ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DEL PLAN DE RECUPERACIÓN ANTE DESASTRES PARA UN SISTEMA INFORMÁTICO HOSPITALARIO"

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

KEVIN ALEXANDER ALFARO PÉREZ

JORGE CRISTHIAN SILVA MUÑOZ

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Quiero agradecer a Dios, por darme salud y la sabiduría necesaria para llegar a escalar con firmeza un escalón más hacia mi vida profesional, por hacer realidad uno de mis sueños tan anhelados, a mi familia que fue mi fuente de apoyo en los momentos más difíciles y también agradecerles por haber estado en cada instante de mi vida con sus consejos e inculcándome buenos valores; por ser unos excelentes guías y enseñarme a apreciar mis estudios para que sigua superándome cada día de mi vida.

Y por último a todas aquellas personas que han estado apoyándome de alguna manera, y que hoy les puedo llamar amigos, siempre formarán parte de mis buenos recuerdos y permanecerán en mi corazón siempre, a todos ellos que han sido un pilar importante en mi vida, agradezco sus consejos y los ánimos prestados.

Kevin Alexander Alfaro Pérez

Mis más sinceros agradecimientos en primer lugar a Dios, porque gracias a sus bendiciones y misericordia he logrado llegar hasta este punto de mi vida, porque a pesar de mi problema de salud me ha levantado de las muchas recaídas que he tenido para mantenerme en pie para seguir luchando por esta meta. A mi madre porque gracias a su disciplina y educación, he logrado una formación personal y profesional de la que estoy contento, Ella ha sido un pilar fundamental en todos los momentos más difíciles, la persona que junto a mí ha cargado la cruz de mi problema de salud sin quejas, más bien con consejos y ánimos incondicionales.

A mis distinguidos docentes que a lo largo de mis estudios han sido también un gran apoyo para la adquisición de conocimientos fundamentales para este proyecto. A mi revisor de proyecto y tutor que sin sus observaciones no hubiese sido posible culminar este trabajo. Finalmente, pero no menos importante a mi novia por el constante ánimo y ayuda en días agobiantes del trabajo, a mi compañero de proyecto por la paciencia brindada y a todas aquellas personas que me han dado una mano en tiempos de necesidad.

Jorge Cristhian Silva Muñoz.

DEDICATORIA

A Dios por haberme levantado en cada momento difícil de mi vida, gracias a él he completado este objetivo, además de mi familia los cuales han estado para servir de apoyo y motivación para esforzarme y luchar por mis sueños, por mis metas propuestas, a todos ellos les dedico este proyecto, porque ellos son los que han logrado forjar la persona que soy ahora.

Kevin Alexander Alfaro Pérez

El presente proyecto lo dedico a Dios, a mi madre y a mis profesores de la carrera. A Dios porque ha cuidado de mí en cada paso que doy, porque ha logrado que en mí no se agote la paciencia y la Fé de que iba a lograr llegar hasta etapa de mi vida. A mi madre quien me ha compartido su fortaleza para no rendirme ante las adversidades presentadas a lo largo de mi vida y a mis profesores de la carrera en la institución que han sido un gran aporte para mí en conocimiento muy importante para el desarrollo de este proyecto. A ellos a quienes les debo todo lo que soy y lo que sé les dedico este esfuerzo.

Jorge Cristhian Silva Muñoz

TRIBUNAL DE EVALUACIÓN

Mg. Robert Andrade Troya

PROFESOR EVALUADOR

Mg. José Patiño Sánchez

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Kevin Alfaro P.

Kevin Alexander Alfaro Pérez

Jorge Cristhian Silva Muñoz

RESUMEN

Los planes de recuperación ante desastres son importantes, sobre todo en lugares donde se maneja información crítica, más aún cuando de esta dependen vidas humanas. Nadie está seguro al 100%, todos estamos expuestos a ciertos acontecimientos ya sean estos naturales o realizados por personas como terrorismo, virus informático, errores en la administración de los servidores, etc.

En el caso de esta investigación de campo realizada en el hospital Guayaquil, se identificó la necesidad de tener un plan de recuperación ante desastres, ya que en los hospitales como este, con mucha concurrencia de usuarios – pacientes, las soluciones tecnológicas en su infraestructura y centro de datos (datacenter) deben ser de alta disponibilidad; por el motivo que maneja información relacionada a la salud y bienestar de las personas, como son: imágenes diagnósticas, exámenes de laboratorio entre otros. La misma que podría atentar directa o indirectamente contra la vida de los pacientes por no contar con el recurso de información cuando se la requiere.

Por lo que hemos realizado un estudio de la infraestructura y centro de datos del hospital Guayaquil, con la finalidad de diseñar un plan de recuperación ante desastres, el cual consiste en la instalación de un segundo centro de datos de manera virtualizada en un lugar seguro, identificado como secundario, la virtualización le ayudara a tener la información disponible con riesgos menores de interrupción, generando mayor seguridad en el personal que labora en el hospital y mejorando así la disponibilidad de servicios para todos sus pacientes.

ÍNDICE GENERAL

AGRADECIMIENTOS ii
DEDICATORIA iv
TRIBUNAL DE EVALUACIÓN v
DECLARACIÓN EXPRESA vi
RESUMEN vii
ÍNDICE GENERAL viii
ÍNDICE DE FIGURAS xi
ÍNDICE DE TABLAS xii
CAPÍTULO 1 1
1. INTRODUCCIÓN AL SISTEMA HOSPITALARIO 1
1.1 Antecedente 2
1.2 Problemática 2
1.3 Metodología 3
1.4 Objetivos 4
1.4.1 Objetivo General 4
1.4.2 Objetivos Específicos 4
CAPÍTULO 2 5
2. ANÁLISIS TÉCNICO Y SOLUCIÓN TECNOLÓGICA 5
2.1 Marco teórico 5
2.1.1 DRP 5
2.1.2 BCP 5
2.1.3 SIM 5

2.1.4 SAN 6
2.1.5 Criticidad 6
2.1.6 Niveles de criticidad 6
2.1.7 Análisis de Criticidad. 7
2.1.8 RTO y RPO 7
2.2 Análisis técnico 8
2.3 Infraestructura a nivel de red 11
2.4 Servidores 12
2.5 Red SAN de Servidores 14
2.6 Inconvenientes presentados por el actual centro de datos 15
2.7 Análisis de Criticidad (AC) 16
2.7.1 Clasificación de equipos según su criticidad 16
2.8 Ancho de banda para el centro de cómputo alterno 18
2.9 Propuesta para la mejora del centro de cómputo. 19
2.9.1 Diseño 19
2.9.2 Esquema físico 20
2.9.3 Esquema lógico o de direccionamiento 21
2.9.4 Distribución de equipos en el centro de cómputo alterno. 22
2.9.5 Alcance 23
CAPÍTULO 3 24
3. PLAN DE RECUPERACION ANTE DESASTRES. 24
3.1 Fases del Diseño. 24
3.1.1 Fase 1 24
3.1.2 Fase 2 24

3.1.3 Fase 3 25
3.1.4 Fase 4 26
3.1.5 Fase 5 26
3.1.6 Fase 6 28
3.2 Responsabilidades de la institución 28
3.2 Propuesta Económica. 30
CONCLUSIONES Y RECOMENDACIONES 31
BIBLIOGRAFÍA 33
ANEXOS 34

INDICE DE FIGURAS

Figura 1.1 Estadísticas de pérdidas en el sector de salud debido a desastres.....1

Figura 2.1 Diagrama de distribución de espacio actual.....9

Figura 2.2 Diagrama general de la red del Hospital.....11

Figura 2.3 Diagrama De Red de Servidores.....12

Figura 2.4 Diagrama De Red SAN del centro de datos.....14

Figura 2.5 Diseño de la solución general.....19

Figure 2.6 Esquema del centro de datos alterno.....21

Figura 2.7 Diagrama final de distribución de equipos del DRP.....23

ÍNDICE DE TABLAS

Tabla 1 Lista de Servicios.....12

Tabla 2 Servicios según criticidad.....16

Tabla 3 Esquema de direccionamiento IP.....22

Tabla 4 Proforma de equipos necesarios para la implementación del DRP.....30

CAPÍTULO 1

1. INTRODUCCIÓN AL SISTEMA HOSPITALARIO

De acuerdo a datos estadísticos que se pueden apreciar en la FIGURA 1.1, proporcionados por UNISDR (The United Nations Office for Disaster Risk Reduction) por sus siglas en ingles Oficinas de las Naciones Unidas para la Reducción de Riesgo de Desastres, se puede evidenciar que los costos originados por los desastres en cuanto al sector de salud se refiere, han llegado casi a una cifra de $13 mil millones de dólares dentro de los años correspondientes al análisis indicado en el gráfico.

