DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ELECTRÓNICO EN TELECOMUNICACIONES

TEMA: ANÁLISIS Y ELABORACIÓN DE UN PLAN DE CONTINGENCIA DE LOS SERVICIOS IT DE LA EMPRESA GRUPO EL COMERCIO C.A. E IMPLEMENTACION DE UN SERVIDOR TIPO NAS PARA GARANTIZAR LA CONTINUIDAD DEL NEGOCIO

AUTOR: VILLACÍS BORJA JUAN CARLOS

DIRECTOR: ING. ROMERO GALLARDO CARLOS GABRIEL

SANGOLQUÍ

2016

CERTIFICACIÓN

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"ANÁLISIS Y ELABORACIÓN DE UN PLAN DE CONTINGENCIA DE LOS SERVICIOS IT DE LA EMPRESA GRUPO EL COMERCIO C.A. E IMPLEMENTACION DE UN SERVIDOR TIPO NAS PARA GARANTIZAR LA CONTINUIDAD DEL NEGOCIO"** realizado por el señor **JUAN CARLOS VILLACÍS BORJA**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor **JUAN CARLOS VILLACÍS BORJA** para que lo sustente públicamente.

Sangolquí, 28 de Enero del 2016

Ing. Carlos Romero Gallardo
DIRECTOR

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, ***JUAN CARLOS VILLACÍS BORJA***, con cédula de identidad N° **1717114753**, declaro que este trabajo de titulación "***ANÁLISIS Y ELABORACIÓN DE UN PLAN DE CONTINGENCIA DE LOS SERVICIOS IT DE LA EMPRESA GRUPO EL COMERCIO C.A. E IMPLEMENTACION DE UN SERVIDOR TIPO NAS PARA GARANTIZAR LA CONTINUIDAD DEL NEGOCIO***" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 28 de Enero del 2016

JUAN CARLOS VILLACÍS BORJA

C.C. 1717114753

AUTORIZACIÓN

DEPARTAMENTO DE ELECTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, ***JUAN CARLOS VILLACIS BORJA***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"ANÁLISIS Y ELABORACIÓN DE UN PLAN DE CONTINGENCIA DE LOS SERVICIOS IT DE LA EMPRESA GRUPO EL COMERCIO C.A. E IMPLEMENTACION DE UN SERVIDOR TIPO NAS PARA GARANTIZAR LA CONTINUIDAD DEL NEGOCIO"*** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 28 de Enero del 2016

JUAN CARLOS VILLACÍS BORJA

C.C. 1717114753

DEDICATORIA

Dedico este proyecto a mis padres, este es el fruto de su trabajo, sacrificio y abnegación, espero seguir siendo un motivo de su orgullo.

A mis hermanos que han sido parte fundamental en mi vida. Espero ser siempre un ejemplo para ustedes.

A mi esposa que fue quien me ayudó desde el primer momento que vivimos juntos, esta es la recompensa a tu sacrificio.

A mis hijas, que han sido mi motor y que espero ser su orgullo y ejemplo durante toda su vida.

A toda mi familia que siempre confiaron en mí y me dieron su apoyo.

AGRADECIMIENTO

Agradezco a mis padres Juan y Yolanda, por brindarme el apoyo necesario en mi vida estudiantil para poder cumplir mis metas y objetivos. Gracias a sus consejos, paciencia y dedicación he logrado encaminarme por un camino de éxito y de bien. A mis hermanos Xiomara y Bryan, que siempre estuvieron a mi lado alentándome para conseguir mis triunfos y a quienes deseo que cumplan sus metas y alcancen logros importantes. A mis abuelitos que siempre con sus sabias palabras me han hecho sentir una persona ganadora.

A mi esposa Tamara Brito que siempre estuvo conmigo en los malos y buenos momentos, quien ha sido mi compañera incondicional. Gracias por tu paciencia y sobre todo por empujarme a alcanzar este objetivo, sin tu apoyo nada de esto fuera posible.

A mis hijas Desirée y Martina quienes han sido mi fuente de inspiración para alcanzar mis objetivos y poder ser un ejemplo en su vida.

A mis amigos que estuvieron a mi lado durante todo este proceso, en especial a Ricardo (+) quien con sus palabras y consejos me ayudaron a no desmayar jamás.

A mis profesores por compartirme sus conocimientos y ser mis guías durante mi carrera. Mi infinito agradecimiento al Ing. Carlos Romero e Ing. Fabián Sáenz quienes han sido los artífices de poder alcanzar mi sueño.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente proyecto de titulación propone la elaboración del Plan de Contingencia de los servicios IT de la empresa Grupo El Comercio C.A. para garantizar el negocio. Como fase inicial, se implementa un servidor tipo NAS para migrar información crítica que se encuentra en un servidor obsoleto. Para el desarrollo del proyecto, se incluye una breve descripción de la empresa y se definen los objetivos y el alcance del proyecto, que sirven como lineamientos iniciales para la elaboración. Antes de elaborar el plan de contingencia y como punto inicial se realizar la implementación del servidor NAS, en el cual se migra información importante correspondiente al sistema editorial e información de las distintas Gerencias de la compañía. Para iniciar el diseño del Plan de Contingencia enfocado al Departamento de Tecnología se realiza un levantamiento de información de los sistemas y servicios implementados en la empresa, se evalúa los posibles riesgos y amenazas a la que está expuesta, se determinan los sistemas, aplicaciones y recursos de TI que abarcan los procesos críticos y acto seguido se determina el tiempo máximo que un proceso puede estar fuera de servicio sin que afecte significativamente al negocio. Se proponen medidas de prevención y control de riesgos para definir las estrategias de continuidad, estableciendo las opciones de recuperación y el flujo que se sigue ante un problema. Una vez culminada las etapas del plan se definen un conjunto de equipos para el restablecimiento de operaciones y los procedimientos que los mismos necesitan para dar continuidad al negocio, finalmente se da a conocer las conclusiones y recomendaciones del trabajo desarrollado.

Palabras claves:

- Contingencia
- NAS
- Migración
- Servidor
- Riesgos

ABSTRACT

The present project titling proposes the development of Contingency Plan for IT services of the company Grupo El Comercio C.A. to ensure the business. As an initial phase is implemented a server type NAS to migrate critical information that is located on a server obsolete. For the development of the project, includes a brief description of the company and defines the objectives and scope of the project, which is used as initial guidelines for the preparation. Before drawing up the contingency plan and as a starting point to NAS server deployment, which migrates important information corresponding to the editorial system and information of the different Managements of the company. To start the design of the Contingency Plan focused on the Department of Technology is carried out a survey of information systems and services implemented in the company, it evaluates potential risks and threats to which it is exposed, it evaluates potential risks and threats to which it is exposed, determine the systems, applications and IT resources covering the critical processes and then determines the maximum time that a process can be taken out of service without that significantly affects the business. Propose certain measures of prevention and control of risks to define the strategies of continuity, setting out the options for recovery and flow that is still in the face of a problem. Once culminated the stages of the contingency plan was defined a set of equipment for the restoration of operations and procedures to give continuity to the business, finally is given to know the conclusions and recommendations of the work developed.

Keywords:

- Contingency
- NAS
- Migration
- Server
- Risks

CAPITULO I

ESTUDIO GENERAL DEL PROYECTO

1.1. Estudio General de la Empresa

Grupo el Comercio nace con la creación del diario EL COMERCIO, el cual fue fundado por los hermanos César y Carlos Mantilla Jácome, como diario independiente, el 1 de enero de 1906. Actualmente efectúa sus actividades de difusión y medios en tres grandes segmentos: Medios Impresos, Impresión comercial y Digital. Sus más reconocidas empresas y productos son Radio Platinum, Radio Quito, revista Líderes, revista Familia, Ultimas Noticias, Diario el Comercio entre otros.

1.1.1. Misión:

Como misión la empresa contribuye al desarrollo del país, mediante contenidos de valor para las distintas audiencias y soluciones de comunicación para los anunciantes. (Grupo El Comercio C.A, 2012)

1.1.2. Visión:

La visión de la empresa es ser la mejor en medios de comunicación del país, focalizando siempre en el desarrollo, innovación, crecimiento, rentabilidad y brindando oportunidades de desarrollo a su gente, sin descuidar la calidad.

1.1.3. Valores:

- Innovación
- Independencia
- Integridad
- Calidad

1.1.4. Organigrama

La estructura de GEC es un sistema de engranajes, en la que cada área y colaborador de la empresa cumple un rol importante. Sin el aporte y esfuerzo, no se obtendría los mismos resultados de calidad y excelencia (ver figura 1).

Figura 1 Organigrama

Fuente: (Grupo El Comercio C.A, 2012)

1.1.5. Portafolio

Grupo El Comercio consta con un amplio portafolio de productos, los cuales se dividen en 3 grandes grupos.

- **Medios Impresos**

El objetivo central de esta división es producir y vender contenidos impresos bajo marcas cuidadosamente administradas por el Grupo, los cuales son producidos con altos estándares de calidad y profesionalismo que están dirigidos a las diversas audiencias, las que, a su vez, obedecen a un mercado específico de anunciantes.

- **Impresión Comercial**

Grupo El Comercio ofrece soluciones globales de impresión de alta calidad para los clientes de los sectores privado y público del país. Adicionalmente, se enfoca en la impresión de libros para las casas editoriales que proveen materiales didácticos y educativos para el mercado latinoamericano, este servicio se logra con la prensa Manroland Uniset de última generación.

- **Digital**

Desarrolla alternativas de solución de contenido multimedia, acorde con los nuevos requerimientos del exigente mercado. Forman parte de esta división de negocio las ediciones digitales de los distintos productos del Grupo, los servicios de noticias SMS, los nuevos portales de clasificados por Internet y el servicio de e-mailing.

1.2. Antecedentes

A la velocidad con la que operan los negocios actuales un incidente de unas pocas horas de duración puede tener un impacto catastrófico en los resultados y en la imagen de la organización que lo sufra.

Hoy por hoy, la información es uno de los principales activos que la empresa debe cautelar mediante el desarrollo de un plan de contingencia, que permita el adecuado funcionamiento del negocio frente a un cese prolongado del servicio informático.

La alta dirección debe tomar conciencia que el desarrollo y la implantación de planes de contingencia comprende toda la organización, pues se trata de una situación de negocios y no puramente informática. Cualquier compañía está sujeta a sufrir un incidente que afecte a su continuidad, teniendo consecuencias más o menos graves, dependiendo de la forma en que se gestione el evento.
A medida que más y más sistemas envuelven procesos distribuidos y comunicación de datos a través de redes en su operación, la utilización de nuevos avances tecnológicos es más deseada. Estos avances pueden ser a través de todo el sistema, un protocolo en específico, un servicio, arquitecturas o topologías de red, o simplemente en cualquier otra área. Las comunicaciones y las redes se han convertido en consideraciones importantes y han incrementado su importancia en el proceso de decisiones para llevar a cabo la migración de servidores.

Los servidores de almacenamiento son equipos muy delicados, necesitan mucho trabajo después de la instalación, es necesario ponerles seguridad y darles los permisos adecuados para que se pueda trabajar con los datos que se coloquen en éstos.
Siempre que se instale un servidor hay que estar conscientes que tarde o temprano habrá que reemplazarlo, ya sea por daño o por obsolescencia, por esta razón se debe estar preparados para estos casos. (InfoWorld, 2008)

En cuanto al proceso de migración, este, no solo implica el reemplazo de software, sino también la funcionalidad, es decir que el usuario cuente con las mismas o mejores formas de llevar a cabo una tarea determinada. Se puede decir

que un objetivo importante de la migración es dar el menor impacto al usuario, para que el cambio de tecnología no sea un proceso engorroso y tedioso.

El modelo tradicional de almacenamiento de datos genera una serie de problemas de administración, genera lo que se denomina “redundancia”, es decir, la existencia no deseada e innecesaria de copias de un mismo archivo en varios servidores. La existencia de archivos duplicados resta eficacia y dificulta las tareas de colaboración y administración de la información. Además, cuando los datos se almacenan en los servidores de la red LAN, el tráfico derivado de las operaciones de copia de seguridad colapsa los recursos de dicha red.
Este modelo presenta un último problema que consiste en que los servidores no pueden compartir datos de distintas plataformas, ya que un sistema de archivos (por ejemplo, NTFS) no puede leer los datos de otro sistema de archivos diferente (como Unix). Existen algunas aplicaciones de terceras marcas que pueden realizar la conversión entre sistemas de archivos, pero son difíciles de utilizar. Por ello, el modelo tradicional de almacenamiento en servidores tiende a desaprovechar valiosos recursos y obliga a los administradores a dedicar más tiempo al reparto de la carga de almacenamiento, a tareas de administración para eliminar la redundancia y a la supresión de cuellos de botella. (Iamateche, 2014)

Es por eso que se ha visto la solución en instalar un sistema NAS el cual es un servidor destinado exclusivamente al almacenamiento de datos (es decir, un array de almacenamiento) que se conecta a la red. Los clientes envían las peticiones de archivos directamente al dispositivo NAS, evitando así a los servidores destinados a fines generales de la red.

1.3. Justificación e importancia

Actualmente la Empresa Grupo El Comercio posee varias aplicaciones, servidores y servicios críticos por lo que es indispensable elaborar un plan de contingencia de los servicios TI para garantizar la continuidad del negocio y así

estar preparados ante algún acontecimiento que ponga en riesgo el servicio hacia los clientes.

