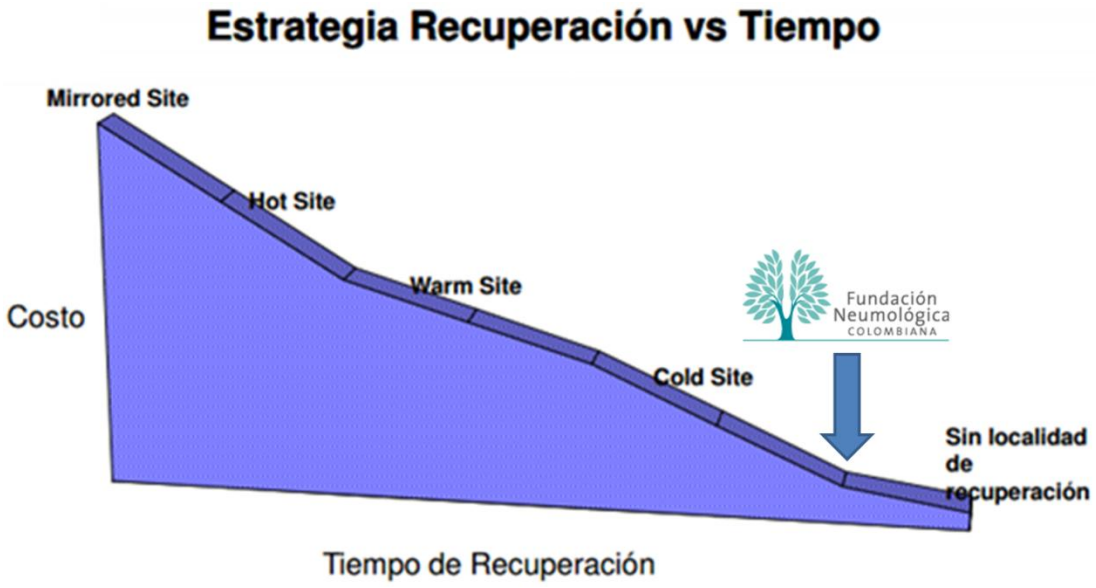
En la siguiente imagen se muestra las estrategias de continuidad y recuperación basadas en tiempos máximos aceptables de duración de la interrupción de servicio:

Imagen 4. Estrategias de Continuidad y Recuperación Impacto Vs Tiempo

Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

En la siguiente imagen se muestra las estrategias de continuidad y recuperación basadas en los costos de cada una de ellas y el punto en donde está la FNC:

Imagen 5. Estrategias de Continuidad y Recuperación Costo Vs Tiempo FNC



Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

La Tabla 6 es un comparativo claro y conciso sobre cada una las alternativas de recuperación:

Tabla 6. Cuadro Comparativo – Alternativas de Recuperación Propuesto

Tipo	Costo	Equipamiento de Hardware	Comunicación	Tiempo Configuración	Sitio
Cold Site	Bajo	Ninguno	Ninguno	Largo	Centro de Computo
Warm Site	Medio	Parcial	Parcial / Completo	Medio	Centro de Computo O Nube
Hot Site	Alto	Completo	Completo	Corto	Nube
Mirrored Site	Muy Alto	Completo	Completo	Ninguno	Centro de Computo o Sitio Alterno

Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

Para los costos se realizó una relación por cada una de las estrategias planteadas, con diferentes proveedores con base a las distintas propuestas, esto se muestra en la sección 7.

5.4.3. Organización y asignación de responsabilidades

Para el desarrollo del plan se debe tener en cuenta la decisión por parte de la FNC al momento de seleccionar la mejor estrategia de recuperación ante un desastre, teniendo en cuenta los siguientes puntos:

- Debe ser desarrollado basado en la estrategia de recuperación seleccionada por la FNC.
- Debe abarcar todos los temas involucrados en la recuperación de un desastre teniendo en cuenta el plan de contingencia desarrollado.
- Se debe contar con los recursos tanto físicos como humanos necesarios asignados por parte de la FNC, para una buena implementación de acuerdo con los tiempos estipulados en el plan de contingencia.

5.6. PRUEBAS

5.6.1. Plan de Pruebas

La fase de prueba debe contener las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro. Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis.

Según COBIT el Plan de Recuperación de Desastres debe ser probado, con el fin de determinar si funciona adecuadamente o si hay partes del plan que deben ser actualizadas. Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones a la operación normal sean mínimas como los fines de semana, adicional deben comprender los elementos críticos y simular condiciones de proceso lo más parecidas a la normales de operación, aunque se realicen fuera de horas. Las pruebas deben incluir las siguientes tareas[12]:

- Verificar la totalidad y precisión del Plan.
- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre los miembros del área de TI, proveedores y otros terceros.
- Medir la capacidad del sitio de respaldo, para ejecutar el proceso requerido.
- Identificar la capacidad de recuperar registros e información vital.
- Evaluar el estado cantidad del equipo y suministros que han sido movidos al sitio de recuperación.
- Medir el desempeño de los sistemas operativos y computacionales.

5.6.2. Tipos de Pruebas

Check list test. Las diferentes áreas revisan el Plan y hacen sus comentarios para asegurarse que nada falte.

Structured Walk-Trough test. Representantes de las diferentes áreas se reúnen y “caminan” a través del Plan, evaluando diversos escenarios desde el principio al fin.