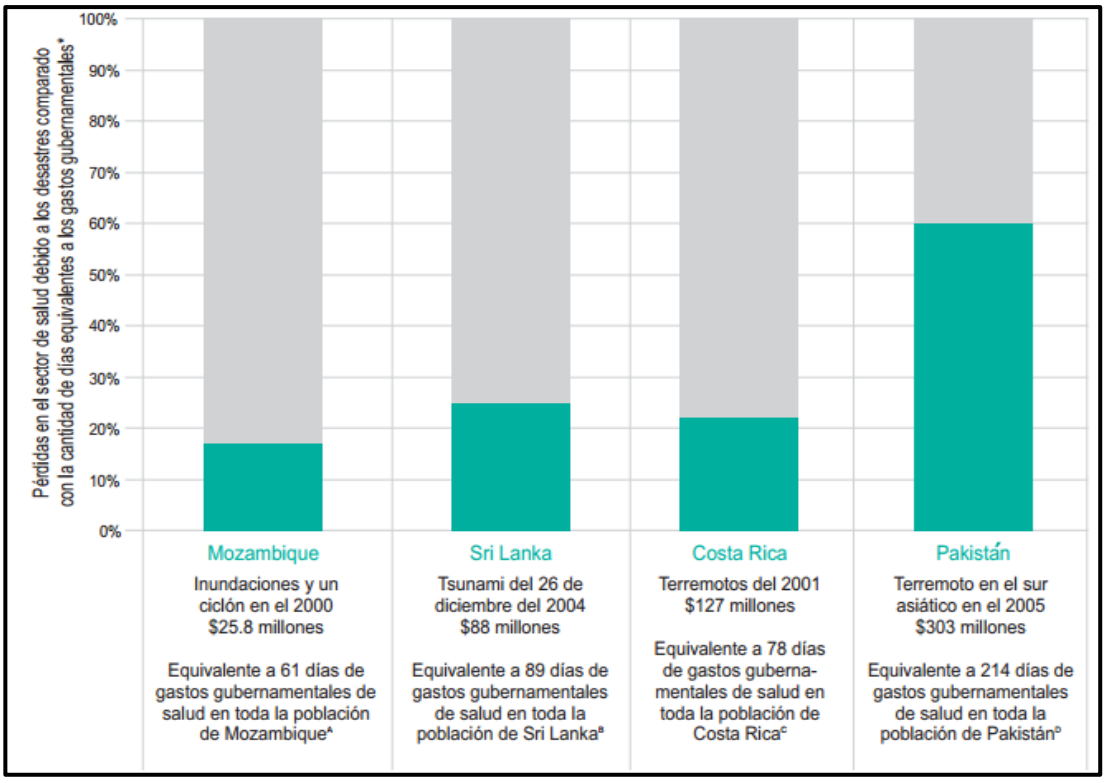

Figura 1.1: Estadísticas de pérdidas en el sector de salud debido a desastres. (Bajado de http://www.unisdr.org/)

Esto ha provocado que la gran cantidad de información que se genera en los centros hospitalarios se vuelva vital y/o crítica para el funcionamiento de los mismos, pudiendo afectar los servicios de salud ofertados al público, generando una

necesidad de proteger esta información, y de garantizar siempre la disponibilidad de la misma, para que sus servicios de salud no sufran interrupciones, garantizando así la calidad permanente de las actividades en los centros hospitalarios.

El almacenamiento y gestión de la información, siempre debe considerar la posibilidad de que existan interrupciones en el servicio proporcionado a la institución, en este caso a los centros hospitalarios; estas interrupciones se pueden deber a errores humanos, ya sean intencionales o no, así como puede deberse a factores externos de tipo climático y también a falla de sus equipos informáticos, provocando un desastre tecnológico.

Estos tipos de desastres tecnológicos han intentado ser cubiertos por mecanismos, conocidos por tradicionales, tales como el respaldo y recuperación de información con herramientas de ofimática, uso de imágenes, etc. Pero estos mecanismos cada vez han demostrado ser poco efectivos en su desempeño y hoy en día existen nuevas posibilidades de llevar a cabo esta protección de datos a través de un diseño para la implementación de un plan de contingencia ante un desastre, el cual consiste en la creación de una infraestructura de red mejorada en comparación con la principal pero en una ubicación distinta, que cuente con los recursos necesarios para el levantamiento de los servicios involucrados.

1.1. Antecedente

El Hospital Guayaquil fundado el 7 de octubre de 1973, es conocido por su gran afluencia de pacientes, por el servicio hospitalario brindado y por la gran reputación de sus profesionales; el mismo que se encuentra ubicado en la ciudad del mismo nombre.

En la actualidad cuenta con el siguiente personal: 56 médicos residentes, 73 licenciadas en enfermería, 178 auxiliares de enfermería y 139 médicos distribuidos en 35 especialidades. Además, tienen un promedio de pacientes hospitalizados de alrededor de 400, varía diariamente. También cuenta con aproximadamente 100 camas para pacientes en todas sus áreas.

Su amplia gama de servicios médicos incluye las siguientes ramas:

- Anestesiología
- Cardiología
- Cirugía Cardiovascular
- Cirugía General
- Cirugía Plástica
- Cirugía Torácica
- Cirugía Vascular Periférica
- Dermatología
- Endocrinología
- Gastroenterología
- Geriatría
- Ginecología
- Hematología
- Infectología
- Medicina Interna
- Nefrología
- Neumología
- Neurocirugía
- Neurología
- Nutrición
- Oftalmología
- Oncología
- Otorrinolaringología
- Proctologría
- Psiquiatría
- Reumatología
- Terapia del dolor
- Traumatología
- Unidad de quemados
- Urología

Este centro hospitalario cuenta con equipos tecnológicos tanto en su área de centros de datos como también en las áreas de servicio a los pacientes, éstos últimos generan información relevante como son: historias clínicas, aproximadamente entre 100 y 50 semanalmente, imágenes de rayos X, ecografías y resonancias magnéticas, con una media de 120 exámenes del centro de imágenes al día. La misma que debe estar siempre disponible para brindar un servicio de primer nivel a la comunidad.

Los Equipos médicos tienen un generador el cual les permite el funcionamiento alrededor de 25 minutos y ellos pueden trabajar aun no teniendo conexión al centro de datos porque tienen un disco duro el cual les permite guardar de 100 a 200 estudios como máximo.

Si el centro de datos llegase a colapsar afectando los servicios del sistema hospitalario, los doctores, enfermeras, etc. no pueden dejar de atender a los pacientes; para ello se emplea un contingente manual, en el cual se toman datos y registros ya sea por herramientas de ofimática o en papel y pluma.

1.2. Problemática

Desde sus inicios, el hospital ha sido y es en su totalidad administrado por el Gobierno Nacional del Ecuador, a través de personal designado por el mismo, los beneficios de este vínculo con el estado se han visto reflejados mayormente en la gratuidad de todos sus servicios y en la re categorización del hospital a nivel 3 el 25 de Abril de 2012, mediante acuerdo Ministerial #667, suscrito por la Srta. Carina Vance Nafla, actualmente ex Ministra de Salud Pública , sin embargo, como punto negativo al costear el estado todas las necesidades de los paciente, no se ha podido recaudar fondos necesarios para las implementaciones adecuadas en el área de informática del hospital, por ello a pesar de que el centro de datos del hospital Guayaquil cuenta con procesos que permiten el respaldo de información intentando tenerla a salvo de cualquier evento que dañe la misma, mitigando así el impacto ocasionado por algún tipo de desastre, estos respaldos de información crítica en la actualidad en el centro

de cómputo no son eficientes ni efectivos, y menos aún garantiza la disponibilidad de la misma; esto crea un problema en el manejo de los datos críticos del hospital dejándolos desprotegidos, mostrando así una falencia que hoy en día se puede evitar teniendo un plan de recuperación ante desastres, que asegure la disponibilidad de la información y calidad en la atención a sus pacientes.

1.3. Metodología

Hoy en día existe una posibilidad de llevar a cabo esta protección de datos, que está siendo ignorada por muchas instituciones, pero que es de suma importancia para sus operaciones, la cual se refiere a un diseño para la implementación de un plan de contingencia ante un desastre. Para esto se detalla a continuación las fases que considera el diseño:

Fase 1.- plasmar los múltiples conceptos necesarios, para comprender todo lo que conlleva el diseño de un plan de contingencia ante desastres y los sistemas que serán involucrados dentro del mismo.

Fase 2.- describir un criterio el cual nos permita definir los niveles de criticidad que se deben considerar en el diseño del plan de recuperación ante desastres, con el fin de clasificar de manera correcta todos los componentes que se verán respaldados con el diseño del plan, de tal forma que se asigne el nivel de prioridad necesario que merece cada uno de ellos.

Fase 3.- mediante entrevistas con el personal de TI de la institución y visitas técnicas realizadas al centro de datos del hospital, se procede al levantamiento de la información con respecto a la infraestructura del espacio físico, así como también de la infraestructura de red actual.

Fase 4.- finalmente con respecto a la información obtenida de la situación actual del centro de datos del hospital, se procede a la descripción de una propuesta para el diseño del plan de recuperación ante desastres, tomando en cuenta aspecto como: espacio físico donde se ubicaran nuevos equipos, equipos necesarios que se van a adquirir acorde al diseño del plan, así como también

los pasos a seguir para el levantamiento, funcionamiento y correcta activación del plan de contingencia ante desastres.

1.4. Objetivos

1.4.1. Objetivo General

Realizar un estudio de la infraestructura y del centro de datos del hospital Guayaquil, con la finalidad de diseñar un plan de recuperación ante desastres, el cual consiste en la instalación de un segundo centro de datos de manera virtual en un lugar seguro, el mismo que pueda ser ejecutado por personal externo calificado, permitiéndole operar en poco tiempo ante cualquier desastre.

1.4.2. Objetivos Específicos

Realizar un análisis sobre el estado en el que se encuentra la infraestructura de red y el datacenter.

Sugerir mejoras de acuerdo a los resultados obtenidos.

Sugerir un plan de contingencia ante desastres para poder obtener alta disponibilidad de la data.

Determinar los procesos a considerar para mantener el plan de recuperación ante desastre de manera activa.

CAPÍTULO 2

2. ANÁLISIS TÉCNICO Y SOLUCIÓN TECNOLÓGICA

2.1. Marco teórico

Antes de pasar con el análisis técnico y el planteamiento de la solución tecnológica para el caso Hospital Guayaquil, es necesario tener en cuenta varios conceptos que serán de gran utilidad para comprender lo expuesto en el presente trabajo.

2.1.1. DRP

Un DRP (Disaster Recovery Plan) o plan de recuperación de desastres, es aquel que se implementa en las empresas u organizaciones con el fin de evitar o minimizar los efectos causados por la presencia de algún desastre, ya sea ocasionado por las fuerzas de la naturaleza o por la presencia del hombre.

2.1.2. BCP

Un BCP (Business Continuity Plan) o plan de continuidad de negocio, es aquel que se implementa cuando ocurre una interrupción no deseada y tiene como objetivo de recuperar y restaurar funciones dentro de un tiempo determinado.

La diferencia entre DRP y BCP es que el DRP se limita a los procesos de infraestructura de TI.