El fin de este plan es permitir el normal funcionamiento de los servicios que ofrece la empresa, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo.

Con la implementación de un nuevo Sistema Editorial varios servidores pasaron a ser críticos, dentro de ellos se encuentra el File Server denominado “Preprensa”. Hay que tomar en cuenta que este servidor se encuentra obsoleto y sin garantía por lo que tiene más probabilidades a tener fallas.

Hoy en día el modelo tradicional de almacenamiento de datos genera una serie de problemas. Hasta hace unos años, la única solución de almacenamiento disponible consistía en la conexión directa de un medio de almacenamiento (disco duro, array RAID, cinta, disco óptico) a un servidor que procesaba todas las peticiones de archivos que le enviaban los clientes.

Este modelo genera una serie de problemas de administración. En primer lugar, no utiliza los recursos de forma eficaz, ya que el espacio de almacenamiento se encuentra en compartimentos estancos (espacios delimitados, cerrados e incomunicados). Puede ocurrir, así, que un servidor se quede sin espacio de almacenamiento, mientras que otro disponga de 100 GB de espacio libre en disco, es decir la información tiende a almacenarse de una forma descontrolada. Normalmente la opción más sencilla y rápida es ampliar el número de discos en los servidores, pero en muchas ocasiones esta opción no es técnicamente viable. La mejor opción pasa por analizar como tratamos nuestra información y cuál es el ciclo de vida que tiene. De esta forma nos daremos cuenta que, de toda la información que tenemos solo una parte la podemos considerar activa, el resto tiene un tratamiento histórico. (Grass Valley, 2014)

Así viendo las necesidades que posee Grupo El Comercio por el gran crecimiento de la Data en el servidor Preprensa, el mal manejo de las cuotas, la

velocidad de respuesta, la tecnología antigua del servidor y sobre todo porque dicho equipo se ha convertido en crítico porque almacena información importante del periódico y de los distintos productos que la empresa ofrece, es por esto que se busca conseguir una solución factible que cumpla todas las necesidades de los clientes (empleados de la empresa) y de los administradores de los sistemas (Departamento de Tecnología – Área Infraestructura & Operaciones).

En este caso las opciones que se plantearon en un inicio fueron dos:

Añadir un segundo servidor, lo cual era correcto, pero de alto costo económico y elevada gestión. Al añadir o sustituir un servidor no se tiene una previsión de crecimiento de datos correcta es posible que en un plazo relativamente corto tengamos el mismo problema, lo cual no parece una opción ideal.

Añadir discos externos, tipo USB, lo cual era incorrecto, pero de bajo costo y nula gestión. Si se añade discos duros externos como alternativa de almacenaje de información se tendrá graves problemas. La administración de este recurso no estará centralizada, su seguridad será nula ante fallos físicos y posiblemente no esté incluido en la política de copias de seguridad lo cual no viene a ser una opción recomendable.

Al ver estos inconvenientes se realizó una investigación en el mercado y se optó por implementar un sistema NAS (Network Attached Storage).

Un dispositivo NAS es un servidor destinado exclusivamente al almacenamiento de datos (es decir, un array de almacenamiento) que se conecta a la red. Tiene una gestión mínima y se integra con la administración del sistema operativo.

A diferencia del almacenamiento de conexión directa (servidores) que tiene la capacidad de ampliación limitada, un sistema NAS tiene una mayor capacidad de ampliación, flexibilidad y seguridad. Tiene el costo de propiedad más bajo de todos los sistemas de almacenamiento, además soporta todas las tecnologías actuales de discos, así como sus sistemas de seguridad. Otra gran ventaja de

este sistema es que podemos tener tantos dispositivos NAS como necesidades tengamos. (Fourdtech, 2014)

Para realizar el proceso de migración existen distintas posibilidades, por ello es indispensable conocer cuáles se adaptan a nuestras necesidades en particular. Si bien podría recurrirse a una sola estrategia, es preferible la combinación de varias alternativas para adaptarse a las necesidades reales de un departamento. Sin embargo, a pesar que se use la mezcla de estrategias de migración, no se debe perder el enfoque o visión general.

El objetivo de este proyecto de grado es desarrollar un plan de contingencia de los servicios TI de la empresa Grupo El Comercio para garantizar la continuidad del negocio, además se implementará un servidor Tipo NAS para realizar la migración de la Data del File Server del Sistema Editorial debido a que el actual es un servidor obsoleto, de tecnología antigua y sin garantía.

Con este plan se garantizará poder actuar ante una emergencia que se presente en los servidores que brindan servicios tales como Sistema Editorial, ERP, Aplicaciones Web, Aplicaciones para Ipad y todas las aplicaciones que de una u otra forma son parte importante parar el funcionamiento diario de la empresa y el negocio. Además, y no más importante los servidores de archivos de: Gerentes, Redacción, Videografía, Multimedia, Fotografía, RRHH, Auditoria, Prensa, Ventas, Tecnología, Repositorio de Linux, entre otros.

Con todo esto se tendrá un mejor control, una mejor administración de los servicios y lo más importante se podrá estar preparados ante alguna emergencia que ponga en riesgo la continuidad del negocio de la Empresa.

1.4. Alcance del Proyecto.

El presente proyecto contempla analizar los problemas que se están presentando en la actualidad y que se podrán presentar a futuro, poniendo en riesgo los servicios que ofrece Grupo El Comercio.

Como paso inicial para evitar posibles fallas del file_server denominado Preprensa se realizó la compra de un servidor Tipo NAS de alto rendimiento con hardware de última generación, el cual dispone de mayor capacidad de espacio, más inteligencia para satisfacer las necesidades de las aplicaciones, de los administradores del centro de datos y facilidad a la hora de brindar soporte. Este servidor se configurará e implementará en el Datacenter de Grupo El Comercio con Windows 2008 Storage Server, así, se busca optimizar el rendimiento, la seguridad, garantizar un consumo más eficiente de la energía, etc.

Otro punto importante y necesario en el desarrollo de este proyecto es que se realizará la migración y sincronización de la Data del servidor de archivos mencionado sin afectación a los usuarios en el servicio, servidor que al momento es crítico por la data que contiene siendo indispensable para el Sistema Editorial y punto inicial para que las ediciones de cada producto sean vistas en los dispositivos android. Actualmente este equipo es de tecnología antigua, sin garantía y que no cumplen con las necesidades de los usuarios en cuanto a la velocidad de respuesta y espacio de almacenamiento. Una vez que se encuentre sincronizada la Data del servidor obsoleto a la NAS se pondrá en producción el nuevo equipo.

A partir de esto se desarrollará un Plan de Contingencia de los servicios TI (Sistema Editorial, servidores de archivos, aplicaciones web y aplicaciones internas de la empresa) para garantizar la continuidad del negocio siguiendo los estándares ISO 27001 y las mejores prácticas de ITIL en su tercera versión, lo

cual viene a ser un conjunto de actividades que buscan definir y cumplir metas que permita al Departamento de Tecnología controlar el riesgo asociado a una contingencia.

Este plan estará orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en previsión de desastres.

Con esto se busca cubrir las necesidades que posee Grupo El Comercio y en especial brindar un mejor servicio a todo el personal que labora en esta Empresa.

1.5. Objetivos

1.5.1. General

Desarrollar un Plan de Contingencia de los servicios IT de la Empresa Grupo El Comercio C.A. e implementar un servidor tipo NAS para garantizar la continuidad del negocio.

1.5.2. Específicos.

- Describir las necesidades que tiene la empresa Grupo El Comercio en Infraestructura detallando los aspectos generales del proyecto para solventar dichas problemáticas.
- Definir un marco teórico con una orientación al desarrollo de un plan de contingencia, a la migración de servidores File_server y a la implementación de un servidor Tipo NAS, además de información del Sistema Operativo que puede soportar el nuevo equipo.
- Realizar un estudio de la situación actual, los problemas que están teniendo los usuarios y evaluar los posibles riesgos.
- Analizar el nuevo sistema a implementar detallando sus beneficios, ventajas que presentarán hacia los usuarios finales y los costos a invertir para poner en funcionamiento la nueva infraestructura.

- Armar, configurar e implementar el nuevo servidor tipo NAS en el Datacenter de Grupo El Comercio.
- Realizar la migración de la data del servidor Preprensa hacia el nuevo equipo NAS para poner en producción y brindar una mejor respuesta del servicio.
- Elaborar el plan de contingencia de los servicios IT que presta GEC basándose en las normas ISO 27000 e ITIL V3.
- Generar políticas de respaldo haciendo uso de la librería HP StorageWorks MSL4048 y de la herramienta Data Protector Manager.
- Realizar las respectivas pruebas de funcionamiento del nuevo servidor y verificar el impacto que tuvo este cambio hacia los usuarios finales.
- Realizar pruebas de funcionamiento del Plan de contingencia elaborado simulando situaciones de emergencia.
- Concluir los resultados obtenidos en esta tesis para así poner énfasis en proyectos futuros relacionados a este tema.

1.6. Metodología

El diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; debida a que se necesita de esfuerzos y gastos considerables, sobre todo si se está partiendo de cero.

Hay que tener presente que mucho dependerá de la Infraestructura TI de la empresa y de los servicios que esta ofrezca para determinar un modelo de desarrollo de plan, en donde se darán los puntos más importantes a tener en cuenta para realizar un método estructurado que ayude a asegurar que se toman en cuenta todos los factores y que se les trata adecuadamente.

La metodología que se empleará para el desarrollo del plan de contingencias de los sistemas de información, tiene ocho fases, siguiendo la experiencia lograda por instituciones de renombre como el INEI, las cuales se puede resumir de la siguiente manera:

- **Planificación:** preparación y aprobación de esfuerzos y costos.
- **Identificación de riesgos:** funciones y flujos del proceso de la empresa.
- **Identificación de soluciones:** Evaluación de Riesgos de fallas o interrupciones.
- **Estrategias:** Otras opciones, soluciones alternativas, procedimientos manuales.
- **Documentación del proceso:** Creación de un manual del proceso.
- **Realización de pruebas:** selección de casos soluciones que probablemente funcionen.
- **Implementación:** creación de las soluciones requeridas, documentación de los casos.
- **Monitoreo**: Probar nuevas soluciones o validar los casos.

CAPITULO II

DESCRIPCION DEL MARCO TEORICO

2.1. Plan de Contingencia TI

2.1.1. Introducción

Dentro de la Gestión y Administración de la infraestructura tecnológica y la Seguridad de la Información en una empresa es importante contar con un plan alternativo con el fin de asegurar la continuidad de un negocio en caso de que ocurran incidentes graves.

Hoy en día las organizaciones dependen más y más de la tecnología, lo cual se ha convertido en un componente clave e importante de la mayor parte de los procesos de negocio, la disponibilidad de los servicios TI es imprescindible para su supervivencia.
Los planes de Contingencia siempre han sido vinculados a empresas grandes e importantes que necesitan reaccionar de forma inmediata ante cualquier evento que interrumpa sus servicios, pero la realidad es que cualquier empresa puede sufrir un incidente que afecte a su continuidad y, dependiendo de la forma en que se gestione dicho incidente, las consecuencias pueden ser más o menos graves.

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes de la Organización, es el fundamento más importante de este Plan de Contingencia. Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, es necesario que El Plan de Contingencia

Informático incluya el Plan de Recuperación de Desastres con el único objetivo de restaurar el Servicio Informático en forma rápida, eficiente, con el menor costo y perdidas posibles

2.1.2. ¿Qué es un Plan de Contingencia TI?

Un plan de contingencia TI es una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.
Los servicios informáticos benefician a toda la organización. Dotarlos de las medidas suficientes para mantener su disponibilidad, confidencialidad e integridad, garantiza la continuidad de los servicios.

Un Plan de Continuidad de Negocio, a diferencia de un Plan de Contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.
En el desarrollo de un Plan de Continuidad de Negocio existen dos preguntas claves:

- ¿Cuáles son los recursos de información relacionados con los procesos críticos del negocio de la compañía?
- ¿Cuál es el período de tiempo de recuperación crítico para los recursos de información en el cual se debe establecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o aceptables?

Un Plan de Contingencia reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades,

políticas y procedimientos, acuerdos con entidades internas y externas. (Instituto Nacional de estadísticas e información, 2001)

2.1.3. Análisis de Riesgos

Para realizar un análisis de los riesgos, se procede a identificar:

- Los objetos que deben ser protegidos.
- Los daños que pueden sufrir.
- Sus posibles fuentes de daño y oportunidad.
- Su impacto en la empresa, y
- Su importancia dentro del mecanismo de funcionamiento.