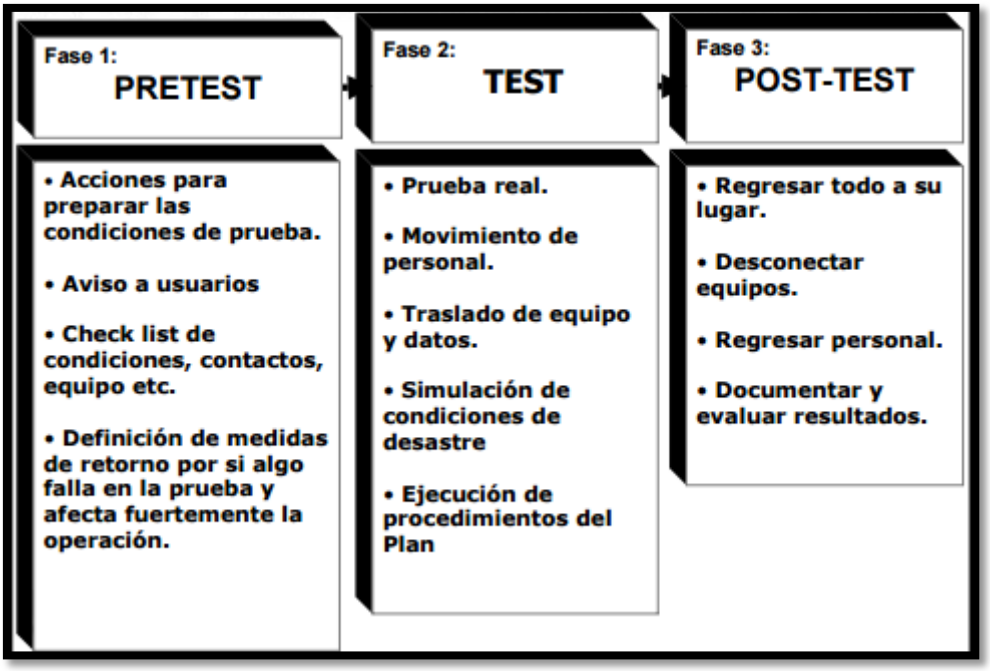
Simulation test. Este toma más gente y planeación. Se revisa un escenario específico y se ejecutan los pasos que se indican en el plan, simulando incluso la relocalización hacia un sitio alterno.

[12] ISACA. (Abril de 2012). *International Professional Association That Deals With ir Governance COBIT 5*. Obtenido de http://www.isaca.org/

Parallel test. Se hace para asegurarse de que los sistemas trabajen de acuerdo a lo esperado en el sitio alterno. Se procesa en el sitio alterno y se comparan los resultados con los que se obtienen en el sitio de producción.

Full interruption test. Esta es una prueba real donde el sitio de producción es detenido y se debe trabajar en las instalaciones y facilidades alternas, en la Imagen 6, se ilustra mejor estas fases.

Imagen 6. Fases del Proceso Full- Interruption Test.



Fuente: ISACA. (Abril de 2012). International Professional Association That Deals With ir Governance COBIT 5. Obtenido de http://www.isaca.org/ (ISACA, 2012)

Las pruebas de recuperación de desastres deben realizarse de modo habitual. Las comunicaciones, la recuperación de datos y la recuperación de aplicaciones suelen ser los ejes de todas las pruebas de recuperación de desastres. Los demás sectores para estas pruebas pueden variar, dependiendo de los objetivos de la organización sobre el punto de recuperación (RPO) y el tiempo de recuperación (RTO).[13]

[13] (ISACA, 2012), (PLAN, Copyright (c) 2009 DRP.com.)

Entrenamiento y distribución del Plan

El entrenamiento y distribución del Plan en la FNC es necesaria para que los involucrados tengan el concomimiento claro de cómo se desarrolla el plan (ISACA, 2012):

Entrenamiento: La administración del Plan debe asegurar que todas las personas involucradas reciban entrenamiento sobre los procedimientos a seguir en caso de desastres. Además de entrenamiento teórico, se debe hacer que el personal participe en las pruebas y simulacros del Plan.

Distribución: El Plan de continuidad contiene mucha información sensitiva, por lo que debe ser distribuido solo a personas autorizadas. El Plan se dividirá en secciones las cuales se entregaran sobre la base de “necesita saber” solamente.

Mejora Continua: Con base en las pruebas y experiencias reales, el plan deberá ser mejorado continuamente, aprendiendo de los errores cometidos.

6. PRESUPUESTO DETALLADO

6.1. MIRROR SITES.

Para la este tipo de propuesta se presentan varias soluciones de distintos fabricantes líderes en el mercado, solo se plantea un supuesto de servidores basándonos en los activos críticos de la información antes mencionados, en la tabla 7 se muestra una solución con la marca DELL:

Tabla 7. Propuesta de equipos – Mirror Sites con marca DELL

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	PowerEdge R730	Procesador: Intel® Xeon® 8 Core. Ram: 16 Disco Duro: 120 GB SSD	$4,745.00 USD	Servidor terminal	Centro de Computo Alterno
Servidor	PowerEdge R730	Procesador: Intel® Xeon® 8 Core. Ram: 16 Disco Duro: 120 GB SSD	$4,745.00 USD	Servidor terminal	Centro de Computo Alterno
Servidor	PowerEdge R730	Procesador: Intel® Xeon® 8 Core, Ram: 64 Disco Duro: 120 GB SSD Red: QLogic 57800 2x10Gb BT + 2x1Gb BT	$6,862.00 USD	Servidor ESXI	Centro de Computo Alterno
Comunicación	N3024	Switch Capa 3 24 Puertos 2x 10GbE SFP	$3,322.00 USD	Equipo de Comunicación	Centro de Computo Alterno

Tabla 7. Continuación

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Almacenamiento	PowerVault MD3400	4x 1TB SAS 10K RPM 4x 600GB SAS 15K RPM	$14,805.00 USD	SAN	Centro de Computo Alterno
Costo Total Propuesta			**$34,479.00 USD**		

Fuentes: (Dell Official Site), (DELL PowerEdge R730), (PowerEdge R730), (Dell Networking N3024 Switch), (PowerVault MD3400, 2015)

En la Tabla 8 se presenta la solución con la marca Hewlett Packard:

Tabla 8. Propuesta de equipos – Mirror Sites con marca HP

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	ProLiant DL360 Gen9	Procesador: Intel® Xeon® 8 Core. Ram: 32 Disco Duro: 120 GB SSD	$4,059.00 USD	Servidor terminal	Centro de Computo Alterno
Servidor	ProLiant DL360 Gen9	Procesador: Intel® Xeon® 8 Core Ram: 32 Disco Duro: 120 GB SSD	$4,059.00 USD	Servidor terminal	Centro de Computo Alterno
Servidor	ProLiant DL180 Gen9	Procesador: Intel® Xeon® 8 Core. Ram: 32 Disco Duro: 120 GB SSD Red: QLogic 57800 2x10Gb BT + 2x1Gb BT	$6,079.00 USD	Servidor ESXI	Centro de Computo Alterno