2.1.3. SIM

Un SIM (Sistema Integrado de Manufactura) hace referencia a la utilización de las herramientas informáticas para el control, monitoreo y visualización en tiempo real. Este sistema ha adquirido una relevante importancia debido a que cuenta con procesos informáticos los cuales proveen datos útiles al momento de determinar si existiera alguna novedad que afectase el normal desarrollo del proceso.

2.1.4. SAN

Una SAN (Storage Area Network) es una red dedicada al almacenamiento, la cual está conectada a la red LAN de la compañía. Una SAN cuenta con una red de alta velocidad, preferiblemente de fibra óptica, un equipo de interconexión dedicada (switch) y elementos para almacenamiento de red (discos duros).

2.1.5. Criticidad

Es un indicador proporcional al riesgo que permite establecer la Jerarquía o prioridades de procesos, sistemas y equipos, creando una estructura que facilita la toma de decisiones acertadas y efectivas, y permite direccionar el esfuerzo y los recursos a las áreas donde es más importante y/o necesario mejorar la confiabilidad y administrar el riesgo.

La criticidad se establece en tres niveles, alta, media y baja. La criticidad es establecida por un valor numérico el cual se determina entre el producto de la probabilidad o frecuencia de ocurrencia de una falla por la suma de las consecuencias de la misma, lo cual establece rasgos de valores para homologar los criterios de evaluación. Está definido bajo la ecuación (2.1).

$$\text{Criticidad} = \text{Frecuencia} * \text{Consecuencia}. \qquad (2.1)$$

2.1.6. Niveles de criticidad

Como se mencionó en el punto anterior, existen tres niveles de criticidad, alta, media y baja los cuales se detallan a continuación:

Alta.- Se ha definido como criticidad alta a aquellos servicios de producción y de desarrollo en cuanto a temas de laboratorio ya que son áreas que generan constantemente datos importantes para la institución como por ejemplo nuevos métodos de análisis que deben ser dados a conocer lo más pronto posible a los médicos para un óptimo diagnóstico de los pacientes.

Media.- En este nivel de criticidad se ubican aquellos servicios que, proporcionan datos de investigaciones que conllevan un largo periodo de estudio y que en un 90% de los casos, no afectan directamente a las operaciones de la institución de una manera crítica, es por eso que

también observamos ambientes de producción en la tabla 1, pero en su descripción se indican que son solo de control de acceso y componentes de capacitación.

Baja.- Estos servicios pueden ser interrumpidos por un amplio periodo de tiempo, son necesarios, pero no urgentes como los anteriores, no detienen los servicios ofertados, ya que la mayoría de ellos son ambientes de desarrollo que proporcionaran información valida en un largo periodo de tiempo para la institución, refiriéndonos a años como, por ejemplo, remodelaciones y parámetros de futuros servicios, que si se detienen solo afectaran en menos de un 5% la operatividad del hospital.

2.1.7. Análisis de Criticidad.

El análisis de criticidad (AC) es un método que permite establecer jerarquías en sistemas, instalaciones y equipos, en función de su impacto global con la finalidad de tomar decisiones. Antes de realizar un análisis de criticidad se debe definir un alcance y propósito para el análisis, establecer criterios de evaluación y seleccionar un método de recuperación.

Hay que tener en cuenta criterios fundamentales al momento de establecer un análisis de criticidad, entre esos tenemos:

- Seguridad
- Ambiente
- Producción
- Costos (operacionales y de mantenimiento)
- Tiempo promedio para reparar
- Frecuencia de falla.

Para la selección del método de evaluación se toman criterios de ingeniería, factores de ponderación y cuantificación.

2.1.8. RTO y RPO

Dentro del plan de continuidad de una institución tanto el RTO como el RPO son factores críticos que definen el éxito del mismo. A continuación se detalla el significado de cada uno.

RPO (Recovery Point Objective). - Objetivo de punto de recuperación, es el tiempo máximo de bloqueo de acceso a la información que puede sufrir la institución.

El tiempo de recuperación se estima en 15 minutos, esto se debe a que el hospital mantiene información delicada de sus pacientes y requiere el menor tiempo de bloqueo a la información.

RTO (Recovery Time Objective). – Objetivo de tiempo de recuperación, es el tiempo máximo de recuperación de servicios que se estima en la institución.

Se acuerda un tiempo de recuperación de 1 hora, para reactivar sus actividades y seguir brindado sus servicios a los pacientes.

2.2. Análisis técnico

Primero en cuanto al sistema de enfriamiento, se verificó que implementan la misma definición, como en la mayoría de centros de datos en Latinoamérica que es el de expansión directa, con temperatura de 18 grados, con equipos de aire acondicionado de 53,000 BTU.

Pasando a lo que es el sistema eléctrico para los equipos cuenta con un Sistema de alimentación ininterrumpida (SAI) de corriente continua de tipo line interactive, capaz de corregir los siguientes problemas: Fallos de alimentación, Caídas de tensión, Picos de corriente, sobretensiones y subtensiones, Infratensiones prolongadas y sobretensiones prolongadas.

En cuanto a la instalación de los cables eléctricos que permiten el funcionamiento de los equipos SAI, se realizó con acometidas internas y cableado eléctrico empotrado, al igual que las tomas de corrientes para los equipos informáticos, toda esta instalación eléctrica es monitoreada con Medidores digitales LED para: Voltaje, corriente y frecuencia, pero carecen de un software de control de energía dentro de la red.

A diferencia del cableado para la interconexión de los equipos de red del área, el cual fue implementado bajo piso falso; se destaca que el cableado estructurado es UTP de categoría 6, el mismo que es substituido en un promedio de 7 u 8 años o solo es substituido parte del cableado cuando se produce algún imprevisto en alguno de los equipos que provoque el reemplazo de los mismos.

Actualmente, hay un área que contiene la porción el centro de cómputo de la institución sobre la cual nos enfocamos, y consta con una dimensión de 6,36 x 6,80 metros ubicado en la planta baja del edificio principal en una zona esquinera del piso completamente cerrado con una única puerta de acceso para personal autorizado, tal y como se puede apreciar en la figura 2.1.

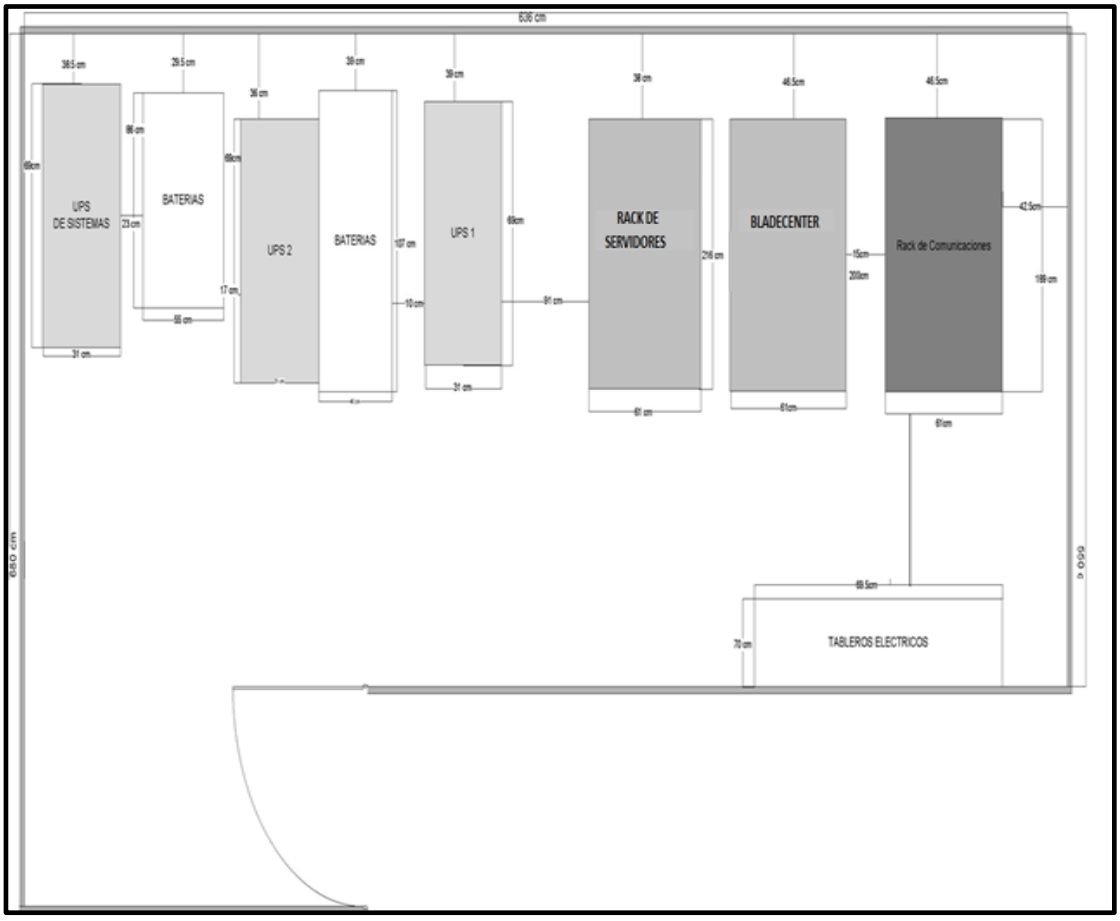

Figura 2.1: Diagrama de distribución de espacio actual (proporcionado por el cliente)

Cabe recalcar que cierta información como por ejemplo, los datos específicos que manejan los equipos del centro de cómputo, visitas prolongadas a la sala de equipos y una descripción al 100% acertada sobre la forma de administración y tipo de mantenimiento de los equipos fue clasificada como confidencial por la directiva del hospital, por lo que nos vimos obligados a omitir cierto tipo de información relacionada con estos aspectos.