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, (ver figura 2). (Benitez Pereira & Casachahua Medina, 2011)

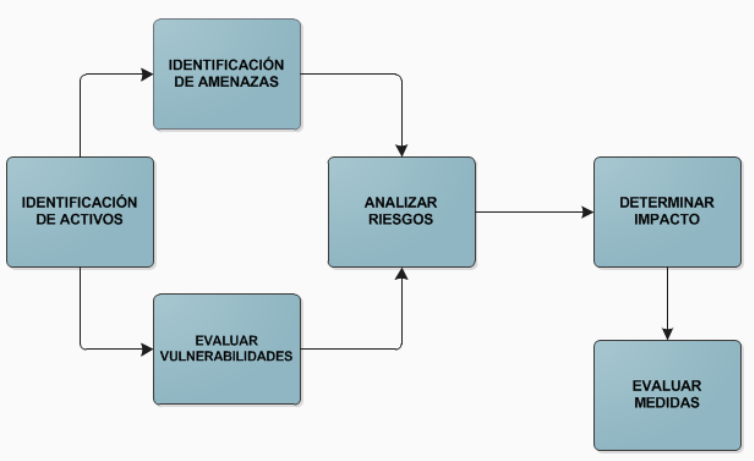


Figura 2 Esquema Análisis de Riesgo

Fuente: (Autor)

2.1.4. Bienes susceptibles de daños

En una compañía se puede identificar los siguientes bienes que se encuentran susceptibles a riesgos.

a) Personal
b) Hardware
c) Software y Utilitarios
d) Datos e Información
e) Documentación
f) Suministros de Energía Eléctrica
g) Suministros de Telecomunicaciones

2.1.4.1. Daños.

Los posibles daños pueden referirse a:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, por ejemplo, cambios de claves o códigos de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- Divulgación de información a instancias fuera de la empresa y que afecte su patrimonio estratégico comercial y/o Institucional, sea mediante robo o infidencia

2.1.4.2. Prioridades.

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que se pierden en la contingencia.

Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

2.1.5. Clases de Riesgos o Amenazas.

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios.

A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

En la figura 3 se observa la clasificación de las distintas amenazas a los sistemas.

Figura 3 Clasificación de las amenazas

Fuente: (Autor)

Dependiendo de la organización y el proceso analizado, serán aplicables distintos tipos de amenazas. Las amenazas tendrán una ***probabilidad de ocurrencia*** que dependerá de la existencia de una vulnerabilidad que pueda ser explotada, para materializarse en un incidente. Por ejemplo, una amenaza del tipo de desastre natural como es un terremoto, tendrá una mayor probabilidad de ocurrencia en una empresa con oficinas en Japón, donde los terremotos ocurren con mayor frecuencia, que en Ecuador. Por lo tanto, a priori podemos decir que el riesgo de daño por terremoto en una compañía situada en Japón es mayor que el de una compañía situada en Ecuador.

Para valorar la probabilidad de una amenaza, en el componente humano existen dos factores a tener en cuenta:

AMENAZA= CAPACIDAD X MOTIVACIÓN

La motivación es una característica humana que es difícil de valorar, pero que sin embargo es un factor a considerar: empleados descontentos, ex-empleados, etc. (Benitez Pereira & Casachahua Medina, 2011).

En la Figura 4 se muestra algunos ejemplos de posibles amenazas, de las cuales debemos tener en cuenta las que pueden afectar a nuestro estudio a la hora de elaborar el Plan de Contingencia IT de la compañía.

AMENAZAS		
DESASTRES NATURALES	DAÑOS ACCIDENTALES	ATAQUES INTENCIONADOS
Huracanes	Fuego fortuito	Fuego intencionado
Inundaciones	Inundaciones	Accesos no autorizados al edificio
Incendios	Falla del aire acondicionado	Actos de vandalismo
	Exceso de humedad	Robos Intencionados
	Humo, gases tóxicos	Manipulación de datos/software y hardware
	Subida de tensión	Uso de software por personal no autorizado
	Fallo de suministro eléctrico	Accesos no autorizados a datos de la compañía
	Fallo de la UPS	Software malicioso
	Accidentes del personal	Robo de equipos, documentos y software
	Capacidad inadecuada de las comunicaciones	Descarga de software no controlada
	Fallo / degradación de las comunicaciones	Interceptación de las líneas de comunicación
	Fallo /degradación del hardware	Manipulación de las líneas de comunicación
	Errores de operación	Abuso de privilegios de acceso
	Fallos en las copias de seguridad	Introducción de virus en los sistemas
	Fallos de los sistemas de autenticación/autorización	Ataques de denegación de servicios
	Perdida de confidencialidad	Copias incontroladas de documentos/software/datos
	incumplimientos legales	Errores en el mantenimiento
		Corrupción de datos
		Incumplimientos legales intencionados

Figura 4 Listado de amenazas

Fuente: (Jiménez, 2009)

2.2. Estudio General de los servidores

2.2.1. Definición de Servidor

Un Servidor o “Server” es una máquina informática con altas capacidades de proceso, encargada de proveer diferentes servicios a un conjunto de computadoras interconectadas entre sí, tanto inalámbricas como las basadas en cable; también permite accesos a cuentas de correo electrónico, administración de dominios empresariales, dominios Web, bases de datos entre otras funciones.

En general, los servidores suelen ser algo más potentes que un ordenador normal, tienen más capacidad tanto de almacenamiento de información como de memoria principal, ya que tienen que dar servicio a muchos usuarios. Tienen sistemas que les permiten resolver ciertas averías de manera automática, así como sistemas de alerta para evitar fallas en operaciones de datos críticos, ya que deben estar encendidos los 365 días del año las 24 horas del día.

Es preferible que los servidores se monten en gabinetes especiales denominados Racks, en los cuales podemos colocar varios servidores debido a sus compartimentos especiales lo que permite ahorrar espacio, además de que es más seguro porque permanecen fijos. (Informática Moderna, 2015)

2.2.2. Aspectos de Hardware

Un servidor es un sistema informático que consta de un hardware y características especiales que son las que lo diferencian a los domésticos, este hardware es más preciso y soporta tareas más complejas; permite también sustituir componentes dañados sin la necesidad de apagar el sistema para llevar a cabo el mantenimiento.

2.2.3. Aspectos de Software

Se requiere un software para poder controlar el hardware, utilizarlo al 100% y que permita el mantenimiento el máximo de estabilidad.

El software está enfocado a ofrecer uno o varios servicios, estos servicios pueden estar diseñados para ofrecer funcionalidades de red o en muchos casos ofrecer funcionalidades para los usuarios de la red.

2.2.4. Tipos de Servidores y sus funciones.

- **Servidor de Archivos (File Server)**

Son típicos de la red local de una empresa, aunque algunos son más potentes que pueden albergar capacidades medidas en exabytes. En este se almacena archivos de diferentes extensiones y los comparte a otros usuarios en la red, (ver figura 5).

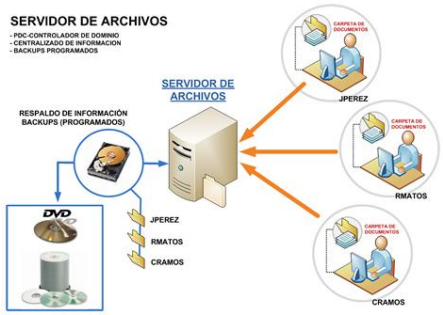


Figura 5 Servidor de Archivos

Fuente: (Redessil, 2015)

- **Servidor de Aplicaciones (Application Server):**

Son servidores que conectan dos aplicaciones, conocidos como *middleware*, la mayoría de veces entre los servidores de bases de datos y el usuario, y a menudo los conectan.

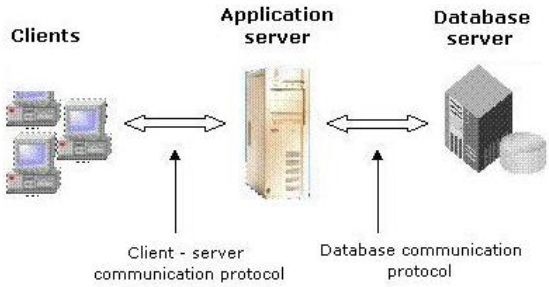


Figura 6 Servidor de Aplicaciones

Fuente: (Redessil, 2015)

- **Servidor de Audio/Video (Audio/Video Servers):**

Estos ayudan a los sitios web mostrar contenido multimedia en forma de flujo continuo (streaming) sin interrupciones, con la posibilidad de escuchar música o ver videos sin necesidad de ser descargados previamente.

- **Servidor de Chat (Chat Servers):**

Estos permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

- **Servidor de fax:**

Almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas del fax.

- **Servidores FTP (FTP Servers):**

Son uno de los servicios más antiguos de Internet, File Transfer Protocol, cuya función es permitir el intercambio de datos entre diferentes servidores u ordenadores.

Figura 7 Servidor FTP

Fuente: (Maryuri, 2008)

- **Servidores Web (Web Servers):**

Básicamente, un servidor web es un programa diseñado para alojar y transferir páginas web. Estos servidores atienden las peticiones que hacen los clientes a través del internet.

Figura 8 Servidor Web

Fuente: (GOMEZ CAMPOS, 2012)

- **Servidor Proxy:**

Un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y para bloquear el acceso a un sitio web.

Figura 9 Servidor Proxy

Fuente: (Maryuri, 2008)

- **Servidor de Base de Datos:**

Da servicios de almacenamiento y gestión de bases de datos a sus clientes. Una base de datos es un sistema que nos permite almacenar grandes cantidades de información.

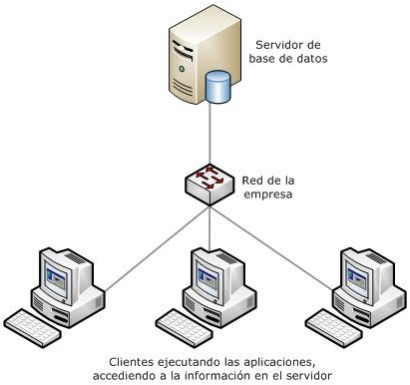


Figura 10 Servidor de Base de datos

Fuente: (Net Humans S.A., 2013)

- **Servidor de impresiones:**

Controla una o más impresoras y acepta trabajos de impresión de otros usuarios de la red, permite realizar las mismas funciones como si la impresora estuviera conectada directamente con el puerto de impresora del sitio de trabajo.

- **Servidor de correo:**

Almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.

Figura 11 Servidor de Correo

Fuente: (GOMEZ CAMPOS, 2012)

- **Servidor DNS:**

Un servidor de DNS (Domain Name System) es capaz de recibir y resolver peticiones relacionadas con el sistema de Nombres. Un servidor de DNS sirve, por tanto, para (1) traducir su nombre de dominio en una dirección IP, (2) asignar Nombres a todas las máquinas de una red y trabajar con nombres de dominio en lugar de IPs.

- **Servidor DHCP:**

Es un protocolo de red en el que el servidor bajo el que está corriendo provee los parámetros de configuración necesarios a las máquinas conectadas a la red que así lo soliciten. Mediante DHCP se asignarán de forma totalmente automática y transparente parámetros como la puerta de enlace, la máscara de subred, la DNS o la propia dirección IP.

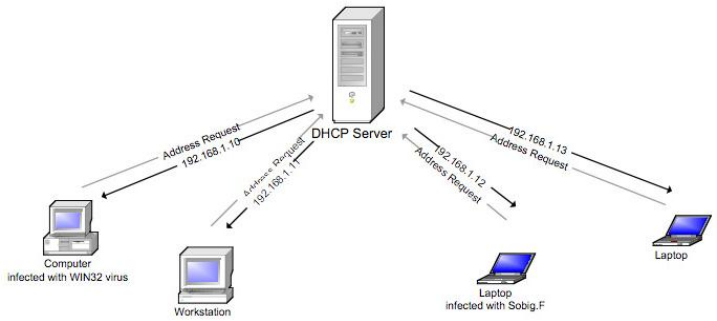


Figura 12 Servidor DHCP

Fuente: (GOMEZ CAMPOS, 2012)

- **Servidor de Directorio Activo/Dominio:**

El directorio activo es un servicio de directorio. Cuyo término se refiere a un directorio donde la información sobre usuarios y recursos está almacenada, y un servicio o servicios que dejan acceder y manipular estos recursos. El directorio activo es una manera de manejar todos los elementos de una red, incluidos ordenadores, grupos, usuarios, dominios, políticas de seguridad, y cualquier tipo de objetos definidos para el usuario. Además de

esto, provee de funciones adicionales más allá de estas herramientas y servicios. (Maryuri, 2008)

2.2.5. Arquitectura.

2.2.5.1. Arquitectura Cliente-Servidor

Es la tecnología que proporciona al usuario final el acceso transparente a las aplicaciones, datos, servicios de cómputo o cualquier otro recurso del grupo de trabajo, a través de la organización, en múltiples plataformas. (Márquez Avendaño, 2013)

Arquitectura en 2 niveles:

En este modelo el cliente solicita recursos y el servidor responde directamente a la solicitud con sus propios recursos, es decir que el servidor no requiere de otra aplicación para proporcionar parte del servicio.

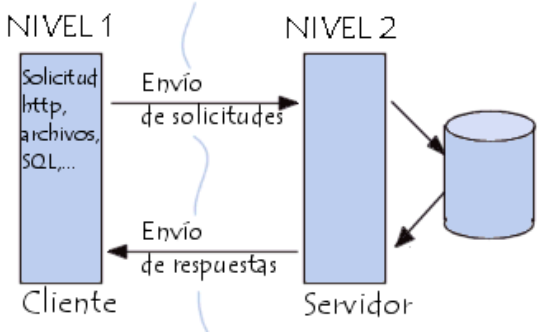


Figura 13 Arquitectura en 2 niveles

Fuente: (Kioskea.net, 2014)

Arquitectura en 3 niveles:

En este modelo existe un nivel intermediario, lo que significa que la arquitectura esta compartida por:

1. Un cliente, quien solicita los recursos, equipado con una interfaz de usuario para la presentación.

2. El servidor de aplicaciones, cuya tarea es proporcionar los recursos solicitados, pero que requiere de otro servidor para hacerlo.
3. El servidor de datos, que proporciona al servidor de aplicaciones los datos que requiere.