Tabla 8. Continuación

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Comunica-ción	HP 2920	Switch Capa 3 24 Puertos 2x 10GbE SFP	$1,005.00 USD	Equipo de Comunicación	Centro de Computo Alterno
Almacena-miento	MSA 2040	4x 1TB SAS 10K RPM 4x 600GB SAS 15K RPM	$8,856.00 USD	SAN	Centro de Computo Alterno
Costo Total Propuesta			**$24,058.00 USD**		

Fuentes: (HP Official Site), (HP ProLiant DL360 Gen9 E5-2630v3 1P 16GB-R P440ar 500W PS Base SAS Server)

En la Tabla 9 se presenta la solución con la marca IBM:

Tabla 9. Propuesta de equipos – Mirror Sites con marca Lenovo IBM

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	System x3650 M5	Procesador: Intel® Xeon® 8 Core Ram: 32 GB Disco Duro: 120 GB SSD	$3,826.00 USD	Servidor terminal	Centro de Computo Alterno
Servidor	System x3650 M5	Procesador: Intel® Xeon® 8 Core Ram: 64 GB Disco Duro: 120 GB SSD	$3,826.00 USD	Servidor terminal	Centro de Computo Alterno

Tabla 9. Continuación

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	System x3650 M5	Procesador: Intel® Xeon® 8 Core Ram: 64 GB Disco Duro: 120 GB SSD Broadcom NetXtreme 2x10GbE BaseT Adapter	$6,723.00 USD	Servidor ESXI	Centro de Computo Alterno
Costo Total Propuesta				**$14,375.00 USD**	

Fuente: (Lenovo System x3650 M5), (IBM - United States)

6.2. HOT SITES.

Para la este tipo de propuesta se presentan varias soluciones de distintos fabricantes líderes en el mercado, solo se plantea un supuesto de servidores basándonos en los activos críticos de la información antes mencionados, en la tabla 7 se muestra una solución con la marca DELL

Para este escenario se realizó unas cotizaciones con varios ofertantes, se configuraron servidores virtuales en la nube con características de hardware parecidas a los servidores físicos, en la Tabla 10 se muestra la solución con Claro:

Tabla 10. Propuesta de servidores Cloud – Hot Sites con Claro Cloud

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server 2008 R2	Procesador: 4 vCPU Ram: 16 GB Disco Duro: 50 GB	$ 1,056,000 Peso Colombiano	Servidor terminal
Servidor	Windows Server 2008 R2	Procesador: 4 vCPU Ram: 4 GB Disco Duro: 50 GB	$ 614,000 Peso Colombiano	Controlador Dominio DFS Servidor Impresión

Tabla 10. Continuación

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server 2008 R2	Procesador: 2 vCPU Ram: 2 GB Disco Duro: 50 GB	$ 420,000 Peso Colombiano	Base de Datos SQL 2008 ENT
Costo Total Propuesta Mensual			**$2,090,000 Peso Colombiano**	

Fuente: (Servidores Virtuales - Soluciones en la Nube- Claro Cloud)

Este contrato con claro es pago mensual fijo, se utilicen o no los servidores. Caso contrario sucede con la solución con Microsoft (Tabla 11), ellos tienen un tipo de tarificación que es solo por uso, tiene otro tipo de costo o facturación por minuto.

Tabla 11. Propuesta de servidores Cloud – Hot Sites con Microsoft Azure

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server STD	Procesador: 8 vCPU Ram: 14 GB Disco Duro: 50 GB	$535,68 USD	Servidor terminal
Servidor	Windows Server STD	Procesador: 2 vCPU Ram: 7 GB Disco Duro: 100 GB	$535,68 USD	Controlador Dominio DFS Servidor Impresión
Servidor	Windows Server STD	Procesador: 2 vCPU Ram: 3.5 GB Disco Duro: 50 GB	$407,72 USD	Base de Datos SQL STD
Costo Total Propuesta Mes			**$1.179,99 USD**	

Fuente: (Microsoft Azure), (Calculadora de Precios, Calcule Rapidamente su Factura)

La solución con Amazon (Tabla 12), su costo es si se utiliza la maquina en el mes y por hora, ellos tienen este tipo de tarificación en caso tal que la maquina registe actividad u utilización.

Tabla 12. Propuesta de servidores Cloud – Hot Sites con Amazon Web Services

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server STD	Procesador: 8 vCPU Ram: 15 GB Disco Duro: 50 GB	$582,68 USD	Servidor terminal
Servidor	Windows Server STD	Procesador: 2 vCPU Ram: 3.7 GB Disco Duro: 100 GB	$145,67 USD	Controlador Dominio DFS Servidor Impresión
Servidor	Windows Server STD	Procesador: 2 vCPU Ram: 7.5 GB Disco Duro: 32 GB	$520,46 USD	Base de Datos SQL STD
Costo Total Propuesta por Mes				**$1.248,81 USD**

Fuentes: (Amazon Web Service Simple Mounthy Calculator)

6.3. WARM SITES

En esta propuesta se seleccionó un servidor tanto físico, como virtual en la nube, que sea capaz de soportar la carga laboral, en la Tabla 13 la solución con DELL:

Tabla 13. Propuesta de equipo – Warm Sites con marca DELL *(Dell Official Site)*

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	PowerEdge R730	Procesador: Intel® Xeon® 8 Core Ram: 16 GB Disco Duro: 120 GB SSD	$4,745.00 USD	Servidor Alterno	Centro de Computo

Fuente: (PowerEdge R730)

En la Tabla 14 se describe la propuesta de un servidor físico con Hewlett Packard:

Tabla 14. Propuesta de equipos – Warm Sites con marca HP *(HP Official Site)*

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	ProLiant DL360 Gen9	Procesador: Intel® Xeon® 8 Core Ram: 32 GB Disco Duro: 120 GB SSD	$4,059.00 USD	Servidor Alterno	Centro de Computo

Fuente: (HP ProLiant DL360 Gen9 E5-2630v3 1P 16GB-R P440ar 500W PS Base SAS Server)

En la Tabla 15 la propuesta de un servidor físico con IBM:

Tabla 15. Propuesta de equipos – Warm Sites con marca Lenovo IBM

Equipo	Referencia	Características	Costo	Servicio a Prestar	Ubicación
Servidor	System x3650 M5	Procesador: Intel® Xeon® 8 Core Ram: 32 GB Disco Duro: 120 GB SSD	$3,826.00 USD	Servidor Alterno	Centro de Computo

Fuente: (Lenovo System x3650 M5)

En la Tabla 16 la propuesta de un servidor virtual en la nube con Claro:

Tabla 16. Propuesta de servidores Cloud – Warm Sites con Claro Cloud

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server 2008 R2	Procesador: 4 vCPU Ram: 16 GB Disco Duro: 50 GB	$ 1,056,000 Peso Colombiano	Servidor Alterno

Fuente: (Servidores Virtuales - Soluciones en la Nube- Claro Cloud)

En la Tabla 17 la propuesta de un servidor virtual en la nube con Microsoft, ellos tienen un tipo de tarificación que es solo por uso, tiene otro tipo de costo o facturación por minuto:

Tabla 17. Propuesta de servidores Cloud – Warm Sites con Microsoft Azure

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server STD	Procesador: 8 vCPU Ram: 14 GB Disco Duro: 50 GB	$535,68 USD	Servidor Alterno

Fuente: (Microsoft Azure), (Calculadora de Precios, Calcule Rapidamente su Factura)

En la Tabla 18 la propuesta de un servidor virtual en la nube con Amazon, tiene un costo de utilización de la maquina en el mes por hora, ellos tienen este tipo de tarificación en caso tal que la maquina registe actividad u utilización.

Tabla 18. Propuesta de servidores Cloud – Warm Sites con Amazon Web Services

Equipo	SO	Características	Costo	Servicio a Prestar
Servidor	Windows Server STD	Procesador: 8 vCPU Ram: 15 GB Disco Duro: 50 GB	$582,68 USD	Servidor Alterno

Fuentes: (Amazon Web Service Simple Mounthy Calculator)

6.4. COLD SITES

El COLD SITES es esencialmente sólo el espacio del centro de datos, donde se tiene la copia básica de la información. Si ocurre un desastre, el área de tecnología puede ayudar fácilmente a mover la información en el centro de datos y obtener una copia de seguridad y funcionamiento.

Esta alternativa de recuperación es con la que actualmente cuenta la FNC, solo se cuenta con copias de seguridad diarias en cintas almacenadas dentro del mismo centro de cómputo.

7. BENEFICIOS DE LA IMPLEMENTACIÓN

El resultado de la implementación de un DRP es poder contar con un plan de contingencia que incluye las responsabilidades y facultades detalla de un Plan de Recuperación de Desastres. Un DRP establece una guía y provee la certeza razonable de que los recursos y las instalaciones críticas de TI permanecerán disponibles en caso de un desastre.

Operacionales

- La capacidad de proteger los sistemas críticos para la FNC tras un desastre natural o humano.
- Mejora de la eficiencia general de la organización y la identificación de la relación de bienes y recursos humanos y financieros para los servicios críticos.
- Provee un sentido de seguridad: El conocimiento y la certeza de que se cuenta con alternativas para la continuación de las operaciones trasmite confianza a la FNC

De Gestión

- Reducción de pérdidas tras un incidente activando el plan de recuperación de desastres.
- La reducción de las posibles responsabilidades legales que pueden ocurrir bajo un desastre.

Estratégicos

- Minimizar el riesgo de retrasos al momento de ocasionarse un desastre.
- Minimizar la toma de decisiones en caso de desastre.
- Minimizar tiempos de recuperación tras un desastre bien sea natural o humano.

De Infraestructura

- Proporcionar un sentido de seguridad mediante la implementación de un DRP.
- Provee un sitio de seguridad: el conocimiento y la certeza de que cuenta con alternativas para la continuación de las operaciones.

De TI

- Garantizar la fiabilidad de los sistemas de reserva al momento de un desastre en la FNC.

8. ALCANCES DEL PROYECTO

La necesidad de diseñar un DRP, está vinculada con el impacto que provoca la dificultad parcial o total de los servicios tecnológicos y los procesamientos informáticos, sobre el normal desarrollo de las actividades de la FNC; específicamente, para afrontar la contingencia relacionada con la interrupción de actividades e inoperatividad de los servicios tecnológicos.

Por ende los procedimientos planteados en este documento, examinan solamente las acciones a realizar ante un desastre o incidente involucrados en los procesos críticos definidos en el Plan.

Adicionalmente, se consideran los riesgos del software, hardware y soluciones del ambiente físico afectados con la operación de los procesos principales del Centro de Cómputo de la FNC.

Las actividades y procedimientos, se relacionan con las funciones que involucran a cada uno de los eventos establecidos para la ejecución del DRP, y dependen de la actividad y colaboración de los usuarios y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.). El avance de las actividades, está condicionado a la aprobación de los mismos por parte del Jefe de TI.

9. LIMITACIONES DEL PROYECTO

Si se decide implementar el DRP por parte de la FNC, dependiendo de la alternativa de recuperación los limitantes serian:

- Recursos Económicos: El presupuesto que sea aprobado puede modificar las características de la alternativa seleccionada por parte de la FNC. El proceso de implementación de la solución puede afectarse dependiendo que el presupuesto aprobado.
- Recursos Tecnológicos: Dependiendo de la alternativa seleccionada estamos sujetos a la disponibilidad de los equipos, servidores virtuales, equipos de activos de comunicación u otros implementos que se necesiten para la solución propuesta.
- Recursos Humanos: Es indispensable contar con el recurso humano capacitado para la implementación, control y seguimiento del DRP.

10. CRONOGRAMA

En la Imagen 7, se muestra el desarrollo de las actividades realizadas en el proyecto:

	Nombre	Inicio	Fin
1	**MARCO TEORICO**	**02/02/2015**	**06/02/2015**
2	El Análisis de Impacto en el Negocio (BIA)	02/02/2015	02/02/2015
3	Plan de Recuperación de Desastres (DRP)	03/02/2015	03/02/2015
4	COBIT (Control Objectives for information and related Technology)	04/02/2015	04/02/2015
5	Gestión de Riesgo	05/02/2015	05/02/2015
6	Administración de Riesgos	06/02/2015	06/02/2015
7	**INGENIERÍA DEL PROYECTO**	**09/02/2015**	**13/02/2015**
8	Descripción de la situación actual	09/02/2015	11/02/2015
9	Requerimientos de la información	11/02/2015	12/02/2015
10	Modelamiento del sistema	12/02/2015	13/02/2015
11	**DESARROLLO DRP**	**16/02/2015**	**17/04/2015**
12	Desarrollo de Políticas DRP	16/02/2015	19/02/2015
13	**Impacto de Análisis del Servicio BIA**	**20/02/2015**	**11/03/2015**
14	Identificación de procesos	20/02/2015	26/02/2015
15	Procesos Críticos	26/02/2015	27/02/2015
16	Identificación de infraestructura	27/02/2015	02/03/2015
17	Análisis de Vulnerabilidades	26/02/2015	11/03/2015
18	Tiempos Objetivo (RTO y RPO)	05/03/2015	10/03/2015
19	**Evaluación de Riesgos**	**12/03/2015**	**27/03/2015**
20	Riesgos Potenciales	12/03/2015	17/03/2015
21	Amenazas, Vulnerabilidades y Controles	13/03/2015	23/03/2015
22	Elementos de Continuidad y Contingencia	16/03/2015	27/03/2015
23	**Desarrollo de estrategias de Recuperación**	**16/03/2015**	**01/04/2015**
24	Alternativas de Recuperación	16/03/2015	27/03/2015
25	Estrategia Recuperación vs Tiempo	27/03/2015	01/04/2015
26	**Desarrollo del plan**	**02/04/2015**	**08/04/2015**
27	Organización y asignación de responsabilidades	02/04/2015	06/04/2015
28	Componentes del Plan de Recuperación de Desastres	06/04/2015	08/04/2015
29	**Pruebas**	**07/04/2015**	**10/04/2015**
30	Plan de Pruebas	07/04/2015	08/04/2015
31	Pruebas de Plan de Pruebas de Recuperación de Desastres	08/04/2015	10/04/2015
32	**Mantenimiento**	**10/04/2015**	**17/04/2015**
33	Mantenimiento del Plan	10/04/2015	14/04/2015
34	Estructura del Plan	15/04/2015	17/04/2015
35	**EVALUACIÓN ECONÓMICA DEL PROYECTO**	**20/04/2015**	**01/05/2015**
36	Presupuesto Detallado	20/04/2015	01/05/2015
37	**BENEFICIOS DE LA IMPLEMENTACIÓN**	**01/05/2015**	**07/05/2015**
38	Operacionales	01/05/2015	01/05/2015
39	De Gestión	04/05/2015	04/05/2015
40	Estratégicos	05/05/2015	05/05/2015
41	De Infraestructura	06/05/2015	06/05/2015
42	De IT	07/05/2015	07/05/2015
43	**Preparacion y terminacion del documento escrito**	**08/05/2015**	**14/05/2015**
44	Revision del documento y Preparacion final	08/05/2015	14/05/2015
45	**Entrega de Proyecto**	**15/05/2015**	**15/05/2015**
46	Presentacion del Proyecto	15/05/2015	15/05/2015

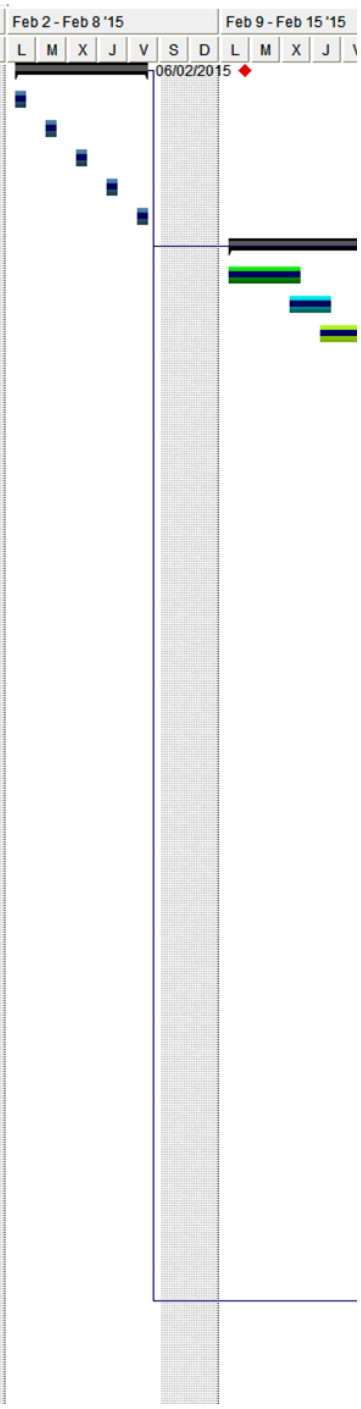


Imagen 7. Cronograma de Actividades (Cronograma DRP, 2015)

11. RECOMENDACIONES

- Realizar actualizaciones periódicas del DRP y documentar cualquier cambio que se realice a los activos de la información, teniendo en cuenta la infraestructura tecnológica.
- Capacitar y preparar al personal responsable de la ejecución del plan.
- Realizar periódicamente los diferentes tipos de pruebas descritos en el presente documento.
- Tomar en cuenta las Políticas propuestas en el documento actual.
- Realizar reuniones periódicas para la revisión del Plan del DRP.
- Actualizar los activos de la información periódicamente y re evaluar los riegos e impactos.
- Tomar una decisión basada en las estrategias de recuperación planteadas en el documento, la estrategia que mejor se adaptaría a los cambios sin incurrir muchos costos es “Propuesta de servidores Cloud – Hot Sites” en el presente documento, esta tiene los requerimientos de tecnología más cercanos a los servidores físicos actuales sin realizar una gran inversión o cambios en la infraestructura, para esta propuesta se tiene planteada un plan de pruebas para tener a consideración vista en el (Anexo 7).

12. CONCLUSIONES

Al diseñar del Plan de Recuperación de Desastres (DRP) para la FNC se encuentra que los activos de información están son totalmente frágiles susceptibles a sufrir cualquier tipo de desastre o caos dentro de sus operaciones, es por ello que es sumamente importante que se cuente con un plan debidamente estructurado y organizado para llevarlo a cabo dentro o después de ese tipo de actividades que puedan afectar la estabilidad de los objetivos de la empresa.

La información reunida en los puntos de análisis de impacto y evaluación del riesgo, permite desarrollar una estrategia correcta para la FNC con un balance óptimo de reducción de riesgo y una o varias alternativas de recuperación. En el presente documento también se incluyen las consideraciones de las prioridades en el proceso de recuperación del servicio, definiendo procesos diferentes para los sistemas más críticos descritos en el archivo de Identificación de Procesos – Descripción de los Activos en cada Proceso.