Se destaca que la institución implementa un equipo storwize que son sistemas de almacenamiento virtualizados donde se utilizan versiones del software

NAVICAT para MySQL las cuales ofrecen una interfaz gráfica intuitiva y de gran alcance para la gestión de bases de datos de un aproximado de 8 Terabytes de datos críticos dentro de los que se destacan historiales médicos de pacientes críticos, informes sobre investigación de enfermedades, así como también resultados de los exámenes de los nuevos equipos del centro de imágenes, además de ofrecer herramientas de desarrollo y mantenimiento. y de gama empresarial que proporcionan la base para implementar una infraestructura de almacenamiento eficaz de datos, se emplean bladecenters para lo que es la implementación de servidores virtuales los mismos que en la actualidad solo poseen 10 cuchillas o blades sobre las cuales se instalan los diferentes servidores descritos en la lista que se mostrara posteriormente; estos dos dispositivos anteriormente mencionados están conectados a conmutadores SAN administrables; este sistema contiene redundancia mediante enlaces de fibra, cabe recalcar que actualmente se implementa VMware VSphere para lo que es la gestión de servidores en el bladecenter.

En cuanto a temas de conectividad, de acuerdo a la información provista, poseen una conexión a internet con una velocidad de 30 Mbps y una conexión de enlace de datos de la misma velocidad contratados por Telconet.
A continuación, en la Figura 2.2 se detalla la información de la infraestructura implementada actualmente en el Centro de Computo Principal.

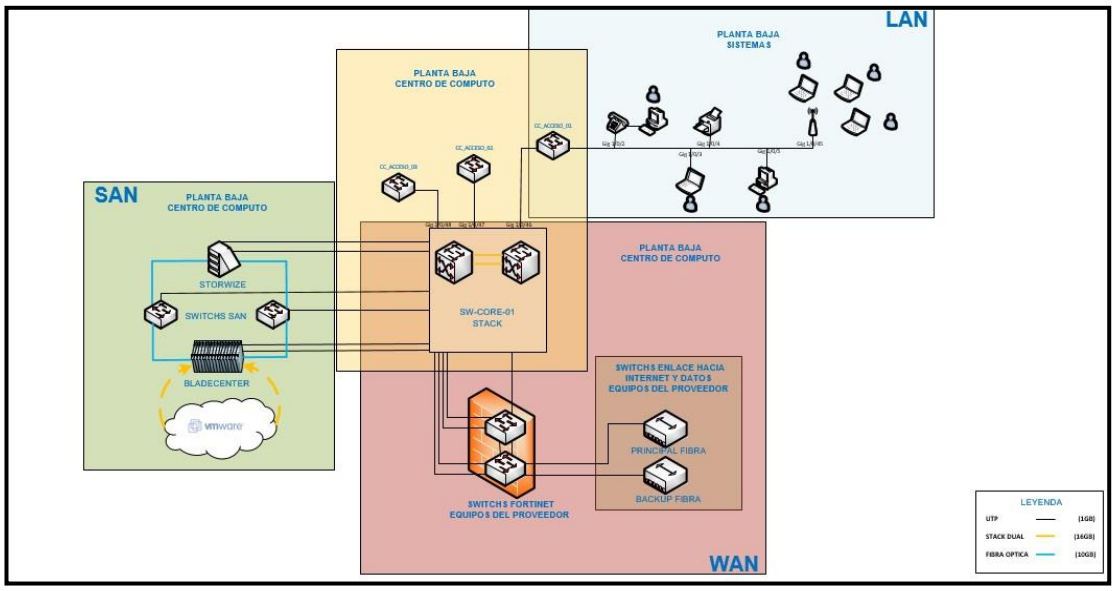

Figura 2.2: Diagrama general de la red del Hospital (proporcionado por el cliente)

2.3. Infraestructura a nivel de red

La infraestructura a nivel de red del área sobra la cual nos vamos a enfocar está conformada de los siguientes equipos:

- 2 Switches de Enlace de Internet y Datos
- 2 Switches Firewall (Proveedor)
- 2 Switches 3750 24p en Stack

Se encuentran implementados 2 switches Cisco 3750 en el Datacenter, los cuales son los CORE de la RED LAN, 2 Switches de enlace de internet y datos, estableciendo 1 como principal y otro como backup, en caso de fallo del primero, y 2 switches firewall, como redundancia para la seguridad, cabe indicar que este servicio es administrado por el proveedor.

En la Figura 2.3 se muestra la información detallada antes mencionada.

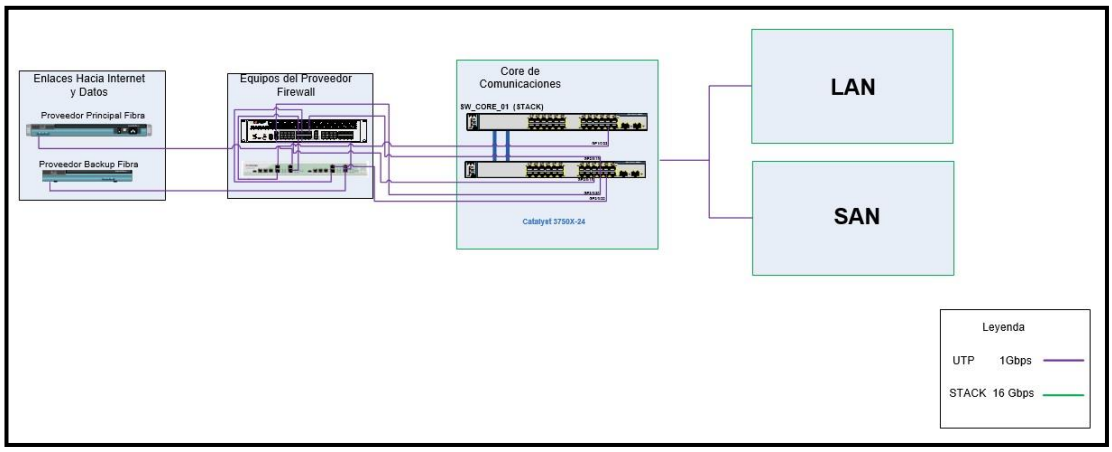

Figura 2.3: Diagrama De Red de Servidores. (Proporcionado por el cliente)

2.4. Servidores

A continuación, se adjunta tabla 1 en la cual se describen los servicios involucrados en el sistema hospitalario. Estos servicios se encuentran instalados en la plataforma virtual de VMware, tal como se muestra en la imagen (4 - servidores).

NOMBRE	DESCRIPCIÓN	AMBIENTE
SRV02AP02	Infrastructure DataBase - Onlycontrol	PRODUCCION
SRV02AP04	Infrastructure DataBase - INFORMIX PREP	PREPRODUCCION
SRV02AP05	Application Server - SCS COMPONENTES (Parametrizacion)	DESARROLLO
SRV02AP06	Application server - ITLink ADM (Admnistrativo)	PRODUCCION
SRV02AP07	Application server - ITLink LIS (Laboratorio)	DESARROLLO
SRV02AP08	Infrastructure - RDS Servinte	PREPRODUCCION
SRV02AP09	Infrastructure - RDS Parametrizacion	PREPRODUCCION
SRV02AP10	Application server - SCS Componentes (Capacitación)	PREPRODUCCION
SRV02AP11 – 12- 14 – 19 – 20 – 21 – 24 – 26 – 31 – 34 – 35 – 36	Infrastructure - Farm RDS	PRODUCCION
SRV02AP13	Application Server - SCS COMPONENTES	PRODUCCION
SRV02AP15	Infrastructure DataBase - ENTERPRISES	PRODUCCION
SRV02AP17	Application server - ITLink LIS (Laboratorio)	PRODUCCION

SRV02AP18	Infrastructure DataBase - HDR INFORMIX	PRODUCCION
SRV02AP23	Application server - ITLink ADM Capacitación y Preproducción	PREPRODUCCION
SRV02AP25	Infrastructure - RDS Farmacia	PRODUCCION
SRV02AP27	Application Server - SCS COMPONENTES RIS	PRODUCCION
SRV02AP28	Application server - ITLink RIS (Imágenes)	PRODUCCION
SRV02AP29	Application Server – MTRA	PRODUCCION
SRV02AP30	Infrastructure - Broaker Farm RDS	PRODUCCION
SRV02AP32	Application Server - INTERFAZ ENTERPRISES	PRODUCCION
SRV02AP33	Application Server - INTERFAZ GASOMETRO	PRODUCCION
SRV02AP37	Infrastructure - RDS Back Office	PRODUCCION
SRV02AP38	Infrastructure - RDS Parametrizacion	PRODUCCION
SRV02AP40	Infrastructure - RDS Servinte Test	PRODUCCION
SRV02AP41	Application server - ITLink ADM (Admnistrativo) – BackOffice	PRODUCCION
SRV02AP42	Infrastructure DataBase - INFORMIX PURGA	PRODUCCION
SRV02AP43	Infrastructure DataBase - INFORMIX BACKOFFICE	PRODUCCION
SRV02BC02	Virtualizaton – HostServer	PRODUCCION
SRV02CD01 – 02	Infrastructure - Domain Controller	PRODUCCION
SRV02DS01	Application Server - Enterprise	DESARROLLO
SRV02DS04	Application Server - SCS Componentes	DESARROLLO
SRV02DS05	Infrastructure DataBase - INFORMIX MANIOBRAS	DESARROLLO
SRV02DS07	Application Server - i Route	DESARROLLO
SRV02DS08	Infrastructure DataBase - SCS informix Preproduccion	PREPRODUCCION
SRV02DS50	Infrastructure DataBase - INFORMIX PRE CHD	DESARROLLO
SRV02DS51	Application Server - SCS COMPONENTES CHD	PREPRODUCCION
SRV02DS52	Infrastructure - RDS Parametrizacion CHD	DESARROLLO
SRV02DS53	Application server - ITLink ADM (Admnistrativo)	DESARROLLO
SRV02FS01	Infrastructure - File Server Qnap	PRODUCCION
SRV02FS02	Infrastructure - File Server	PRODUCCION
SRV02HS05 – 06 – 07 – 08 – 10 – 11 – 12 – 13 – 14	Virtualizaton – HostServer	PRODUCCION
SRV02IT01	Infraestructure – Respaldos	PRODUCCION
SRV02IT02	Infraestructure – Synergy	PRODUCCION
SRV02IT03	Infraestructure – Avaya	PRODUCCION
SRV02IT04	Infraestructure - Respaldos ITCA	PRODUCCION
SRV02IT05	Infraestructure – DHCP	PRODUCCION

SRV02SS01	Infrastructure - Pinter Server	PRODUCCION

Tabla 1: Lista de Servicios.