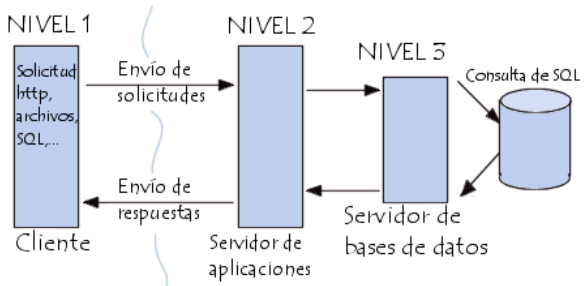


Figura 14 Arquitectura en 3 niveles

Fuente: (Kioskea.net, 2014)

2.2.5.2. Características de la arquitectura Cliente-Servidor

Las características básicas de la arquitectura Cliente-servidor son las siguientes:

- Combinación de un cliente que interactúa con el usuario, y un servidor que interactúa con los recursos compartidos, en donde la interfaz relaciona el cliente con el usuario y el servidor actúa como un motor de software que maneja recursos compartidos tales como bases de datos, archivos, impresoras, aplicativos, etc.
- Las tareas del cliente y del servidor tienen diferentes requerimientos en cuanto a recursos como velocidad del procesador, memoria, velocidad y capacidades del disco.
- Se establece una relación entre procesos distintos, los cuales pueden ser ejecutados en la misma máquina o en máquinas diferentes distribuidas a lo largo de la red.
- Un servidor puede dar un servicio a muchos clientes estableciendo una relación muchos a uno.

- Los clientes corresponden vienen a ser procesos activos, en tanto que los servidores pasivos, ya que son los clientes los que hacen las peticiones y los servidores esperan las mismas.
- Existe la posibilidad de conectar clientes y servidores independientemente de sus plataformas.

El concepto de escalabilidad tanto horizontal como vertical es aplicable a cualquier sistema Cliente/Servidor. La escalabilidad horizontal permite agregar más estaciones de trabajo activas y la escalabilidad vertical permite mejorar las características del servidor o agregar múltiples servidores. (Márquez Avendaño, 2013)

2.3. Servidor File server

2.3.1. ¿Qué es un File Server?

El Servidor de Archivos (File Server) es un equipo responsable de la centralización del almacenamiento y gestión de los archivos de forma que otros equipos de la misma red puedan acceder a los mismos, es decir, se comparte información a través de la red sin necesidad de transferir físicamente los archivos en dispositivos de almacenamiento externo.

En una red sofisticada, un servidor de archivos puede ser un dispositivo de almacenamiento conectado a la red dedicada (NAS) que también sirve como una unidad de disco duro remoto para otros equipos, permitiendo que cualquier usuario en la red pueda almacenar archivos en él como si fuera su propio equipo.

2.3.2. Características de un File Server

La característica principal de un servidor de archivos es que proporciona servicios de almacenamiento y recuperación de archivos, incluyendo funciones de seguridad que controlan los derechos de acceso a los archivos. Desde el punto de vista del cliente, la localización de los archivos compartidos es compartida y transparente, es decir, no existe diferencias perceptibles si un

archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina.

2.3.3. Ventajas y Desventajas de un File Server.

A continuación, en la Figura 15 se mostrará las ventajas y desventajas de un servidor de archivos.

VENTAJAS	DESVENTAJAS
Mayor Facilidad del mantenimiento. Por ejemplo, es posible sustituir, reparar, aumentar, o aún volver a poner un servidor mientras que sus clientes siguen siendo inafectados por ese cambio.	La congestión del tráfico en la red ha sido una desventaja en este modelo. Mientras que el número de peticiones simultaneas del cliente a un servidor aumenta, el servidor puede sobrecargarse seriamente.
Los servidores pueden mejorar el acceso y recursos de control, para garantizar que solamente dichos clientes con los permisos apropiados pueden tener accesos y cambiar datos.	El paradigma del servidor de cliente carece de robustez de una buena red del P2P. Una caída del servidor ocasionaría que las peticiones de los clientes no sean satisfechas.
Funciona con diversos clientes múltiples de diversas capacidades	

Figura 15 Principales Ventajas y Desventajas de un Servidor de Archivos

Fuente: (Autor)

2.3.4. Arquitectura de un File_Server.

La arquitectura de un File_Server o Servidor de Archivos se basa en la existencia de una o varias máquinas que almacena datos y estaciones de trabajo que ejecutan aplicaciones que los procesan. Los clientes en este tipo de aplicaciones son activos, (ver figura 16).

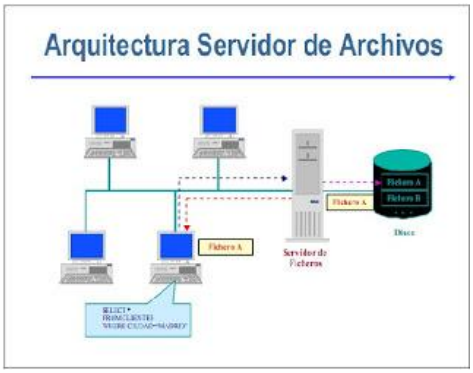


Figura 16 Arquitectura Servidor de Archivos
Fuente: (Jarrin, 2010)

2.4. Sistema de Archivos.

2.4.1. Introducción.

Todas las aplicaciones computarizadas necesitan almacenar y recuperar la información superando las limitaciones de almacenamiento real, trascendiendo a la duración de los procesos que utilizan o generan, e independizando a la información de los procesos permitiendo el acceso a la misma a través de varios procesos.

Las condiciones esenciales para el almacenamiento de la información a largo plazo son:

- Debe ser posible almacenar una cantidad muy grande de información.
- La información debe sobrevivir a la conclusión del proceso que la utiliza.
- Debe ser posible que varios procesos tengan acceso concurrente a la información.

La solución a esto es el almacenamiento de la información en discos y otros medios externos en unidades llamadas **archivos**, los cuales deben ser persistentes, es decir que no deben verse afectados por la creación o terminación

de un proceso, además pueden ser manipulados como una unidad por operaciones como: abrir, cerrar, crear, eliminar, renombrar y listar.

El Sistema de Archivos es la parte del sistema de administración del almacenamiento responsable, principalmente, de la administración de los archivos del almacenamiento secundario.
Es la parte del S. O. responsable de permitir *"*compartir controladamente*"* la información de los archivos.

2.4.2. Funciones del Sistema de Archivos.

A continuación, se listará algunas de las funciones que cumple un Sistema de Archivos.

- Los usuarios deben poder crear, modificar y borrar archivos.
- Se tiene varios tipos de acceso controlado: "Acceso de Lectura", "Acceso de Escritura", "Acceso de Ejecución" o varias combinaciones de estos.
- Se debe poder estructurar los archivos de la manera más apropiada a cada aplicación.
- Los usuarios pueden ordenar la transferencia de información entre archivos.
- Se deben proporcionar posibilidades de respaldo y recuperación para garantizar la pérdida accidental de información o la destrucción maliciosa.
- En ambientes sensibles, el sistema de archivos debe proporcionar posibilidades de *Cifrado* y *descifrado*
- El sistema de archivos debe ser una interface amigable para el usuario.

2.4.3. Archivos.

Un archivo es un conjunto de bits que son almacenados en un dispositivo, el cual es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. Los archivos informáticos facilitan una manera de organizar los

recursos usados para almacenar permanentemente datos en un sistema informático virtual.

2.4.4. Nombre de los archivos.

Es la cadena de texto que se utiliza para designar a un archivo. Algunos Sistemas Operativos distinguen entre mayúsculas y minúsculas, en tanto que otros no.

El nombre de un archivo consta de dos partes: **nombre y extensión.** El nombre no puede comenzar con un espacio y no se puede utilizar ciertos caracteres (/ : ” | = < > |), en tanto que la extensión puede o no decir el tipo de contenido de un fichero. (.jpg, .mp3, .txt).

2.4.4.1. Estructura de un archivo.

La estructura de archivos es el nivel más básico de organización. Es la combinación de representaciones de datos en archivos y al poseer una estructura de archivos asegura que los usuarios y programas pueden acceder y escribir a los archivos. Un buen diseño de estructuras de archivos brindará acceso a grandes capacidades de información, sin gastar tiempo de espera por el disco, (ver figura 17).

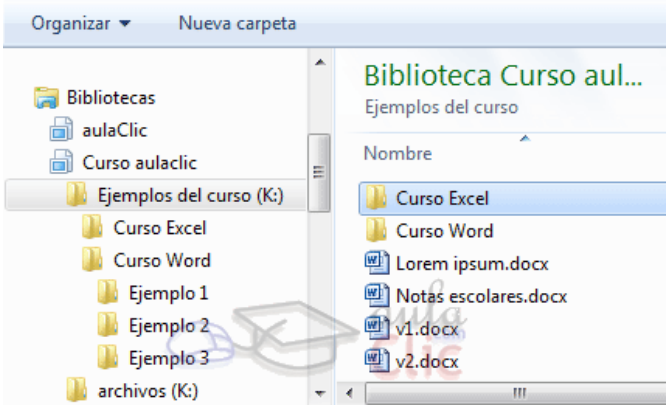


Figura 17 Ejemplo estructura de archivos

Fuente: (Autor)

2.4.4.2. Tipos de Archivos.

Los archivos se dividen en dos grandes grupos:

- **Ejecutables*:*** Son aquellos que han sido programados bajo algún lenguaje específico para realizar acciones y rutinas por sí mismos.

Ejemplo: .EXE, .COM, .BAT, .DLL, etc.

- **De datos:** Son aquellos que principalmente contienen datos y necesitan de una aplicación específica para ser abiertos.

Ejemplo: .TXT, .DOC, .XLS, etc.

2.4.4.3. Acceso a un archivo.

Se refiere al método utilizado para acceder a los registros de un archivo prescindiendo de su organización. Existen distintas formas de acceder a los datos:

- **Secuenciales:** Los registros se leen desde el principio hasta el final del archivo, de tal forma que para leer un registro se leen todos los que preceden.
- **Directo:** Cada registro puede leerse / escribirse de forma directa solo con expresar su dirección en el fichero por él número relativo del registro o por transformaciones de la clave de registro en él número relativo del registro a acceder.
- **Por Índice:** Se accede indirectamente a los registros por su clave, mediante consulta secuenciales a una tabla que contiene la clave y la dirección relativa de cada registro, y posterior acceso directo al registro.
- **Dinámico:** Es cuando se accede a los archivos en cualquier de los modos anteriormente citados.

La elección del método está directamente relacionada con la estructura de los registros del archivo y del soporte utilizado.

2.4.4.4. Atributos de archivos.

Cada archivo tiene su nombre, datos y elementos adicionales llamados atributos, que varían considerablemente de sistema a sistema.

- **Protección:** quién debe tener acceso y de qué forma.
- **Contraseña:** contraseña necesaria para acceder al archivo.
- **Creador:** identificador de la persona que creó el archivo.
- **Propietario:** propietario actual.
- **Bandera exclusivo - para - lectura:** 0 lectura / escritura 1, para lectura exclusivamente.
- **Bandera de ocultamiento:** 0 normal, 1 para no exhibirse en listas.
- **Bandera de sistema:** 0 archivo normal, 1 archivo de sistema.
- **Bandera de biblioteca:** 0 ya se ha respaldado, 1 necesita respaldo.
- **Bandera ascii / binario:** 0 archivo en ascii, 1 archivo en binario.
- **Bandera de acceso aleatorio:** 0 solo acceso secuencial, 1 acceso aleatorio.
- **Bandera temporal:** 0 normal, 1 eliminar al salir del proceso.
- **Banderas de cerradura:** 0 no bloqueado, distinto de 0 bloqueado.
- **Longitud del registro:** número de bytes en un registro.
- **Posición de la llave:** ajuste de la llave dentro de cada registro.
- **Longitud de la llave:** número de bytes en el campo llave.
- **Tiempo de creación:** fecha y hora de creación del archivo.
- **Tiempo del último acceso:** fecha y hora del último acceso al archivo.
- **Tiempo de la última modificación:** fecha y hora de la última modificación al archivo.
- **Tamaño actual:** número de bytes en el archivo.
- **Tamaño máximo:** tamaño máximo al que puede crecer el archivo.

2.4.4.5. Operaciones con archivos.

Las operaciones más comunes al sistema relacionadas con los archivos son:

- **Crear:** el archivo se crea sin datos.
- **Eliminar**: si el archivo ya no es necesario debe eliminarse para liberar espacio en disco.
- **Abrir:** antes de utilizar un archivo, un proceso debe abrirlo. Lo que permite que los atributos y la lista de direcciones se graben en la memoria principal para un rápido acceso en las siguientes llamadas.
- **Cerrar:** cuando los archivos ya no sean necesarios se deben cerrar para liberar la tabla de espacio interno.
- **Leer:** los datos se leen del archivo; y se proporciona el buffer necesario para colocarlos.
- **Escribir:** los datos se escriben en el archivo, en la posición actual.
- **Añadir:** es una forma restringida de “write”. Solo puede añadir datos al final del archivo.
- **Buscar:** especifica el punto donde posicionarse. Cambia la posición del apuntador a la posición activa en cierto lugar del archivo.
- **Obtener atributos:** permite a los procesos obtener los atributos del archivo.
- **Establecer atributos:** algunos atributos pueden ser determinados por el usuario y modificados luego de la creación del archivo.
- **Cambiar de nombre:** permite modificar el nombre de un archivo ya existente.