En el diseño del DRP se presentan alternativas para el restablecimiento de la información y la pérdida potencial permitida, cada uno de ellos representa un costo y un esfuerzo muy diferente, la conclusión final con base en los requerimientos de la FNC es tomar la más completa con mayor alcance a la reducción del riesgo y reducción mínima a la posibilidad de pérdida de información.

13. BIBLIOGRAFÍA

Libro
ALABERTO. Alexander. Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005, Bogotá, Alfaomega Grupo Editor, 2007, pgs. 15-20.

Resumen
ALABERTO. Alexander. Gestión de incidentes de seguridad informática, Madrid España, SatarBook Editorial, 2011, pgs. 15-35.

Resumen
CHAPMAN. Jacqueline. Plan de recuperación de Negocios en una semana, Londres, Hodder & Stoughton Editorial, 2002, pgs. 11-38.

Libro
GÓMEZ VIEITES. Álvaro. Enciclopedia de la Seguridad Informática, 2ª Edición, México, Alfa omega Grupo Editor, 2007, pgs. 37- 195.

Libro
ISACA, Framework. COBIT 5. For Information Security, Estados Unidos de América, 2012.

Libro
SALLIS. Ezequiel. Ethical hacking, Un enfoque metodológico para profesionales. Buenos Aires, Alfaomega Grupo Editor, 2009, pgs. 25-30.

14. CIBERGRAFÍA

20071, I. (s.f.). *ISO 20071*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:20071:-11:ed-1:v1:en

AbaNet, I. d. (s.f.). *AbaNet*. Obtenido de http://www.abanet.net/acronimos.html

Amazon Web Service Simple Mounthy Calculator. (s.f.). Recuperado el 08 de 05 de 2015, de http://calculator.s3.amazonaws.com/index.html

BCI. (s.f.). *Business Continuity Institute*. Obtenido de http://www.thebci.org/

Calculadora de Precios, Calcule Rapidamente su Factura. (s.f.). Recuperado el 10 de 05 de 2015, de http://azure.microsoft.com/es-es/pricing/calculator/?scenario=full

Cronograma DRP. (02 de 02 de 2015). *DRP FNC*. Obtenido de https://drive.google.com/file/d/0B-qJ1S7CaUQqbjlTcHZlRUxYakk/view?usp=sharing

Dell Networking N3024 Switch. (s.f.). *The Dell Online Store: Build Your System*. Recuperado el 13 de 05 de 2015, de http://configure.us.dell.com/dellstore/config.aspx?c=us&cs=04&l=en&model_id=networking-n3000-series&oc=bcctk1&s=bsd&fb=1&vw=classic

Dell Official Site. (s.f.). *Dell Official Site*. Obtenido de http://www.dell.com/

DELL PowerEdge R730. (s.f.). *The Dell Online Store: Build Your System*. Recuperado el 14 de 05 de 2015, de http://configure.us.dell.com/dellstore/config.aspx?c=us&cs=04&fb=1&l=en&model_id=poweredge-r730&oc=pe_r730_1356&s=bsd&vw=classic

Empresa, B. L. (s.f.). *SCRIBD Dirección general de unidades de negocio [en línea]*. Recuperado el 30 de 03 de 2015, de http://es.scribd.com/doc/7132807/Gestion-Riesgos-Tecnologicos

FNC, F. N. (s.f.). *FNC*. Recuperado el 2015 de 03 de 13, de FUNDACIÓN NEUMOLÓGICA COLOMBIANA: http://www.neumologica.org/index2.html

HP 2920-24G Switch (J9726A). (s.f.). *Amazon*. Recuperado el 10 de 05 de 2015, de http://www.amazon.com/HP-J9726A-2920-24G-Switch/dp/B00BJ42JYG

HP MSA 2040 SAN Dual Controller SFF Storage/S-Buy. (s.f.). *HP*. Recuperado el 10 de 05 de 2015, de http://store.hp.com/webapp/wcs/stores/servlet/us/en/pdp/hp-msa-2040-san-dual-controller-sff-storage-s-buy?Redirect_SMB_ETR=Yes&CatalogCategoryID=#!&TabName=specs

HP Official Site. (s.f.). *HP*. Obtenido de http://www.hp.com/

HP ProLiant DL180 Gen9 E5-2630v3 2P 32GB-R P840/4G 16SFF SAS 800W RPS ES Server. (s.f.). *HP*. Recuperado el 11 de 05 de 2015, de http://www8.hp.com/us/en/products/proliant-servers/product-detail.html?oid=7142235#!tab=specs

HP ProLiant DL360 Gen9 E5-2630v3 1P 16GB-R P440ar 500W PS Base SAS Server. (s.f.). *HP*. Recuperado el 11 de 05 de 2015, de http://www8.hp.com/us/en/products/proliant-servers/product-detail.html?oid=6830385#!tab=specs

IBM - United States. (s.f.). *IBM*. Obtenido de http://www.ibm.com/

ISACA. (Abril de 2012). *International Professional Association That Deals With ir Governance COBIT 5*. Obtenido de http://www.isaca.org/

Lenovo System x3650 M5. (s.f.). *IBM US IBM*. Recuperado el 10 de 05 de 2015, de http://www-304.ibm.com/shop/americas/webapp/wcs/stores/servlet/default/ProductDisplay?productId=4611686018426657951&storeId=1083993954&langId=-1&categoryId=4611686018425313555&dualCurrId=1074768503&catalogId=-4840

Microsoft Azure. (s.f.). *Microsoft Azure*. Recuperado el 13 de 05 de 2015, de http://azure.microsoft.com/es-es/pricing/

PLAN, D. R. (Copyright (c) 2009 DRP.com.). *DISASTER RECOVERY PLAN*. Recuperado el 13 de 03 de 2015, de http://drptopicosii.site90.com/introdrp.html

PowerEdge R730. (s.f.). *The Dell Online Store: Build Your System*. Recuperado el 12 de 05 de 2015, de http://configure.us.dell.com/dellstore/config.aspx?c=us&cs=04&fb=1&l=en&model_id=poweredge-r730&oc=pe_r730_1356&s=bsd&vw=classic

PowerVault MD3400. (13 de 05 de 2015). *The Dell Online Store: Build Your System*. Obtenido de http://configure.us.dell.com/dellstore/config.aspx?c=us&cs=04&fb=1&l=en&model_id=powervault-md32x0-series&oc=brct82&s=bsd&vw=classic

Servidores Virtuales - Soluciones en la Nube- Claro Cloud. (s.f.). *Claro Cloud*. Recuperado el 11 de 05 de 2015, de http://www.clarocloud.com.co/wps/portal/co/cloud/empresas/servicios-cloud/infraestructura/servidores-virtuales#info-02-bc

Valero, N. (2009). *RECUPERACION DE DESASTRES Y CONTINUIDAD DEL NEGOCIO.* Universidad Externado de Colombia.