2.5. Red SAN de Servidores

La infraestructura de Storage Area Network (SAN por sus siglas en ingles) de la institución se encuentra en Switches IBM 2498-B24 en una configuración redundante. En caso de existir algún problema no esperado en un switch la conectividad a los dispositivos correspondientes continúa funcionando ininterrumpidamente.

Se encuentran implementados 2 Switches IBM 2498-B24, en donde cada switch tiene configurada su propia fabric, es decir una red SAN independiente que provee conectividad a cada dispositivo conectado. Al momento de realizar cambios en la configuración, es realizada en 1 fabric a la vez sin presentar caídas en los accesos o en los servicios de los dispositivos finales. En la siguiente figura 2.4 se muestra la información detallada antes mencionada.

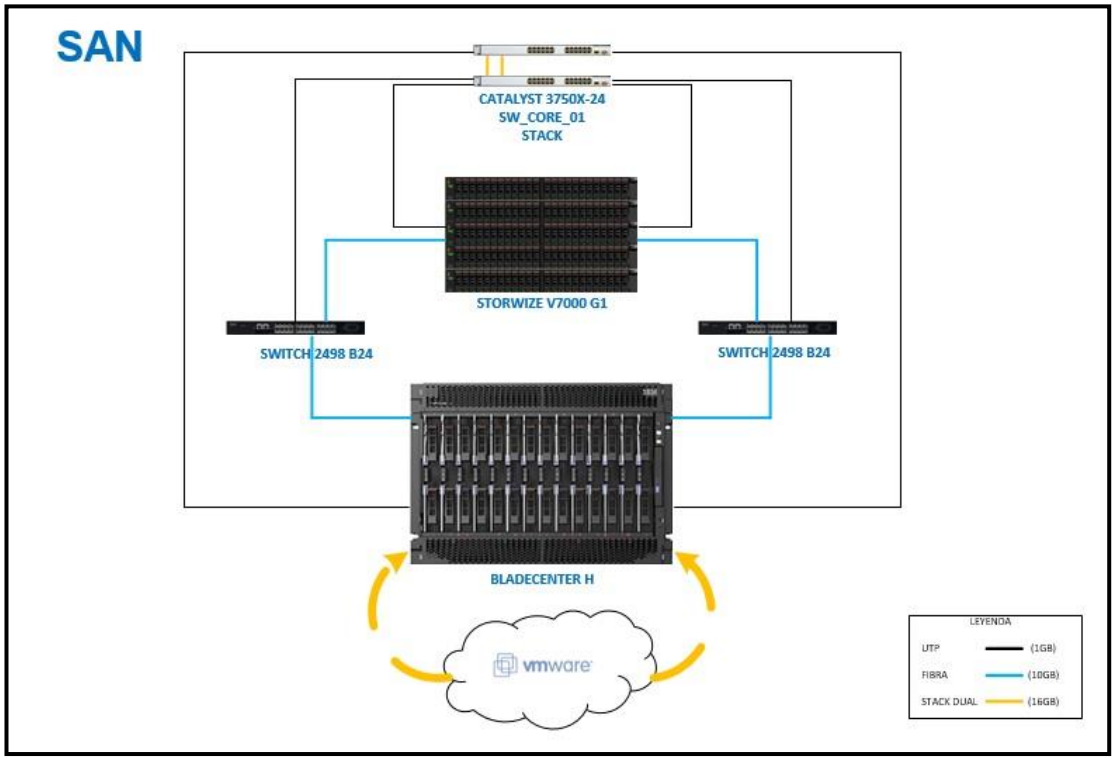

Figura 2.4: Diagrama De Red SAN del centro de datos.

2.6. Inconvenientes presentados por el actual centro de datos

En una de las entrevistas realizadas al personal de sistemas del hospital, se recopilo información sobre fallas de consideración que han sucedido en el centro de datos y han afectado los servicios hospitalarios:
Nos informaron que el equipo storwize v7000 de generación uno que esta implementado en el centro de cómputo del hospital, presentó una caída por el lapso de cinco horas, lo que a su vez dio origen a un gran impedimento en cuanto al acceso de información que era transmitida en la red de aproximadamente 15 pacientes, que justamente se encontraban en fase de registros de su historia clínica, retrasando las labores de los galenos y provocando malestar en aproximadamente 200 usuarios, poniendo en riesgo las vidas de pacientes por su retraso en la atención.

Se concluyó que el dispositivo de red presenta fallas en la configuración originado a raíz de un corte en el suministro de energía que se había producido mientras las instalaciones eran remodeladas.

Al no contar con un DRP Disaster Recovery Plan (por sus siglas en ingles), el hospital como se mencionó anteriormente perdió su capacidad de operación de aproximadamente un 50% debido a que los registro de datos se lo hizo de en papel y pluma; la operatividad de otros servicios también se vio afectada, el sistema de servidores que esta implementado en un Bladecenter presento daños en tres cuchillas o blades sobre las que se virtualizan los servidores y varias unidades de almacenamiento presentaban bloqueos de acceso a la información en el equipo storwize v7000.

La institución en todas sus áreas cuenta con un sistema de continuidad manual, es decir, deben emplear mecanismos para poder obtener y preservar los datos adquiridos de manera escrita o en documentos de office para poder tener el ambiente trabajando mientras que el personal de sistemas resuelve el desastre informático que puede haber ocurrido.

El año pasado se presentó un fallo humano en las configuraciones de los conmutadores pertenecientes al núcleo del centro de cómputo dejando sin conectividad a nivel general durante cuatro horas, debido a una mala actualización del firmware uno de los equipos de red antes mencionados al momento de levantar el sistema, no se tomó la medida correspondiente ya que los dispositivos de red se encontraban en modo apilamiento, perdiendo el orden maestro que tenían preestablecido.

Podemos constatar que los desastres informáticos pueden venir de muchas maneras, y se debe pensar en la mejor medida para poder tener una continuidad de servicios en el hospital; además debemos estar preparados para desastres con un impacto mayor como son los incendios, el terrorismo y virus informático, etc.

2.7. Análisis de Criticidad (AC)

2.7.1. Clasificación de equipos según su criticidad

A continuación, en la tabla 2 se detallan los servidores que forman parte del sistema hospitalario, con su respectiva criticidad.

NOMBRE	DESCRIPCIÓN	AMBIENTE	CRITICIDAD
SRV02AP02	Infrastructure DataBase – Onlycontrol	PRODUCCION	BAJA
SRV02AP04	Infrastructure DataBase - INFORMIX PREP	PREPRODUCCION	BAJA
SRV02AP05	Application Server - SCS COMPONENTES	DESARROLLO	MEDIA
SRV02AP06	Application server - ITLink ADM	PRODUCCION	BAJA
SRV02AP07	Application server - ITLink LIS (Laboratorio)	DESARROLLO	ALTA
SRV02AP08	Infrastructure - RDS Servinte	PREPRODUCCION	BAJA
SRV02AP09	Infrastructure - RDS Parametrizacion	PREPRODUCCION	BAJA
SRV02AP10	Application server - SCS Componentes (Capacitación)	PREPRODUCCION	BAJA
SRV02AP11 –	Infrastructure - Farm RDS	PRODUCCION	BAJA

12 – 14 – 19 – 20 – 21 – 24 – 26 – 31 – 34 – 35 – 36			
SRV02AP13	Application Server - SCS COMPONENTES	PRODUCCION	ALTA
SRV02AP15	Infrastructure DataBase – ENTERPRISES	PRODUCCION	ALTA
SRV02AP17	Application server - ITLink LIS (Laboratorio)	PRODUCCION	BAJA
SRV02AP18	Infrastructure DataBase - HDR INFORMIX	PRODUCCION	ALTA
SRV02AP23	Application server - ITLink ADM Capacitación y Preproducción	PREPRODUCCION	ALTA
SRV02AP25	Infrastructure - RDS Farmacia	PRODUCCION	ALTA
SRV02AP27	Application Server - SCS COMPONENTES RIS	PRODUCCION	ALTA
SRV02AP28	Application server - ITLink RIS (Imágenes)	PRODUCCION	ALTA
SRV02AP29	Application Server – MTRA	PRODUCCION	ALTA
SRV02AP30	Infrastructure - Broaker Farm RDS	PRODUCCION	ALTA
SRV02AP32	Application Server - INTERFAZ ENTERPRISES	PRODUCCION	ALTA
SRV02AP33	Application Server - INTERFAZ GASOMETRO	PRODUCCION	ALTA
SRV02AP37	Infrastructure - RDS Back Office	PRODUCCION	ALTA
SRV02AP38	Infrastructure - RDS Parametrizacion	PRODUCCION	ALTA
SRV02AP40	Infrastructure - RDS Servinte Test	PRODUCCION	ALTA
SRV02AP41	Application server - ITLink ADM (Admnistrativo) - BackOffice	PRODUCCION	ALTA
SRV02AP42	Infrastructure DataBase - INFORMIX PURGA	PRODUCCION	ALTA
SRV02AP43	INFORMIX BACKOFFICE	PRODUCCION	ALTA
SRV02BC02	Virtualizaton – HostServer	PRODUCCION	ALTA
SRV02CD01 – 02	Infrastructure - Domain Controller	PRODUCCION	BAJA
SRV02DS01	Application Server - Enterprise	DESARROLLO	MEDIA
SRV02DS04	Application Server - SCS Componentes	DESARROLLO	BAJA
SRV02DS05	Infrastructure DataBase - INFORMIX MANIOBRAS	DESARROLLO	BAJA