2.4.4.6. Archivos mapeados a memoria.

Un archivo mapeado a memoria es un esquema que permite la asociación entre un archivo y una porción de la Memoria Virtual, lo que permiten acceder a archivos de disco a través de punteros de memoria. Esta correlación permite a una aplicación o a algunos usuarios ejecutar acciones de lectura y escritura (sobre el archivo) directamente, como si se encontrara en la memoria principal.

2.4.5. Directorios.

Los directorios son contenedores virtuales en los cuales se almacenan una agrupación de archivos y otros subdirectorios, atendiendo a su contenido, a su propósito o a cualquier criterio que decida el usuario.

2.4.5.1. Sistemas Jerárquicos de Directorios.

El directorio contiene un conjunto de datos por cada archivo referenciado, es así que una posibilidad es que el directorio contenga por cada archivo referenciado el nombre, sus atributos y las direcciones en disco donde se almacena los datos. Otra posibilidad es que cada entrada del directorio contenga: El nombre del archivo, un apuntador a otra estructura de datos donde se encuentran los atributos y las direcciones en disco. (Studija, 2007)

A continuación, se observa la organización de directorios

- **Directorio Único:** Un solo directorio con todos los archivos de los usuarios, como se observa en la figura 18.

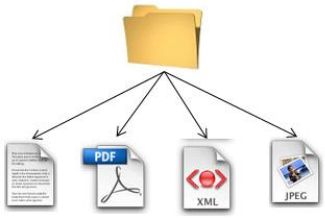


Figura 18 Un solo directorio compartido por todos los usuarios.

Fuente: (Autor)

- **Un directorio por usuario:** Se habilita un solo directorio por usuario, (ver figura 19).

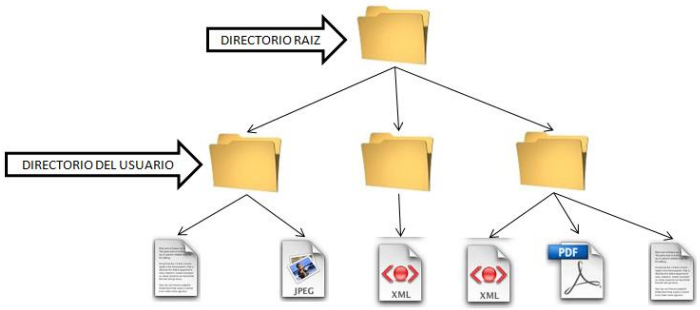


Figura 19 Un directorio por usuario

Fuente: (Autor)

- **Un árbol de directorios por usuario:** Cada usuario puede tener tantos directorios como necesite, respetando una jerarquía general, (ver figura 20).

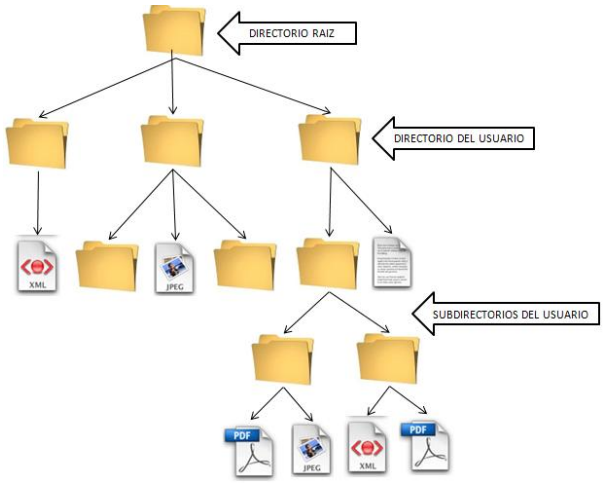


Figura 20 Un árbol arbitrario por usuario

Fuente: (Autor)

2.4.5.2. Nombre de las rutas de acceso

Los principales métodos para nombres de los archivos son:

- **Ruta Absoluta:** Una ruta absoluta o completa comienza con la letra de unidad seguida de dos puntos, es decir, se indica toda la ruta del archivo

incluyendo el directorio raíz. Ejemplo **C:\carpeta1\carpeta2\archivo1.doc.** (Ureña Gómez, 2012)

- **Ruta Relativa:** Se muestra la ruta a partir de donde este en ese momento situado, exceptuando el directorio raíz. Por ejemplo, si estamos en la ruta **C:\carpeta1** y queremos acceder al **archivo1** que está dentro de la **carpeta2,** seria **carpeta2\archivo1.** Para ir al directorio padre, usamos dos puntos seguidos **(..).** (Ureña Gómez, 2012)

2.4.5.3. Operaciones con directorios

Las operaciones permitidas para el manejo de los directorios tienen variación de sistema a sistema. Las más comunes son:

- **Crear:** Se crea un directorio vacío.
- **Eliminar:** Se elimina un directorio, que debe estar vacío.
- **Abrir directorio:** Se pueden leer los directorios: Antes de poder leer un directorio, éste debe ser abierto.
- **Cerrar directorio:** Cuando se ha leído un directorio, éste debe ser cerrado para liberar el espacio correspondiente de la tabla interna.
- **Leer directorio:** Regresa la siguiente entrada en un directorio abierto, sin importar el tipo de estructura de directorios que se utilice.
- **Cambiar de nombre:** Cambia el nombre de un directorio de manera similar al cambio para archivos.
- **Ligar:** es una técnica que permite que un archivo aparezca en más de un directorio: Especifica un archivo existente y el nombre de una ruta de acceso.

  Crea un enlace del archivo ya existente con el nombre especificado en la ruta de acceso.
- **Desligar:** se elimina una entrada del directorio:

  Si el archivo que se desea desligar aparece solo en un directorio (el caso normal): Se elimina del sistema de archivos.

Si el archivo que se desea desligar, está presente en varios directorios: Solo se elimina la ruta de acceso especificada y las demás rutas permanecen. (Vergara, 2004)

2.4.6. Implantación del sistema de archivos y sus relaciones con la asignación y liberación de espacio.

Se considera aspectos tales como: la forma de almacenamiento de archivos y directorios, la administración del espacio en disco y la forma de hacerlo de manera eficiente y confiable.

Por tal razón se deben tener presentes problemas tales como la “fragmentación” creciente del espacio en disco, lo cual ocasiona problemas de performance al hacer que los archivos se desperdiguen a través de bloques muy dispersos. Una técnica para aliviar el problema de la “fragmentación” consiste en realizar periódicamente una Reorganización de los archivos automáticamente según algún criterio predefinido.

2.5. Estudio General de la NAS

2.5.1. Definición de NAS

Network Attached Storage, es una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con computadores o servidores clientes a través de la red, haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Por lo general, posee su propio sistema de archivos que aloja al sistema operativo, así como también una serie de discos independientes que se utilizan para alojar los datos que se van a guardar. (Garth A. & Van Meter, 2000)

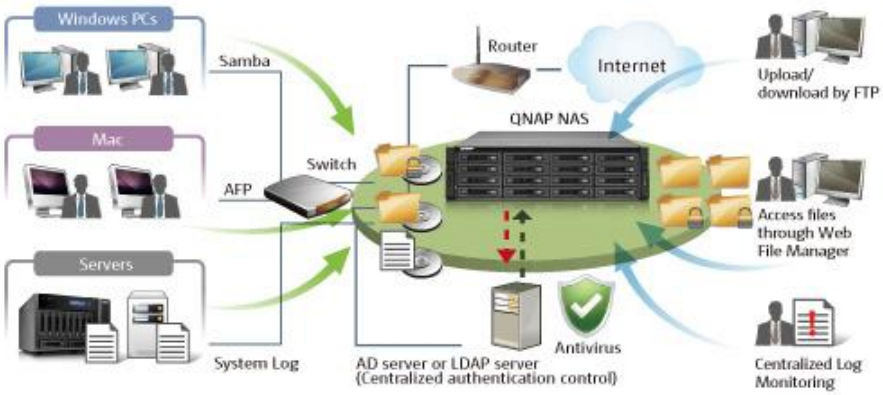


Figura 21 Sistema NAS

Fuente: (Computo y Accesorios, 2015)

2.5.2. Sistemas Operativos que soporta un servidor tipo NAS

Existe una gran variedad de sistemas operativos que soporta un servidor tipo NAS, dependiendo las necesidades de una empresa. A continuación, se enlistará algunos sistemas operativos que son usados con estas tecnologías.

- **FreeNAS:** Es el sistema más popular y se trata de una distribución basada en FreeBSD 7.2 con interfaz web y scripts PHP. Es compatible con RAID 0,1,5 con sistema de archivos SMB (CIFS - Windows), AFP (Mac OS), NFS (Unix/Linux), además soporta FTP/TFTP, Rsync, iSCSI, uPnP, ZFS y encriptación de volúmenes. (Mundo NAS, 2011)
- **CryptoNAS**: Está pensando especialmente para trabajar con volúmenes encriptados los cuales son accesibles a través de SMB/CIFS y pueden ser accedidos usando herramientas tipo FreeOTFE o desde versiones Linux más actuales. Por supuesto tiene soporte para cualquier volumen montado sobre IDE, SCSI, USB, FireWire, SATA y RAID, puesto que está basado en un kernel de Linux 2.6.20. (Mundo NAS, 2011)
- **Openfiler:** basada en Linux y se ha liberado bajo licencia GPLv2, pudiendo ser instalada en ordenadores, servidores e incluso virtualizada; soporta los protocolos de red SMB / CIFS, NFS, HTTP / WebDAV y FTP.

Openfiler también ofrece amplias funciones de gestión de intercambio, como el control de acceso basado en multi-grupo en una base por acción, SMB / CIFS de instantáneas y acciones públicos / clientes. (Mundo NAS, 2011)

- **OpenMediaVault:** Está basada en Debian y nos habilita servicios como ssh, sftp, smb/cifs, rsync entre otros, además es de diseño modular lo que facilita la mejora en complementos y añadidos por la comunidad disponibles de forma gratuita. (Mundo NAS, 2011)
- **Windows Storage Server:** Es una versión de Windows Server que está con licencia para fabricantes de equipos originales para su uso de dispositivos NAS. Esta modificación del sistema operativo nos permite construir un servidor capaz de crear y exponer en red unidades de disco (NAS) usando el estándar (ISCSI), este estándar define como se proporcionan unidades de disco en redes TCP/IP. (GuilleSQL, 2007)

2.5.3. Dispositivos NAS.

Los dispositivos de almacenamiento NAS, que vienen preparados para almacenar archivos para los usuarios con un mínimo de carga de administración general, puede ser una solución asequible para las PYMEs en el contexto económico actual que exige hacer más con menos. Elegir el mejor sistema para cada entorno de almacenamiento requiere un poco de planificación.

En el mercado se puede encontrar cajas NAS diseñadas por proveedores como Buffalo Technology Inc., D-Link Corp. y la división de Iomega EMC Corp. que tienen un precio relativamente bajo, las cuales tienen un motor de escasa potencia y no pueden ofrecer protección RAID para los datos. Además, no proporciona un rendimiento razonable para más de cinco a diez usuarios, no manejan la estructura ACL de Windows lo cual limita su flexibilidad de seguridad.

Existen otros dispositivos NAS de cuatro bahías de proveedores como la División Iomega de EMC y Netgear, los cuales ofrecen un rendimiento tres o cuatro veces mayor que las cajas NAS básicas pero siguen sin tener prestaciones avanzadas como Snapshots (instantáneas) y duplicación, pero pueden ser suficientes para las PYMES.El mercado de NAS de gama media, que vende sistemas que van de unos 2.000 $ hasta los 15.000 $, está dominado por grandes y pequeños proveedores, que incluyen con su hardware una u otra edición del Servidor de Almacenamiento Windows de Microsoft Corp. o del Servidor de almacenamiento de datos unificado Windows.

Windows Storage Server añade algunas prestaciones decisivas, entre ellas la administración web, una serie de herramientas de administración personalizables instaladas en fábrica, una función búsqueda de archivos que incluye la indexación de todo el texto y un almacenamiento único a nivel de archivo. Estos dispositivos NAS de empresa también pueden tener controladores de disco y servidores de red redundantes, que mejoran la disponibilidad más allá de lo que se podría conseguir con sistemas inferiores. (TechTarget S.A., 2012)

2.6. Diferencia entre Sistema Operativo Windows Server 2003 Standard Edition y Windows 2008 Storage Server

2.6.1. Windows Server 2003 Standard Edition.

Windows Server 2003 Standard Edition es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a las necesidades, tanto de manera centralizada como distribuida. Es un sistema altamente productivo que es a la vez seguro, confiable, altamente disponible y escalable. (Microsoft, 2015)

Tabla 1
Beneficios de Windows Server 2003 Standard Edition

Beneficio	Descripción
Sistema Seguro	✓ Proporciona una infraestructura integrada que ayuda a asegurar que la información de negocios esté segura. ✓ Proporciona fiabilidad, disponibilidad y escalabilidad para poder ofrecer la infraestructura de red que los usuarios solicitan.
Sistema Productivo	✓ Proporciona herramientas flexibles que ayudan a ajustar el diseño e implementación de las necesidades organizativas y de red. ✓ Ayuda a administrar la red proactivamente al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones.
Conectado	✓ Nos ayuda a crear una infraestructura de soluciones de negocio para mejorar la conectividad con empleados, socios, sistemas y clientes.
Mejor economía	✓ Proporciona una guía preceptiva y de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar. ✓ Ayuda a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la implementación de un servidor. ✓ Bajar el coste total de propiedad (TCO) para recuperar rápido la inversión.