15. ANEXOS

Anexo 1 Desarrollo de Políticas para implementación DRP.

POLITICAS DE IMPLEMENTACIÓN DRP (PLAN DE RECUPERACIÓN DE DESASTRES)
FUNDACIÓN NEUMOLOGICA COLOMBIANA

1. El departamento de tecnología de la Fundación Neumológica Colombiana desarrollará planes de contingencia para cada aplicación principal o sistema de soporte general que cumpla las necesidades de operación crítica de TI en el evento de una interrupción superior a 24 horas.
2. Los procedimientos para su ejecución serán documentados de manera formal por parte del encargado de desarrollar el Plan de Contingencia y deberá ser revisado semestralmente y actualizado según sea necesario por el jefe de TI para su validación y aprobación.
3. Dicha actualización (a partir de la segunda versión en adelante) incluirá un capítulo donde se especificará las altas y bajas de los planes específicos de contingencia, así como aquellos que por uno u otro motivo fueron modificados respecto a su versión original.
4. Se mantendrán 2 copias vigentes de respaldo y se repartirá una copia a todas las áreas involucradas en los planes.
5. El plan puede asignar responsabilidades a funcionarios asignados para facilitar la recuperación y/o continuidad de funciones esenciales de TI.
6. Se debe evaluar el impacto de las contingencias que se presenten periódicamente.
7. Los recursos necesarios para asegurar la viabilidad de los procedimientos deberán ser adquiridos y mantenidos.
8. El personal responsable de sistemas claves serán entrenados para ejecutar los procedimientos de contingencia.
9. Proponer la capacitación al personal nuevo del servicio, sobre las actividades que deben ejecutar cuando se presente la contingencia.
10. Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el plan de contingencia.
11. Proponer reuniones periódicas sobre el plan de contingencia.

Anexo 2 Identificación de Procesos – Descripción de los Activos en cada Proceso (FNC) (Inventario de Activos)

Inventario de Activos de la Informacion

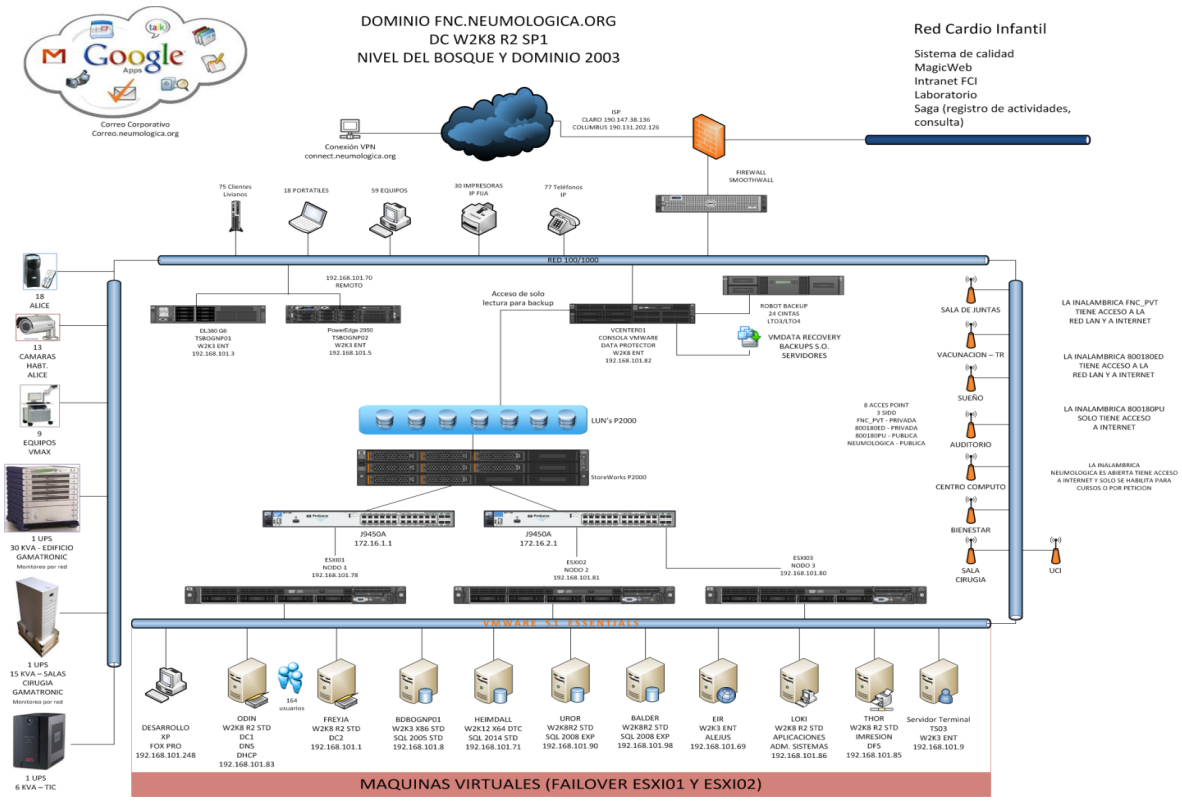
Nr	Organización y Procesos relevantes			Nombre del Activo	Descripcion del activo	Tipo de información de activos [Copia en papel , archivos electrónicos (especificar el tipo) , medios extraíbles / dispositivo (especificar el tipo)]
	Unidad Operativa / Funcion	Nombre del Proceso	Dueño del Proceso			
1	Direccion Medica	Alejus	Personal Asistencial	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Electronicos, base de datos FOX.
2	Direccion Administrativa	Servinte	Personal Administrativo	Servinte	Software administrativo de aplicativo contable, facturacion, activos fijos, suministros, caja y bancos, cartera	Electronicos, base de datos sql 2005.
3	Direccion Administrativa	NovaSoft	Personal Nomina	NovaSoft	Software administrativo de nomina	Electronicos, base de datos FOX.
4	Pruebas Funcion Pulmonar	Vmax	PRFP	Vmax	Software de captura de informacion de estudio de pruebas de funcion pulmonar	Electronicos, base de datos FOX.
5	Pruebas Funcion Pulmonar	Ndd	PRFP	Easy on-PC	Software de captura de informacion de estudio de pruebas de funcion pulmonar	Electronicos, base de datos access
6	Pruebas Funcion Pulmonar	MedGraphics	PRFP	Brezze	Software de captura de informacion de estudio de pruebas de funcion pulmonar	Electronicos, base de datos access
7	Pruebas Funcion Pulmonar	Estadisticas	PRFP	Pruebas Funcion Pulmonar 201x.xlsx	Cuadro de mando, datos estadisticos y preciosos de facturacion del servicio, pacientes de alejus y calidad	Electronicos, archivo excel, conexión a base de datos con vistas a servinte y alejus
8	Consulta Externa Adultos	Estadisticas	COAD	Consulta Externa	Cuadro de mando, datos estadisticos y	Electronicos, archivo excel, conexión a base de