SRV02DS07	Application Server - i Route	DESARROLLO	BAJA
SRV02DS08	Infrastructure DataBase - SCS informix Preproduccion	PREPRODUCCION	BAJA
SRV02DS50	Infrastructure DataBase - INFORMIX PRE CHD	DESARROLLO	BAJA
SRV02DS51	Application Server - SCS COMPONENTES CHD	PREPRODUCCION	BAJA
SRV02DS52	Infrastructure - RDS Parametrizacion CHD	DESARROLLO	BAJA
SRV02DS53	Application server - ITLink ADM (Admnistrativo)	DESARROLLO	BAJA
SRV02FS01	Infrastructure - File Server Qnap	PRODUCCION	BAJA
SRV02FS02	Infrastructure - File Server	PRODUCCION	BAJA
SRV02HS05 – 06 – 07 – 08 – 10 – 11 – 12 – 13 – 14	Virtualizaton – HostServer	PRODUCCION	MEDIA
SRV02IT01	Infraestructure - Respaldos	PRODUCCION	ALTA
SRV02IT02	Infraestructure – Synergy	PRODUCCION	ALTA
SRV02IT03	Infraestructure – Avaya	PRODUCCION	ALTA
SRV02IT04	Infraestructure - Respaldos ITCA	PRODUCCION	ALTA
SRV02IT05	Infraestructure – DHCP	PRODUCCION	BAJA
SRV02SS01	Infrastructure - Pinter Server	PRODUCCION	MEDIA

Tabla 2: Servicios según criticidad

2.8. Ancho de banda para el centro de cómputo alterno

Según el estudio realizado, el hospital cuenta con una cantidad de 1400 usuarios, esta cantidad se ve reducida, ya que el DRP se va a centrar solo en una porción critica del centro de datos principal debido a esto la cantidad de usuarios que directamente se conectan a esa porción de red oscila entre 75 y 200, que son los que se mantienen en constante conexión con los servicios que brinda el mismo.

Por lo tanto, debido a la cantidad de servicios y en base al ancho de banda que tienen ellos en la actualidad hemos definido que se necesitará un mínimo de una conexión a internet con una velocidad de 80 Mbps, al igual que una conexión de enlace de datos de la misma velocidad.

2.9. Propuesta para la mejora del centro de cómputo.

Luego de observar, analizar y documentar el estado del centro de cómputo y su red de cableado, se ha planteado una mejora con la cual se asegura que el departamento de IT junto con toda la información procesada en el centro de cómputo, luego de sufrir una catástrofe, vuelva a estar operativo en el mayor tiempo posible.

2.9.1. Diseño

Luego de revisar la información recopilada en el análisis técnico, se identifica que la mejor opción es la implementación de un centro de datos de categoría Internacional, como los que oferta TELCONET CLOUD CENTER I en Guayaquil, los cuales se encuentran a la vanguardia de la tecnología y seguridad en infraestructura, permitiendo garantizar los servicios de Housing que demandan las empresas e instituciones públicas; con esto se prevee asegurar la disponibilidad de información en el centro hospitalario en un 90%. A continuación, en la figura 2.5 se muestra el diseño de la solución general antes mencionado.

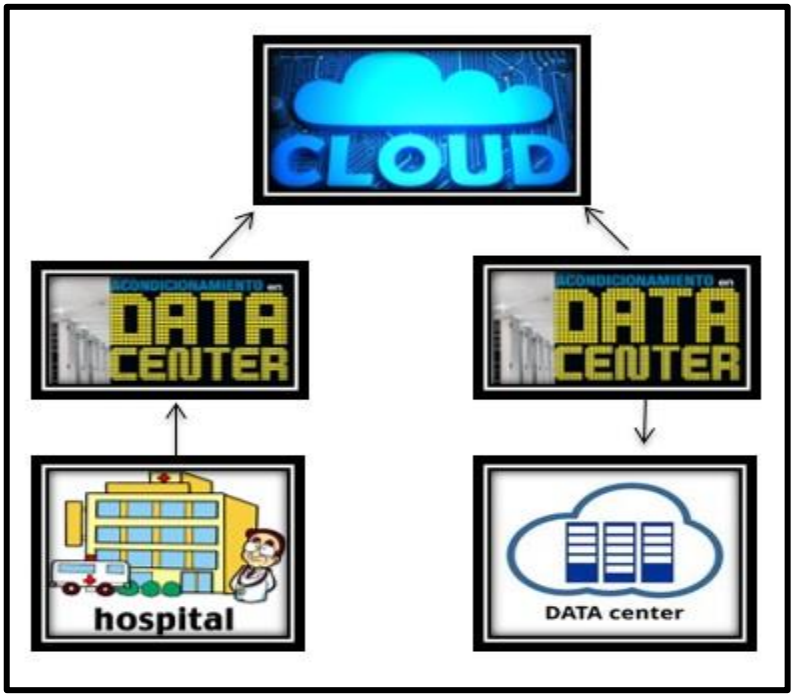

Figura 2.5: Diseño de la solución general.

2.9.2. Esquema físico

Principalmente se deberá contar con una infraestructura de mayor capacidad a la implementada en el centro de cómputo principal con respecto a lo que a sistemas de enfriamiento se refiere y el sistema de cableado que de preferencia sea en piso falso para de esta manera garantizar el correcto funcionamiento, rendimiento y mantenimiento de cada uno de los servicios brindados. Por ello se decide implementar un Storwize V7000 Generación 2, el cual proveerá el almacenamiento a la solución, con un aproximado de 80 Tb de capacidad total, mediante la controladora del Storwize se realizará la configuración de la IP de administración, la cual otorgara acceso vía Web a una interfaz gráfica que permitirá la administración del equipo (para mayor información del STORWIZE consultar el ANEXO 1). Para la conexión del Storwize se utilizarán 2 switches 2498 B24, que a su vez formaran parte de la red SAN, en los que se recomienda el uso del asistente EZSwitchSetup, que es una herramienta de configuración incorporada diseñada para guiar a los usuarios novatos a través de la configuración del switch, a menudo en menos de cinco minutos (para mayor información de los SWITCHES 2498 consultar ANEXO 2). Y 2 switches Catalyst 3750 para la red LAN dentro de los cuales se empleara el uso de la licencia Advanced IP Services, que es ahora incluido en la licencia de servicios IP, esto nos permitirá mayor control de acceso al equipo, así como también mejor administración de rutas para lograr un balanceo de carga óptimo (para mayor información de los SWITCHES CATALYST 3750 consultar ANEXO 3). En cuanto a servidores, se implementará un Bladecenter H, el cual posee la capacidad de instalación de 14 servidores o cuchillas con un nivel alto de procesamiento y entre sus características más relevantes constan:

- Procesadores Intel Xeon E5-2600 v2 de la familia de productos, con hasta 12 núcleos, y 24 hilos simultáneos.
- Cache máximo de 30 MB.

- Memoria (max) 512 GB (32 GB DIMM), 16 zócalos DIMM - VLP registrada ECC DDR3, con soporte de duplicación de memoria.

(Para mayor información del BLADECENTER consultar ANEXO 4).

A continuación, en la figura 2.6 se muestra el diseño propuesto para la implementación de la infraestructura del centro de datos alterno.

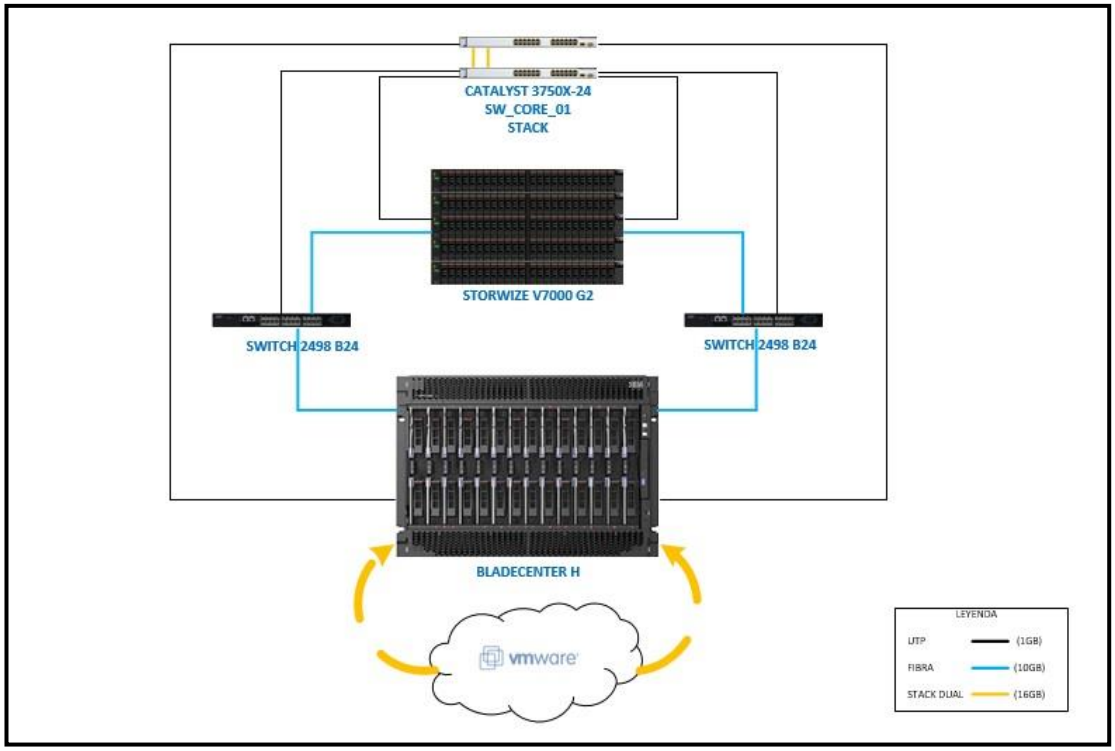

Figura 2.6: Esquema del centro de datos alterno.