Fuente: (Autor)

2.6.2. Windows Storage Server 2008

Windows Storage Server 2008 pertenece a la familia de los productos Windows Storage Server y se basa en las tecnologías y características de Windows Server 2008. Ofrece a los clientes nuevas capacidades de almacenamiento, implementación simplificada y una administración más sencilla. (Microsoft, 2015).

Tabla 2
Beneficios de Windows Storage Server 2008

Beneficio	Descripción
Fáciles accesos para los clientes	✓ Para un usuario final en una red, un dispositivo NAS es parecido a un servidor de archivos, la única diferencia es que una NAS configurada con WSS es un equipo específicamente diseñado para almacenamiento de archivos de una manera más robusta
Soporte iSCSI	✓ La conectividad iSCSI abre la puerta para que los servicios de E/S basada en bloques, es decir, los destinos de almacenamiento en el dispositivo NAS puede aparecer en un servidor como almacenamiento conectado localmente. ✓ También significa que puede ser utilizada para las instancias de máquinas virtuales Microsoft Hyper-V.
Almacenamiento de instancia única (SIS) v2	✓ Reduce el consumo de espacio en disco eliminando archivos duplicados en los volúmenes de datos.
Optimización del servidor de archivos	✓ Optimizado por defecto para la función de servidor de archivos de alrededor del 8% de ganancia sobre los ajustes estándar.
Administración remota en entornos heterogéneos	✓ Esta es una característica realmente fresca que permite ingresar por escritorio remoto de pantalla completa con sólo ir a http://server/desktop.
Uso compartido de archivos de Windows	✓ SMB de alto rendimiento 2.0 para Windows y todas las mejoras realizadas para los equipos de protocolo NTFS.
Sistema de archivos de red NFS	✓ Rendimiento mejorado, NFS y SMB interoperabilidad
Administrador de recursos del servidor de archivos	✓ Directorio de cuotas, filtrado de archivos e informes
Espacio de nombres DFS y replicación DFS	✓ Replicación de archivos eficaz en redes WAN
Cifrado de unidad BitLocker	✓ BitLocker impide que un ladrón rompa las protecciones del sistema o realice la visualización de los archivos almacenados en la unidad protegida sin conexión.
Windows PowerShell	✓ Una línea de comandos de shell y lenguaje de scripting basado en tareas diseñadas especialmente para la administración del sistema. Control y automatización de la administración del sistema operativo Windows y las aplicaciones que se ejecutan en Windows.

Fuente: (Barreto, 2011)

2.6.3. Diferencias entre los sistemas operativos.

Tabla 3
Diferencia de servicios entre Windows server 2003 y Windows Storage server 2008

Servicios	Windows Server 2003 Standard Edition	Windows Storage Server 2008 Standard edition
Servicios de Directorio Activo	Si	Si (ilimitada)
Servicio de fichero (smb)	Si	Si
Servicio de Impresión	Si	Si
Clustering	---	---
Servicio de Balanceo de carga	Si	Si
Servicio IIS	Si	Si
Servicio de Fax	Si	Si
Cortafuego básico	Si	Si
Servicio de Terminal	SI	Si
Límite VPN	1000 conexiones concurrentes	Ilimitado
Windows System Resource Manager	---	Si
DFS Namespace and Replication	---	Si
Almacenamiento de instancia única	---	Si
DHCP Server	---	Si
Server Backup y BitLocker	---	Si
Servicios para Macintosh	---	Si

Fuente: (Autor)

Tabla 4
Diferencia de requisitos del sistema entre Windows server 2003 y Windows Storage server 2008

Requisito de Hardware	Windows Server 2003 Standard	Windows Storage Server 2008 Standard
Velocidad mínima de CPU	133 MHz	1 Ghz (x86) o 1.4 GZ (x64)
Velocidad recomendad de CPU	550 MHz	2 Ghz o más
Memoria RAM máxima	4 GB	32 GB
CPU Sockets	Hasta 4	Hasta 4
Disk (number / interfaces / RAID type)	Any/any/any	Any/any/any
Nics	---	Ilimitado

Fuente: (Autor)

2.7. Migración de Sistemas.

2.7.1. ¿Qué es migración?

Una migración tecnológica es un proceso de cambio en los elementos del software y/o hardware, la cual incluye una serie de pasos a seguir:

- Determinación de la causa de la migración.
- Fijar el momento de la migración.
- Fijar el procedimiento de migración.
- Evaluar la migración.

Un proceso de migración no puede darse sólo con la sustitución del software, pues están involucrados factores de preparación y previsión que deben ser tomados en cuenta, es decir, todas las migraciones deben basarse en una cuidadosa planificación para así evitar posibles pérdidas de información o funcionalidad.

2.7.2. ¿Por qué se debe realizar una migración?

Aunque la sustitución de equipos antiguos o caducados sigue siendo un motivo común para realizar la migración de datos, existe diversas razones para hacer una migración, tales como: mejorar el desempeño y tiempo de respuesta, cumplir con nuevos requerimientos de usuario, de la aplicación o políticas de seguridad, la compatibilidad con otras aplicaciones, la actualización de versiones, la estandarización de la tecnología de información en la organización, facilitar el intercambio de datos entre procesos, el aumento en el volumen de datos, nuevos procesos de negocio, mejoras en la seguridad o en el control de la información entre otros.

2.7.3. ¿Por qué no se debe realizar una migración?

Aunque la nueva tecnología es una de las razones principales para llevar a cabo la migración, se debe considerar cuidadosamente si el esfuerzo llevado durante la migración, es hecho únicamente con el fin de implementar nueva tecnología al ambiente sin que esta tenga mayor utilidad dentro de la empresa, es decir, que siempre se debe cuestionar si se está agregando más valor al ambiente cuando se implementa una nueva tecnología en particular.

2.7.4. Herramientas de migración.

Hoy en día con el avance de la tecnología se puede encontrar un sin número de herramientas para realizar la migración de datos de un servidor a otro. A continuación, se enlistará algunas herramientas que nos permite realizar la migración de datos.

- **Synkron:** Es un programa creado bajo licencia GPL v.2 que permite la sincronización de archivos y carpetas de manera que se pueda efectuar copias de seguridad o mantener actualizados los contenidos de una memoria USB. Además, admite la restauración de documentos a versiones anteriores. (Ministerio de Educación, cultura y Deporte de España, 2009).

- **Synctoy:** Programa de Microsoft, que mejora y agiliza el trabajo con Windows de diversas formas. En concreto, ésta permite llevar a cabo el trabajo de sincronización de directorios de forma mucho más rápida y cómoda. El programa trabaja con parejas de directorios y permite gestionar tantas de ellas al mismo tiempo como quieras, cada una de ellas con su propia configuración. (Brandt, 2012)
- **Allways Sync:** Es un programa gratuito de sincronización de archivos y carpetas para Windows, con el cual se puede sincronizar datos entre dos ordenadores, además de replicar y respaldar datos y sincronizar dispositivos removibles con un disco local. (Anónimo, 2010)
- **Magic Transfer:** Esta herramienta cada vez que detecta cambios en documentos recientes, añade una pestaña de Favoritos o se recibe un correo electrónico indicando los cambios que se realizaron en las PCs utilizadas. (Cruz, 2012)
- **Uranium Backup:** Es un software de copia de seguridad ligero y fiable que sirve para proteger los datos personales y empresariales. Se trata de una solución completa capaz de ajustarse a todas las necesidades. Es una herramienta muy potente, pero su interfaz es muy sencilla. Dispone de un sistema de informes que avisa en caso de que se produzca un fallo. Todo está bajo control. (Nanosystems S.r.l. , 2015)
- **Robocopy:** Es un comando de replicación de directorios, disponible desde la Línea de Comandos. Posee características como retomar copias fallidas, saltarse archivos bloqueados por el sistema operativo sin interrumpir el progreso de la copia y puede copiar datos eficientemente a través de una red local. Funciona en modo de comando y al final de la copia se tiene información útil como la cantidad de archivos omitidos, el tamaño y la duración de la copia. (Escuela Abierta de Nuevas Tecnologías, 2009)

- **Double Take:** Es la primera solución de alta disponibilidad y recuperación de catástrofes en tiempo real que ofrece opciones para servidores físicos, virtuales o en la nube. Double Take reduce los costos de mantenimiento mediante la optimización de la infraestructura existente y la ampliación con la que se genera en el futuro, además permite la protección periódica de aplicaciones y datos en tiempo real, protege Exchange, SQL, SharePoint, BES, Oracle, MySQL y más. (Vision Solutions, 2015)
- **Veeam Backup & Replication:** Es mucho más que backup; ofrece una recuperación rápida, flexible y fiable de las aplicaciones y los datos virtualizados. Se junta el backup y la replicación en una solución única para reinventar la protección de datos y ofrecer el backup de VM número 1 para los entornos virtuales de VMware vSphere y Microsoft Hyper-V. (Veeam, 2015)

2.8. Métodos y Políticas de Respaldo

2.8.1. Introducción.

Hoy en día para los profesionales del área de las Tecnologías de la información y de las comunicaciones, lo más importante es la información. Archivos, bases de datos, e incluso imágenes que pueden ser el activo más importante de una empresa.

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, con el fin de contar con la mayor parte de la información para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

La importancia radica en que todos los dispositivos de almacenamiento masivo de información tienen la posibilidad de fallar, por lo tanto, es necesario que se cuente con una copia de seguridad de la información importante, ya que la probabilidad de que 2 dispositivos fallen de manera simultánea es muy difícil.

Algunos ejemplos de medios de respaldo son cinta, DVD, BluRay, discos virtuales (proporcionados por Internet) o simplemente en otro disco duro. Esto sistemas se usan posteriormente para recuperar o restaurar los datos o la información en el equipo original, ya sea un Computador, Servidor o Base de Datos en caso que se requiriese por pérdidas o corrupción de la información.

Los principales usos de los respaldos son:

1. Restaurar un Computador / Servidor a un estado operacional después de un desastre (copias de seguridad del sistema)
2. Para restaurar un pequeño número de archivos o Base de datos después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos).
3. Para recuperar la información a un punto del tiempo ya pasado con fines de obtener reportes, e informes de determinada fecha, o periodo de tiempo.
4. En la empresa, además es útil y obligatorio, para evitar ser sancionado por los órganos de control en materia de protección de datos, (Bancos, Balances de Empresas) o para consideraciones de certificación en las normas ISO. (Hernandez Zapardiel).

2.8.2. Tipos de Respaldo.

- **Completo (Full):** Se respaldan todos los archivos, y se va eliminando cada vez que se realiza. Se puede recuperar toda la información.
- **De Incremento (Incremental):** Se guardan únicamente los archivos que han cambiado desde la última vez que se realizó el respaldo. Es más rápido. Con el ultimo respaldo Completo y de todos los Respaldos de Incremento siguientes se puede recuperar el Sistema
- **Diferencial (Differential):** Se guardan los archivos que hayan cambiado desde el último Respaldo Completo. No se borran los Backup, y solo se

requiere del último Respaldo Completo y del último respaldo Diferencial para la recuperación de archivos. (NETGLOBALIS, 2012)

2.8.3. Métodos para el respaldo de información.

- **Manual:** El administrador copia directamente los archivos a respaldar por medio de comandos o por medio del explorador de archivos de su respectivo sistema operativo.
- **Automático:** por medio de una aplicación, el administrador programa los archivos a guardar, el mismo que se va actualizando en tiempo real (simultáneamente), conforme se van registrando cambios en los archivos. (Bligoo, 2015)

2.8.4. Dispositivos y servicios para respaldo de información.

Conforme aumenta la capacidad de almacenamiento de los dispositivos de información, también los usuarios tienden a necesitar guardar mayores cantidades de datos (videos, música, archivos de Office, imágenes, etc.). En la mayoría de empresas se manejan grandes volúmenes de información, por lo que es indispensable respaldar bases de datos, reportes, correo electrónico, etc.

Entre los dispositivos y servicios para respaldo de información están los siguientes:

- **Cintas de almacenamiento:** son los dispositivos que más se usan día a día, debido a su bajo costo y gran capacidad de almacenamiento, aunque la gran desventaja es su lentitud. Desde el dispositivo de almacenamiento principal, se copian los archivos hacia la unidad que escribe/lee las cintas.
- **Servidores Web:** actualmente por medio de Internet, es posible subir los archivos a respaldar al servidor de algún proveedor, esto se hace por medio de la red. Tiene la desventaja de que la conexión tiene que ser muy

veloz y segura, para evitar que los datos sean interceptados mientras llegan al servidor.