Anexo 3 Identificación de Procesos – Descripción de los Activos en cada Proceso (FNC) (Vulnerabilidades PC)

Procesos Criticos de Activos de la Informacion

Organización y Procesos relevantes	Informacion detallada del Activo		Vulnerabilidades	Amenaza	Probabilidad 5 Probable 4 Muy probable 3 Moderada 2 Improbable 1 Rara	Impacto 5 Catastrofico / Perdidas Enormes 4 Mayor / Perdidas mayores 3 Moderado / Perdidas medias 2 Menor / Perdidas bajas 1 Insignificante / Perdidas minimas	Riesgo Inherente
Unidad Operativa / Funcion	Nombre del Activo	Descripcion del activo					
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Integridad de la base de datos	Archivos compartidos en la red, se debe tener la carpeta compartida con privilegios a todos los usuarios que acceden a sistema	4	5	20
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Caida en la conexión de red	La informacion de la base de datos no esta disponible	3	5	15
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Caida en la conexión de red	Las transacciones en el momento de la caida corrompen la base de datos	3	5	15
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Caida en la conexión de red	No si tiene acceso a las pruebas realizadas a los pacientes	3	5	15
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Seguridad en la Carpeta de acceso a la BD	Perdida de disponibilidad en el repositorio de almacenamiento de pruebas realizadas al paciente	2	5	10
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Usuarios Genericos de consulta para el acceso a la informacion	No se tiene control sobre quien es reponsable del acceso y a las acciones realizadas con el usuario	4	3	12
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Compartir los usuarios y contraseñas del personal asistencial	No se tiene control sobre quien es reponsable del acceso y a las acciones realizadas con el usuario	3	3	9
DIME	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	Reportes en linea para las estadisticas del sistema	Al realizar los reportes en momentos u horas pico, la transaccion de la informacion puede causar lentitud en el sistema al usuario	3	4	12

Anexo 4 Esquema de Red e Infraestructura FNC.



Anexo 5 RPO y RTO PC.

RPO y RTO de los Procesos Criticos

Nr	Organización y Procesos relevantes		Informacion detallada del Activo		RPO	RTO
	Nombre del Proceso	Dueño del Proceso	Nombre del Activo	Descripcion del activo		
1	Alejus	Personal Asistencial	Alejus	Software de captura de informacion para las historias clinicas y pruebas que se realizan a pacientes	24 Horas	4 Horas
2	Servinte	Personal Administrativo	Servinte	Software administrativo de aplicativo contable, facturacion, activos fijos, suministros, caja y bancos, cartera	24 Horas	4 Horas
3	NovaSoft	Personal Nomina	NovaSoft	Software administrativo de nomina	24 Horas	4 Horas
4	PC	CONTAB	PC	Equipo de acceso al sistema, contiene aplicativo ERP servinte, con los modulos de contabilidad	48 Horas	48 Horas
5	PC	Nomina	PC	Equipo de acceso al sistema, contiene aplicativo NovaSoft, para liquidar la nomina	48 Horas	48 Horas
6	Correo	TEIN	Correo	Software de cominicacion interna y externa por correo electronico.	0 Horas	1 Hora
7	Firewall	TEIN	Smoothall	Software de segurdad perimetral, cortafuegos, filtrado de contenido, VPN, IpSec	4 Horas	2 Hora
8	Firewall	TEIN	Servidor	Equipo de seguridad perimetral, cortafuegos, conexiones con los modem de claro y columbus	4 Horas	4 Horas
9	Estudio Sueño	SUEÑ	Alice Base Station	Equipo medico, captura toda la informacion transmitida por el paciente para enviarlo por red al pc repositorio de informacion	72 Horas	72 Horas

Anexo 6 Procedimientos de contingencia FNC.

Procedimientos de contingencia FNC

14/04/2015
Fundación Neumológica Colombiana
Cristhian Garzón

Anexo 7 Lista de Chequeo Plan de Pruebas.

El esquema presentado para el plan de pruebas está basado en la solución "Propuesta de servidores Cloud – Hot Sites" en el presente documento, para esto se sugiere la siguiente lista de chequeo para los activos críticos de información:

- Se debe verificar los servicios que se van a implementar en esta solución, teniendo en cuenta los activos críticos de la información descritos en el del archivo Identificación de Procesos – Descripción del Activo en cada Proceso (Matriz de Riesgos PC).
- Los servidores que se implementen en esta solución deben cumplir con los requerimientos mínimos de hardware para su funcionamiento, estos servidores deben tener una conexión con el Dominio y anexarlos con las políticas antes ya descritas.
- Se debe realizar pruebas de conectividad, simular carga de estrés a los servidores y aplicativos como un ambiente de producción, para poder detectar posibles fallas y falencias al momento ejecutar la solución propuesta para el DRP.
- Verificar el cumplimiento y expectativas acorde al RTO y RPO evaluado dentro del plan de pruebas.
- Evaluar y capacitar el desempeño del personal encargado de ejecutar el plan de pruebas.
- Evaluar la coordinación entre los miembros del área de TI, proveedores y otros terceros.
- Medir la capacidad de la solución Hot Sites, para ejecutar los activos críticos en la activación del plan de pruebas.
- Documentar el resultado y evaluación de las pruebas ejecutadas.