2.9.3. Esquema lógico o de direccionamiento

Debido a que la mayoría de los servicios hospitalarios funcionan a través de la interconexión entre servidores, lo que indica que se comunican a través de IP's o nombre de dominio por cada servidor involucrado, se ha determinado que para el direccionamiento de la solución se implementara una VLAN extendida, para de esta manera mantener el direccionamiento IP que actualmente manejan los servicios del sistema hospitalario, una vez activado el Plan de recuperación ante desastres o DRP.

El objetivo de implementar la VLAN extendida es minimizar el impacto al momento de activar el centro de datos alterno como principal.

A continuación, en la tabla 3 se detalla el direccionamiento establecido en el centro de datos alterno.

ESQUEMA DE DIRECCIONAMIENTO IP							
ID	DESCRIPCIÓN	VLAN ID	DEFAULT GATEWAY	MASCARA		RANGO	
						IP MIN	IP MAX
1	Adm_Equipos	30	192.168.30.0	255.255.255.128	25	192.168.30.1	192.168.30.126
2	Produccion	40	192.168.40.0	255.255.255.0	24	192.168.40.1	192.168.40.254
3	Desarrollo	50	192.168.50.0	255.255.255.128	25	192.168.50.1	192.168.50.126
4	Certificacion	60	192.168.60	255.255.255.128	25	102.168.60.1	192.168.60.126

Tabla 3: Esquema de direccionamiento IP

2.9.4. Distribución de equipos en el centro de cómputo alterno.

Finalmente se muestra en la figura 8 el diagrama de distribución de espacio y ubicación de equipos del DRP en el lugar solicitado.

En la figura 2.7 se puede observar la distribución del DRP en el alquiler de un espacio cuyas dimensiones son de tres metro cuadrados, en el fondo en la esquina izquierda con respecto a la puerta de ingreso, en un espacio de 31 x 107 cm. se ubicaran las baterías y al lado con un espaciado de 10 cm. y en una dimensión de 30 x 60 cm. el UPS otorgado por la compañía que nos proveerá el servicio de housing, en la parte central se ubicara en una dimensión de 41 x 200 cm. el dispositivo storwize v7000 de generación 2 y con un espaciado de 1 metro en una dimensión de 61 x 200 cm. se ubicara el rack de servidores SERVINTE el cual estará a cargo de la administración de servicios médicos y las aplicaciones con proveedores externos, seguido de un rack de comunicaciones en una dimensión de 70 x 100 cm. finalmente en la

parte frontal en una dimensión de 70 x 70 cm. se encontraran los tableros eléctricos del sistema.

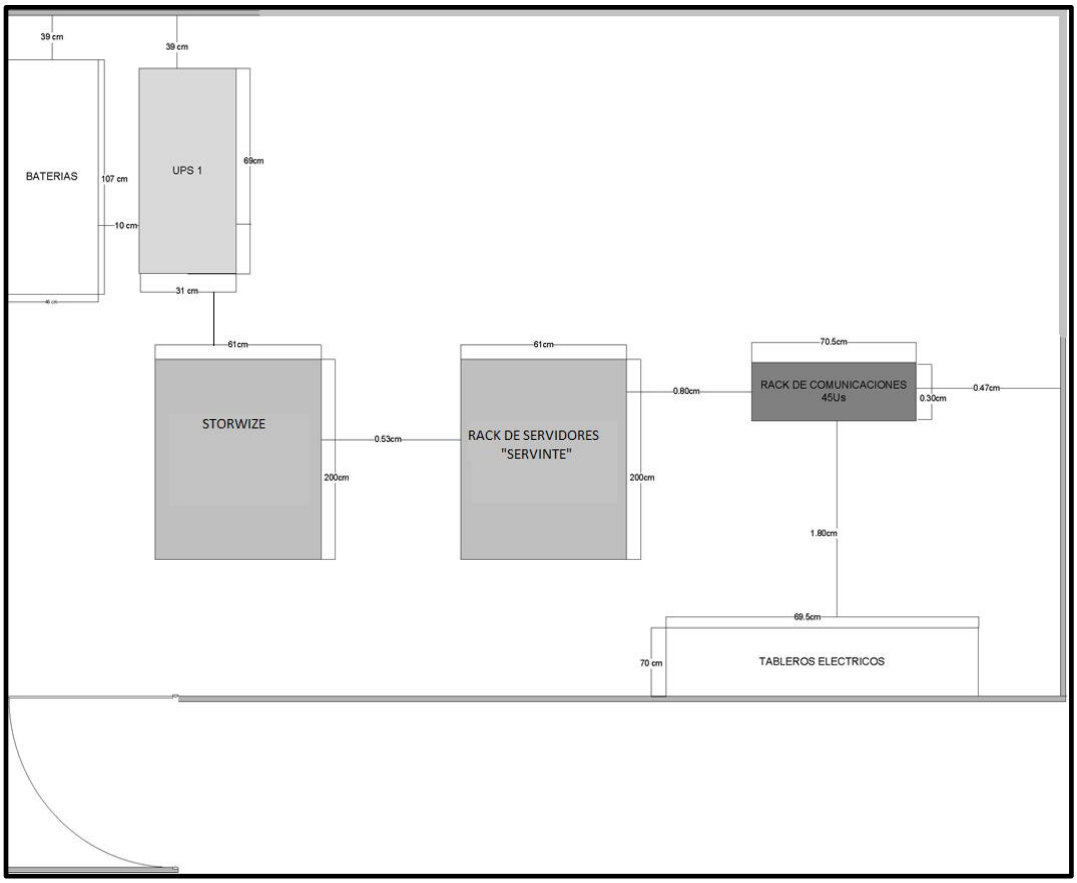

Figura 2.7: Diagrama final de distribución de equipos del DRP.

2.9.5. Alcance

Los planes de recuperación y sus procedimientos correspondientes en caso de desastre son responsabilidad de los departamentos involucrados entre ellos: la gerencia y el departamento técnico.

El plan considera los siguientes aspectos de manera general:

- Restablecimiento de los equipos de infraestructura, los servicios de criticidad alta, que garanticen la operación del hospital.
- Restablecimiento de los servidores virtuales de criticidad alta para el funcionamiento del sistema hospitalario.

CAPÍTULO 3

3. PLAN DE RECUPERACION ANTE DESASTRES.

3.1 Fases del Diseño.

3.1.1 Fase 1

Una vez realizada la recopilación de datos, la detección de las fallas posibles ante diferentes escenarios y el establecer los equipos con características mínimas para poder resolver los problemas, se debe armar un plan de recuperación ante desastres. La ejecución del mismo estará a cargo de cinco miembros del equipo de IT designados por la directiva junto con el jefe de departamento de gestión de riesgos y el jefe del departamento de IT del hospital. Ellos serán escogidos después de un análisis de las habilidades tanto a nivel de pericia, experiencia e instrucción.

3.1.2 Fase 2

Esta fase consiste en la compra y alquiler de bienes que nos servirá para la implementación del nuevo datacenter. En esta fase se procede a gestionar la compra de los equipos con las características previamente establecidas, sobre los cuales se realizará la instalación de la infraestructura contingente para soportar aquellos servicios de mayor criticidad y de esta manera garantizar su disponibilidad. Una vez que al menos se cuente con el 50% de los equipos, se procederá a gestionar el alquiler del espacio físico. Se debe alquilar un espacio debidamente acondicionado y que cumpla con todos los requisitos, permisos y estándares de construcción apropiados para garantizar la seguridad y el correcto funcionamiento de los equipos de red, servidores, etc. Se deberá garantizar control de acceso y medidas de seguridad física por parte del proveedor del centro de datos, en el cual se procederá posteriormente a implementar un sistema de cableado estructurado adecuado de fibra siguiendo los estándares internacionales

correspondientes para lograr la conexión del sistema DRP con el edificio principal de la institución.

De acuerdo con lo investigado para la solución mencionada, es necesario establecer un enlace dedicado con el nuevo datacenter que se encontrara fuera de las instalaciones del hospital. Las empresas CONECEL y TELCONET brindan un servicio completo o de solo renta del espacio físico debidamente adecuado según los requerimientos del contratante y cumpliendo los estándares necesarios para el funcionamiento de dicho sitio, según el estudio realizado se requerirá el alquiler de un espacio de 2 racks para implementar la solución expuesta anteriormente. En este caso hemos realizado el ejercicio con la empresa TELCONET ya que es la empresa que brinda más beneficios incluidos en el alquiler del servicio de housing tales como: mantenimiento y asesoría técnica las 24 horas del día, servicio de vigilancia, cumplimiento de normas de construcción apropiadas, monitoreo adicional del funcionamiento de los equipos.

3.1.3 Fase 3

En la fase tres, se procederá a informar las nuevas características de los equipos adquiridos al personal de IT encargado del DRP. Una vez realizado este procedimiento el personal designado será responsable de la instalación y configuración de los equipos mediante la siguiente planificación:

- Instalación y configuración de infraestructura

1. Instalación de equipos adquiridos.
2. Configuración de equipos adquiridos.

- Configuración de la red de nuevos equipos

1. Validación de cableado estructurado.
2. Validación de redundancia de energía.
3. Conexión y configuración de red LAN en equipos adquiridos.
4. Conexión y configuración de red SAN en equipos adquiridos.

- Configuración de equipos de infraestructura SAN.

1. Configuración de Bladecenter H.
2. Configuración de Storwize V7000 Gen2.
3. Configuración de Fabrics en SAN Switch.
4. Configuración de Blades HS23 (VMware).
5. Configuración de Vcenter (Consola de administración de VMware).

3.1.4 Fase 4

La fase 4 està comprendida por la realización de pruebas en la implementación con el fin de detectar posibles fallas.

- Implementación de laboratorio de pruebas.

1. Definición de servidores a considerar (Desarrollo).
2. Configuración de réplica entre Storages.
3. Validación del procedimiento DRP a nivel de servidores.