- **Discos duros:** actualmente estos son los que dominan el mercado, ya que cuentan con una muy alta capacidad para guardar datos, tanto en empresas como en el entorno doméstico ya que tiene una alta velocidad de lectura/escritura. Simplemente se copian los archivos del dispositivo primario al disco duro.
- **Discos espejo de servidores:** Es la copia automática entre discos duros mientras se trabaja de manera normal, es decir, un servidor anexo va clonando las acciones del servidor principal mientras exista modificación. Esto se logra mediante una aplicación especial instalada en ambas computadoras, con lo cual si el disco principal falla, se activa el otro disco mientras se resuelve la avería del sistema. (InformaticaModerna, 2015)

2.8.5. Políticas de seguridad de la información.

Una política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

El propósito de las políticas de seguridad de la información es proteger la información y los activos de datos de una Empresa. Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

CAPITULO III

INSTALACION DE LA NAS EN EL DATACENTER DE GRUPO EL COMERCIO COMO FASE INICIAL PARA MINIMIZAR LOS RIESGOS DE FALLAS DEL SERVIDOR PREPRENSA

3.1. Situación Actual.

3.1.1. Análisis de la situación inicial y sus problemas.

Los servidores son equipos informáticos importantes, el hardware que contienen es capaz de funcionar durante varios años, las 24 horas del día, los 7 días de la semana.

La vida útil de estos equipos en gran manera dependerá de una correcta selección al momento de adquirirlos y de realizar los mantenimientos preventivos y correctivos en tiempo y forma. Varios expertos mencionan que el tiempo de vida útil de un servidor va de 3 a 5 años de funcionamiento.

Como se mencionó anteriormente, el servidor Preprensa es uno de los servidores más importantes de la empresa, pero actualmente este equipo se encuentra obsoleto ya que tiene alrededor de 8 años de trabajo. Otras problemáticas que presenta son el reducido espacio de disco y la lentitud a la hora de responder a los usuarios.

Actualmente la data se respalda en un disco externo lo que no es muy seguro poniendo así en riesgo la información y no brindando seguridad a la misma. El servidor solo se encuentra conectado a la LAN (ver figura 22), lo que dificulta tener respaldos de forma rápida a un sistema dedicado a esta función por ejemplo (respaldo en cintas, respaldo en disco, etc.)

Para un mejor servicio a los usuarios es necesario invertir en un servidor de última generación, con mayor espacio en disco, mejor procesador y memoria;

además es importante renovar el sistema operativo para aprovechar las características de hardware.

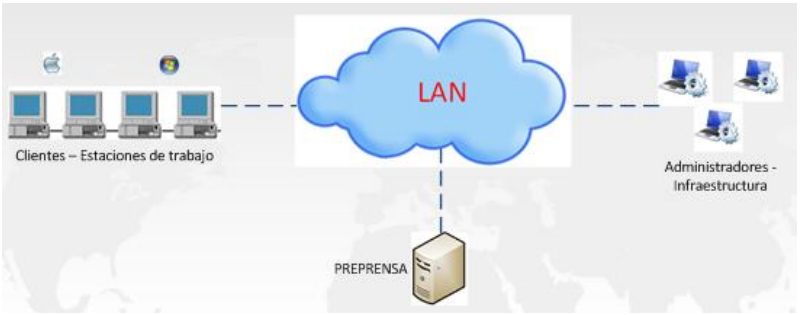


Figura 22 Servidor Preprensa en la LAN

Fuente: (Autor)

3.1.2. Ventajas con la migración.

Es importante renovar los servidores de una empresa, a pesar de la gran inversión que esto implica ya que una renovación aportará seguridad y tranquilidad a la estructura informática, a prevenir de parones inesperados y averías por sorpresa, ya que estas averías pueden salir cara a la empresa.
Existen diversos motivos para realizar una migración, tales como la preservación o difusión de los contenidos, mejoras en el funcionamiento, cumplir con nuevos requerimientos de usuario o de software, la interoperabilidad, la actualización de versiones, la estandarización de la tecnología, el aumento en el volumen de datos, nuevos procesos de negocio o mejoras en la seguridad o el control de la información, entre otros escenarios posibles.

Con la migración se pretenderá solucionar los problemas que anteriormente se nombraron, garantizando así un mejor servicio al usuario y otorgando seguridad de la información.

3.2. Propuesta inicial a implementar para minimizar el riesgo de fallas en el servidor Preprensa.

3.2.1. Introducción

Con el fin de minimizar el riesgo de fallas en el servidor denominado Preprensa de Grupo El Comercio C.A se ha visto la posibilidad de migrar su información a un nuevo servidor con mejores características y potencialidad, el cual es apto para cumplir con las necesidades del usuario.

El servidor de Preprensa actualmente es un servidor de archivos en el cual se aloja información muy importante para la empresa, lo cual es prescindible para el negocio. En este servidor se encuentra información como: avisos comerciales, imágenes, publicidad las cuales son trabajadas para los distintos productos que ofrece la Compañía.

En estos últimos años, se ha tenido varias quejas de los usuarios que hacen uso de este servidor, como por ejemplo lentitud a la hora de abrir una carpeta o archivo, archivos que se pierden sin ninguna explicación, etc., lo cual dificulta el trabajo diario de los empleados. Desde el punto de vista del administrador al tener estas quejas se ha observado que el equipo se llega a saturar llegando a estar en picos del 80 al 100 % del consumo de memoria y CPU por lo que nos vemos obligados en reiniciar el servidor para poder liberar memoria lo que implica indisponibilidad a los usuarios, además de tener espacio limitado en el server; con respecto a la seguridad de los archivos se complica debido a que no existe implementada una política de respaldo por lo que los usuarios tienen que volver a empezar con su trabajo, ahora esto es más crítico debido a que se va a almacenar los pdfs generados por el sistema editorial de las distintas ediciones, mismos que son utilizados para imprimir en las placas que utiliza la prensa para las ediciones impresas así como para subir al sistema que procesa las ediciones para los dispositivos móviles.

Por tal razón y viendo la criticidad de este servidor se decide migrar hacia un servidor tipo NAS el cual tiene mejores características en cuanto a hardware y

mayor almacenamiento, además se tendrá un control ordenado de las distintas carpetas con el uso de cuotas, con esto se garantizará un mejor rendimiento y administración del servidor.

3.2.2. Estudio comparativo de las características de los servidores entre el servidor a migrar y el servidor NAS.

Grupo El Comercio y los analistas de Infraestructura han montado su infraestructura con servidores HP, los cuales han brindado buenos resultados por su tecnología y su facilidad de administración.

El servidor que actualmente se encuentra operativo es un servidor HP Proliant DL380 G4 (ver figura 23) que fue ensamblado y adquirido en el año 2006, ha sido el servidor más vendido en el mundo debido a su disponibilidad y capacidad de gestión de categoría empresarial, pero al ser este servidor obsoleto y analizar el crecimiento de la Data se ha optado por implementar un servidor tipo NAS, específicamente un Storage Server HP StorageWorks X1800 (ver figura 24), el cual es una solución de almacenamiento compartido de gran capacidad y fácil de manejar.

Figura 23 Servidor HP Proliant DL380 G4

Fuente: (Autor)

Figura 24 Servidor HP StorageWorks X1800

Fuente: (Autor)

A continuación, se muestra en la tabla 5 las especificaciones generales de los servidores antes mencionados.

Tabla 5
Características generales de los servidores HP Proliant DL380 G4 y HP StorageWorks X1800

ESPECIFICACIONES	HP PROLIANT DL380 G4	HP STORAGEWORKS X1800 STORAGE SERVER
Procesador	Hasta 2 procesadores dual core Intel Xeon a 3.2 GHZ, 3.4 GHz ó 3.6 GHz con 1MB de caché de segundo nivel	Hasta 2 procesadores multi core Intel Xeon 2.4 o 2.6 Ghz con 8 MB de cache
Memoria	Memoria máxima soportada 12 GB, tecnología DDR2	Memoria máxima soportada 32 GB, tecnología DDR3 SDRAM (posibilidad de hacer transferencias de datos más rápidamente)
Controlador de almacenamiento	Controlador Smart Array 6i plus (integrado en la placa del sistema) O bien Smart Array P600 con caché de escritura respaldada por batería opcional de 256 MB (modelos SAS)	Smart Array P410i en ranura integrada o bien Smart Array P812 RAID - SATA 3Gb/s / SAS 6Gb/s (doble de potencia en su desempeño)
Número de Bays disponibles	8 Bays 3.5" discos SCSI	16 Bays 2.5" discos SAS y FATA
Arreglo de discos soportados	Raid 0, 1, 5	RAID 0, 1, 5, 6, 10, 50, 60
Tarjeta de Fibra	Dispone de la ranura para instalar soporta hasta 4 GB	Dispone tarjeta de fibra con 2 puertos de 8 GB
Sistemas Operativos compatibles	Microsoft Windows Server 2000 Microsoft Windows Server 2003 NovellNetWave Linux (Red Hat, SuSE) SCO UnixWare, OpenServer Vmware Virtualization Software	Microsoft Windows Storage Server 2008 Standard x64 Vmware Virtualization

Fuente: (Autor)

El servidor X1800 tiene un cambio considerable en la forma de cómo un servidor debe integrar la plataforma informática de los centros de datos desde una pequeña hasta una gran empresa, es ideal para todo tipo de clientes y responde a las actuales demandas de eficiencia de energía.

Este servidor además del ahorro de energía permite centralizar los archivos consolidando elementos independientes de almacenamiento en una sola plataforma. Se instala en una amplia variedad de entornos de servicios de

archivos heterogéneos, con compatibilidad con los protocoles SMB/CIFS, NFS, HTTP, FTP y WebDAV.

A continuación, se observa en la tabla 6 las diferentes configuraciones implementadas en cada servidor.

Tabla 6
Configuraciones implementadas en los servidores DL380 y X1800

Especificaciones/Modelo	HP PROLIANT DL 380	HP STORAGEWORKS X1800 STORAGE SERVER
Generación	Generación 4	Generación 6
Procesador	1 Dual Core Intel Xeon (TM) 3 GHz (2 Cpus)	2 Quad Core Intel Xeon E5530 2,4 GHz (8 cpus)
Memoria RAM	1 GB	18 GB
Sistema Operativo	Windows Server 2003 R2 Standard Edition	Windows Storage Server 2008 Standard Edition
Tipo de discos	2 discos SCSI 10k 36,4 GB	16 discos SAS 6G DP 10K 300 GB
	2 discos SCSI 10k 300 GB	
	2 discos SCSI 15k 300 GB	
Controladora de almacenamiento	Smart Array 6i Embebida	Smart Array P812 en Ranura 4
Arreglo de discos	SCSI Array A: RAID 1 (2 discos SCSI 10k 36,4 GB) (Para unidad C)	SAS Array A: RAID 1 (2 discos SAS 300 GB) (Para unidad C)
	SCSI Array B: RAID 1 (2 discos SCSI 10k 300 GB) (Para unidad F)	SAS Array B: RAID 5 (6 discos SAS 300 GB) (Para unidad F)
	SCSI Array C: RAID 1 (2 discos SCSI 15k 300 GB) (Para unidad F)	SAS Array C: RAID 5 (8 discos SAS 300 GB) (Para unidad D)
Tamaño Unidades de discos	Unidad C: 32 GB aprox.	Unidad C: 279 GB aprox.
	Unidad F: 560 GB aprox.	Unidad F: 1,28 TB aprox.
		Unidad D: 1,90 TB aprox.
Configuración Network Team	Deshabilitado	Habilitado
Tarjeta de Fibra instalada	No	Si

Fuente: (Autor)

Vemos que el servidor NAS posee mejores características tanto en Hardware como en Software, mayor almacenamiento llegando a quintuplicar el actual. En comparación a los discos, el servidor NAS posee discos SAS los cuales presentan una velocidad de transferencia de 6 GB/s a comparación de los discos SCSI que trabajan a 320 MB/s. La controladora Smart Array P812 tiene un alto regulador de potencia y rendimiento, proporciona nuevos niveles de conectividad de almacenamiento y soporta hasta 108 unidades de disco

Con esto se puede garantizar que el servicio hacia los usuarios va a ser óptimo ya que el nuevo servidor Preprensa será robusto a nivel de hardware e inteligente a nivel de sistema operativo y administración.

3.2.3. Estudio de los tipos de arreglos de discos

Un arreglo de discos es conocido también como RAID (Redundant Array of Independent Disks), consiste en la organización de múltiples discos para formar una única unidad lógica en la que se almacenan los datos de forma redundante y ofrecen mayor funcionalidad.

3.2.3.1. Ventajas de un RAID

- El rendimiento general del sistema aumenta
- Si uno de los discos falla, la unidad continúa funcionando, sin pérdida de tiempo ni de datos.
- Ofrece más fiabilidad de almacenamiento de datos
- La reconstrucción de los datos del disco que ha fallado se hace de forma automática sin intervención humana.

3.2.3.2. Tipos de RAID

Existen varios tipos de arreglos, pero los más utilizados a nivel general son: RAID 0, RAID 1 y RAID 5 los cuales se detallan a continuación.

- **RAID 0**

Este tipo de RAID no proporciona redundancia, pero maneja varios discos como si fuera uno solo, lo que brinda mayor velocidad de lectura y escritura, (ver figura 25). La desventaja de este tipo de arreglo es que si un disco falla el sistema se cae, es decir, habría una pérdida total de los datos.

Hay que tomar en cuenta que, si uno de los discos que lo componen es menor en capacidad, ésta determinará el tamaño para el resto de discos, aunque tengan una capacidad mayor.