- Implementación Global de DRP

1. Definición de servidores a considerar en DRP (Producción).
2. Configuración de réplica entre Storages.
3. Validación del procedimiento DRP a nivel de infraestructura.

Los miembros del personal de IT designados como responsable del DRP deberán contar con información actualizada sobre el estado actual de la red central del hospital para que, en caso de presentarse algún incidente, el personal de IT pueda analizar la situación, determinar la magnitud del problema o posible desastre y si hay alguna posibilidad de resolverlo sin que se vea afectada la operatividad de la red a gran escala, de esta manera se evitaran posibles falsas alarmas y activaciones innecesarias del sistema DRP.

3.1.5 Fase 5

Tomando en cuenta los diferentes escenarios posibles que se pueden presentar, tales como:

- Catástrofes.
- Incendios.

- Fallos en el suministro eléctrico.
- Ataques terroristas.
- Interrupciones organizadas o deliberadas.
- Sistema y/o fallos del equipo.
- Error humano.
- Virus y ataques informáticos.

El datacenter principal cuenta con la replicación de datos, la misma que le permite realizar la copia de datos entre storages. Esta característica será aprovecha en el DRP para garantizar la disponibilidad de la información en ambos sitios.

Para iniciar la activación del DRP, es decir habilitar el centro de cómputo secundario como principal se deberá seguir los siguientes pasos:

1. El comité de desastres del Hospital deberá determinar si se activa o no el DRP ante un incidente registrado. Es decir que solo el comité tendrá la potestad de determinar la habilitación del DRP.
2. Una vez obtenida la aprobación de habilitación del DRP, se detendrá la copia de datos entre los storage, para de esta manera evitar que la misma se corrompa por el corte abrupto ocurrido.
3. Se presentarán los últimos datos copiados en el storage ubicado en el centro de cómputo alterno hacia los servidores o cuchillas físicas del Bladecenter, los datos no deberán superar la pérdida de 15 minutos de información según lo establecido.
4. Se iniciarán las máquinas virtuales según el orden de criticidad establecido y se procederá a validar el funcionamiento respectivo del sistema operativo y de las aplicaciones o servicios que brinde cada uno de los mismos.
5. Una vez validados los servicios, se dará aviso al comité de desastres del Hospital para que aprueben la activación normal de las actividades.

3.1.6 Fase 6

Para iniciar la reactivación del centro de cómputo principal, es decir regresar al sitio de operación original. Se deberá ejecutar los siguientes pasos:

1. El comité de desastres del Hospital deberá confirmar que el sitio principal se encuentra en óptimas condiciones para reactivar la operación en el sitio original.
2. Una vez obtenida la aprobación de la reactivación del centro de cómputo principal, se reiniciará la copia de datos entre los storage, para de esta manera asegurar la información en el sitio principal.
3. Se presentarán los últimos datos copiados en el storage ubicado en el centro de cómputo principal hacia los servidores o cuchillas físicas del Bladecenter, los datos no deberán superar la pérdida de 15 minutos de información según lo establecido.
4. Se iniciarán las máquinas virtuales según el orden de criticidad establecido y se procederá a validar el funcionamiento respectivo del sistema operativo y de las aplicaciones o servicios que brinde cada uno de los mismos.
5. Una vez validados los servicios, se dará aviso al comité de desastres del Hospital para que aprueben la activación normal de las actividades.

3.2 Responsabilidades de la institución

Como parte de las responsabilidades y consideraciones a tomar por parte de la institución, se identifica lo siguiente:

- **Aplicaciones o servicios del sistema hospitalario.**

1. Redactar la carta de aceptación de servicios a involucrar en el DRP.
2. Entregar documentación de recuperación de desastres.
3. Mantener actualizada la información de los servicios que ofrece el hospital (inventarios).
4. Mantener actualizado el plan de recuperación de desastres, basados en el inventario realizado en el punto anterior.

- **Almacenamiento de respaldos**

1. Mejorar el lugar de almacenamiento y rotulado de respaldos diarios y mensuales.
2. Confirmar que el respaldo de información vital para el negocio se esté almacenando adecuadamente.
3. Realizar pruebas periódicas de restauración, para validar la integridad de la información.
4. Gestionar la copia de respaldos en cinta y establecer una estrategia para el almacenamiento de estas en un lugar alterno.

- **Actividades de respuesta**

1. Agregar números telefónicos de las personas responsables del dentro de datos.
2. Incluir lista de chequeo de tareas en el procedimiento de recuperación de desastre.

- **Actividades de reanudación**

1. Los números de teléfono de domicilio del personal de ITS necesitan ser incluidos.
2. Coordinar con el proveedor de enlace de datos e internet la creación de una estrategia de recuperación definida para la restauración inmediata de enrutadores y conmutadores del Hospital.

- **Procedimientos**

1. Verificar la existencia del procedimiento de control interno en el Hospital.
2. Verificar la existencia de un manual de emergencias en el Hospital.

- **Capacitaciones periódicas al personal**

1. Informar acerca de la existencia del manual de contingencia.
2. Capacitación constante al personal sobre las evacuaciones y seguridad.
3. Incentivar al personal e informar mediante folletos, volantes, evacuaciones y evaluaciones sobre qué hacer en caso de desastres.

3.3 Propuesta Económica.

A continuación, en la tabla 4 se detalla la proforma de la infraestructura involucrada en el centro de datos alterno.

PROFORMA			
DESCRIPCION	PRECIO UNITARIO	CANTIDAD	TOTAL
Cisco WS-C3750V2-24PS-E 3750V2 Series Catalyst Switch	2513,00	2	5.026,00
Switch IBM 2498-B24	3800,00	2	7.600,00
Storwize v7000 gen2 tipo 2076 modelo 5024 + caja de expansion 48x v7000 gen2 modelo 2076	16500,00	1	16.500,00
Controladora Storwize v7000 gen2	1695,00	1	1.695,00
Discos de 10000 rpm, 900 gb	766,00	32	24.512,00
Bladecenter H tipo 8852 modelo hc1 chasis	12500,00	1	12.500,00
Cuchillas HS23 tipo 7875 modelo ac1 2 X 2.4GHZ E5-2609, 64GB Ram, 2x 500GB 7.2k	2000,00	14	28.000,00
SWITCHES INTERNOS (BLADECENTER)			
Switch SAN Brocade 300 BR-320-0008 24 puertos	1650,00	2	3.300,00
Switch LAN Ibm Cisco Nexus 4001i n4k-4001i-xpx	2000,00	2	4.000,00

Cable utp cat 6 de 2 metros	5,50	10	55,00
Cable de Fibra Optica 3mt multimodo om4	9,00	14	126,00
Cable de Fibra Optica 2mt multimodo om4	8,00	8	64,00
Licencias VMware vsphere 5 estándar	995,00	28	27.860,00
VMware vcenter 5 standar	4995,00	1	4.995,00
Servicio de mantenimiento mensual			280,00
Servicio de implementacion			2.000,00
Alquiler de servicio de Housing, 2 racks incluidos por mes			400,00
PRECIOS VALIDOS POR 6 MESES		SUBTOTAL	138.913,00
		14 % IVA	19.447,82
		TOTAL	158.360,82

Tabla 4: Proforma de equipos necesarios para la implementación del DRP.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

A raíz de las visitas técnicas al hospital se ha podido concluir que es necesario contar siempre con un enlace alterno dedicado para la comunicación con cualquier entorno de respaldo con el que se vaya a contar.

Se pudo observar que actualmente el hospital no cuenta con las debidas actualizaciones tanto en software como en hardware, por lo que, no se está haciendo uso de herramientas de replicación constante y segura como las que posee VMWare.

Se pudo constatar que el hospital actualmente no cuenta con la infraestructura necesaria para un DRP, ni tampoco con un personal capacitado de forma óptima para el manejo adecuado de los recursos informáticos actuales que posee la institución.

Recomendaciones

Finalmente, como resultado del estudio realizado podemos realizar las siguientes recomendaciones:

Adoptar las guías realizadas en el presente trabajo dentro de la institución hospitalaria, en el departamento de infraestructura para solventar los riesgos presentados durante un desastre.

El jefe del área de IT, siempre debe realizar campañas informativas sobre el plan de contingencia, y capacitaciones sobre evacuaciones y seguridad, al personal médico y empleados en general.

Realizar una prueba anual del prototipo del Plan de Recuperación de Desastres (DRP) y actualizarlo permanentemente, de forma que se pueda corregir errores que puedan presentarse.

Realizar simulacros de falla a nivel de servidores para validar la consistencia de los respaldos y entrenamiento de personal.

BIBLIOGRAFÍA

[1] Susan Snedaker, *Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Edition.* Estados Unidos: Syngress, 2013.

[2] Jon Tate, Massimo Rosati, Morten Dannemand, Nancy Kinney,Lev Sturmer, *Implementing the IBM Storwize V7000 Gen2,* Estados Unidos: IBM Redbooks, 2016.

[3] Información de sistemas eléctricos [Online]. Available:

http://electronica-teoriaypractica.com/como-funciona-un-sai-o-ups/.

[4] El análisis de criticidad [Online]. Available:

http://bibing.us.es/proyectos/abreproy/5311/fichero/5-+Analisis+de+criticidad.pdf

[5] Bryan C. Martin, *Disaster Recovery Plan Strategies and Processes*, 2002 [Online]. Available:

https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564

ANEXOS

Anexo 1

http://www.ibm.com/connect/ibm/attachments/V820078E43406L36/IBM_Storwize_V7000_and_Storwize_V7000_Unified_Disk_Systems_Data_Sheet.pdf

Anexo 2

http://www-03.ibm.com/systems/ph/resources/storage_san_b-type_san24b-4_express_TSD03041USEN.PDF

Anexo3

http://www.andovercg.com/datasheets/cisco-faq_c3750_Public1.pdf

Anexo 4

http://www-01.ibm.com/common/ssi/rep_ca/8/897/ENUS109-438/ENUS109-438.PDF

Anexo 5

http://www.standard.no/pagefiles/961/z-008.pdf