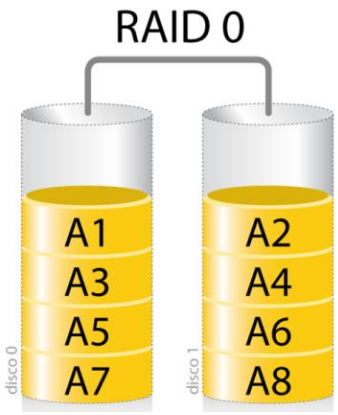


Figura 25 Tipo de arreglo RAID 0

Fuente: (Wikipedia, 2015)

- **RAID 1**

También conocido como “mirroring” o “modo espejo”, este tipo de arreglo es utilizado para garantizar la integridad de los datos, es decir, en caso de fallo de un disco duro, es posible continuar las operaciones en el otro disco sin ningún problema ya que el modo RAID 1 duplica todos los datos de cada unidad de almacenamiento de forma sincronizada a otra unidad de almacenamiento, (ver figura 26).

La desventaja de este tipo de configuraciones es el gran sacrificio de espacio que supone. Sí, al trabajar en modo espejo se realizan copias redundantes de datos, de forma que, si tenemos, por ejemplo, dos HDDs de 1 TB en RAID 1 no

disfrutaremos de 2 TB totales de espacio, sino de 1 TB, ya que el segundo TB será utilizado para las grabaciones redundantes.

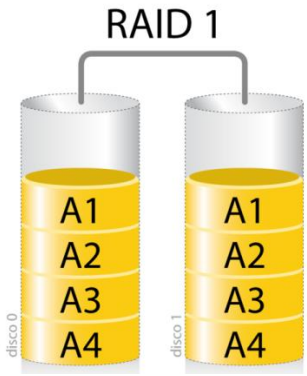


Figura 26 Tipo de arreglo RAID 1

Fuente: (Wikipedia, 2015)

- **RAID 5**

Este tipo de arreglo se denomina también como distribuido con paridad, debido a que distribuye la información en todo el conjunto de discos, (ver figura 27). A diferencia del RAID 0, RAID 5 elabora un bit de paridad con el cual es posible reconstruir la información del arreglo en caso de la pérdida de alguno de los discos. La información y los bits de paridad son distribuidos en todos los discos, garantizando que siempre se encontrarán en discos distintos. RAID 5 tiene un mejor desempeño que RAID 1, pero cuando uno de los discos falla, el desempeño de la lectura llega a degradarse.

Este tipo de arreglos es el más usado a nivel empresarial, pero debemos tener en cuenta que si se utiliza discos SATA de gran capacidad (a partir de 500 GB) los tiempos de reconstrucción son más largos, lo que provocaría una degradación a mediano plazo del rendimiento del controlador por lo que es recomendable utilizar discos SAS.

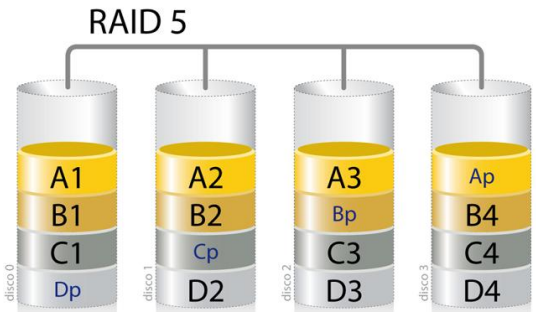


Figura 27: Tipo de arreglo RAID 5

Fuente: (Wikipedia, 2015)

3.2.4. Análisis de crecimiento.

Debido al constante crecimientos de datos que genera la empresa hoy en día, se ha vuelto muy necesaria la búsqueda de una solución con mayor almacenamiento para satisfacer las necesidades que actualmente se requiere.
El problema de crecimiento de los servidores de archivos no va a desaparecer debido a que la empresa se ve obligada a conservar datos durante períodos más prolongados para cumplir la normativa expuesta en la ley de comunicación.
Actualmente el servidor de generación 4 tiene una unidad de almacenamiento de 900 GB de lo cual se encuentra usado el 99%, es por esto que con la implementación de servidor tipo NAS tendremos mayor almacenamiento interno con la ventaja de expandir el espacio presentando otras unidades desde un Storage externo conectado en la mima Red.

Para administrar de mejor manera el file server se hará uso de la administración de cuotas de archivos, esta funcionalidad es muy importante ya que el almacenamiento en el servidor es costoso, por lo tanto, otorgarle permisos a los usuarios que guarden cuanta cosa quieran es un gran error. Las cuotas del sistema de archivos restringen la cantidad de espacio que los usuarios pueden consumir, además de obtener informes o reportes sobre los usuarios o las carpetas que están consumiendo grandes cantidades de espacio en disco.

Con esto podremos analizar el crecimiento anual del servidor y si existen archivos basuras que no son necesarios para el fin del negocio de la empresa.

3.3. Estudio del sistema de migración a utilizar.

Después de investigar varios sistemas de migración se optó por utilizar el software *Uranium Backup*, el cual es un software de copia de seguridad ligera y fiable que sirve para proteger los datos personales y empresariales. Uranium Backup puede realizar copias de seguridad de archivos y carpetas, imágenes de discos, bases de datos y máquinas virtuales en muchos tipos diferentes de periféricos de almacenamiento, como NAS y cintas, y lo más importante es que puede realizar la copia no solo de archivos y carpetas sino también de los atributos de seguridad. (Nanosystems S.r.l. , 2015)

Las licencias de Uranium tienen una duración de por vida y permiten realizar una única instalación del programa en una máquina física o virtual, a continuación, en la tabla 7 se observará las diferentes características y funcionalidades que tiene cada licencia.

Tabla 7

Licencias de Uranium Backup

FUNCIONALIDADES DE LAS DISTINTAS LICENCIAS DE URANIUM BACKUP						
Uranium Backup Free	**Uranium Backup Base**	**Uranium Backup Pro Tape**	**Uranium Backup Pro DB**	**Uranium Backup Pro Shadow**	**Uranium Backup Pro Virtual**	**Uranium Backup Gold**
Planificación, registros	Planificación, registros	Planificación, registros	Planificación, registros	Planificación, registros	Planificación, registros	Planificación, registros
-	Sincronización	Sincronización	Sincronización	Sincronización	Sincronización	Sincronización
-	Servicio	Servicio	Servicio	Servicio	Servicio	Servicio
-	Grabación en CD/DVD/BD	Grabación en CD/DVD/BD	Grabación en CD/DVD/BD	Grabación en CD/DVD/BD	Grabación en CD/DVD/BD	Grabación en CD/DVD/BD
-	Backup en FTP	Backup en FTP	Backup en FTP	Backup en FTP	Backup en FTP	Backup en FTP
-	Imágenes de disco	Imágenes de disco	Imágenes de disco	Imágenes de disco	Imágenes de disco	Imágenes de disco
-	-	Backup en cinta	Backup de Exchange/SQL	Instantánea (VSS)	Instantánea (VSS)	Backup en cinta
-	-	-	-	-	Backup de MVs ESX/ESXi	Backup de Exchange/SQL
-	-	-	-	-	-	Instantánea (VSS)
-	-	-	-	-	-	Backup de MVs ESX/ESXi

Fuente: (Nanosystems S.r.l. , 2015)

Para nuestro caso haremos uso de la licencia FREE la cual nos permite migrar los datos de un servidor al otro y lo más importante de todo es que se podrá migrar con los permisos de seguridad de cada carpeta y archivos que tiene actualmente en el servidor origen, haciendo así transparente para el usuario final el momento que se cambie de equipo.

Uranium Backup Free es un software fiable que incluye una herramienta de planificación completa, un sistema de informes completo con notificación por correo electrónico. (Nanosystemns, 2016).

Principales Ventajas de Uranium Backup Free

- **Transferencia de datos y duplicación de archivos**

Puede copiar archivos y carpetas en prácticamente cualquier dispositivo de almacenamiento masivo: discos duros USB/Firewire/SATA externos, unidades RDX/REV, dispositivos NAS, etc.

- **Orígenes y destinos ilimitados**

La gran flexibilidad permite configurar tareas de copia de seguridad con un número ilimitado de elementos de origen y copiar los datos en un número ilimitado de ubicaciones, también con ejecuciones en paralelo y un alto rendimiento.

- **Exclusión de la copia de seguridad carpetas y archivos específicos**

Ahorra espacio de almacenamiento en los dispositivos de copia de seguridad y consigue un mejor rendimiento de la copia de seguridad excluyendo archivos y carpetas específicos de la copia de seguridad. Uranium permite configurar fácilmente filtros avanzados basados en extensiones de archivos (inclusión y exclusión), rutas de acceso específicas e incluso rutas de acceso parciales o dinámicas.

- **Compresión ZIP y cifrado AES 256 bits**

Uranium puede comprimir archivos y carpetas utilizando la eficaz y altamente compatible compresión Zip64 con el fin de ahorrar espacio de almacenamiento.

También puedes cifrar tus datos con el algoritmo más seguro que existe hoy en día: AES 256 bits.

- **Copia de permisos NTFS (ACL)**

Uranium Backup puede copiar y sincronizar también atributos de seguridad de NTFS (ACL) y, por tanto, es posible mantener los permisos existentes que se han aplicado específicamente a los archivos o a las carpetas.

- **Planificación de copias de seguridad automáticas**

Uranium Backup incluye una herramienta de planificación automática y flexible, para poder configurar las copias de seguridad del ordenador en cualquier momento sin que tengan que recordártelo. Uranium también puede ejecutarse como servicio de Windows, para que funcione de manera automática y transparente en segundo plano, sin necesidad de que un usuario haya iniciado sesión en el sistema.

- **Eficaz sistema de notificaciones por correo electrónico**

Después de cada copia de seguridad, Uranium Backup puede enviar una notificación por correo electrónico que indica si la copia de seguridad se ha realizado correctamente. Uranium ofrece uno de los sistemas más completos y eficaces de notificación por correo electrónico con numerosas opciones, condiciones y parámetros.

3.4. Implementación de la NAS en el Datacenter de Grupo El Comercio

3.4.1. Armado e Instalación de la NAS en el Datacenter.

El servidor HP StorageWorks X1800 fue adquirido y ensamblado con las con las siguientes características.

- 2 procesadores Intel Xeon E5530
- 9 memorias RAM 2GB 2RX8 PC3 10600R-9
- 16 discos SAS 6G DP 10K de 300 GB
- 2 fuentes de poder

- 1 tarjeta de fibra con 2 puertos
- 2 transceptores de fibra de 8GB
- 6 ventiladores

Antes de realizar el ensamblado de cualquier servidor se debe tener en cuenta las siguientes normas de seguridad.

1. Utilizar manilla antiestática para evitar las descargas que pueden dañar el equipo.
2. Antes de abrir la carcasa del servidor asegurarse que se encuentre desconectado los cables de corriente, video, dispositivos USB, etc.
3. Tocar la parte metálica del equipo por lo menos 15 segundos para evitar que nuestra energía estática dañe algún componente cuando se manipule.
4. Al desconectar o conectar alguna pieza no se la debe forzar sino entra, esto podría partirla o doblarla.
5. Tratar de no tocar mucho los chips de los componentes, debido a que podría provocar deterioro de los mismos.

Instalación de Procesadores.

La instalación de los procesadores es la parte más delicada ya que las pastillas de la placa del sistema son muy frágiles y se dañan fácilmente, es por eso que es muy importante no tocar las conexiones del zócalo, ni inclinar o deslizar el procesador al introducirlo en él.

Una vez colocado el procesador se debe asegurar de cerrar el soporte de sujeción del zócalo antes de cerrar la palanca de bloqueo del procesador. La palanca debería cerrarse sin oponer resistencia.

Para finalizar se debe instalar el disipador térmico sin tocar la parte inferior del dispositivo tras retirar la cubierta, (ver figura 28).

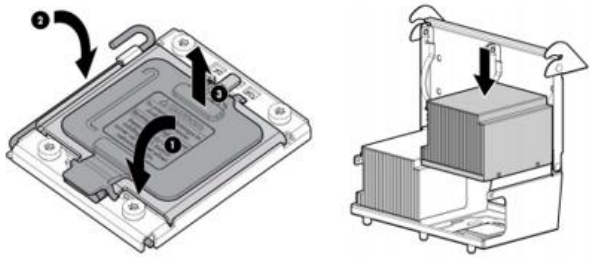


Figura 28 Instalación de procesador y disipador térmico

Fuente: (Autor)

Instalación de Ventiladores.

Para evitar dañar los componentes del servidor, los paneles lisos de los ventiladores deben instalarse en los compartimentos de ventilador 5 y 6 en una configuración de un único procesador.

Las dos únicas configuraciones válidas de ventiladores se enumeran en la tabla 8.

Tabla 8
Configuraciones válidas de ventiladores en el servidor X1800

Configuración	Compartimento del ventilador 1	Compartimento del ventilador 2	Compartimento del ventilador 3	Compartimento del ventilador 4	Compartimento del ventilador 5	Compartimento del ventilador 6
1 procesador	Fan	Fan	Fan	Fan	Panel liso para ventilador	Panel liso para ventilador
2 procesadores	Fan	Fan	Fan	Fan	Fan	Fan

Fuente: (Autor)

En una configuración de un único procesador, se necesitan cuatro ventiladores y dos paneles lisos en los compartimentos de ventiladores específicos para la redundancia, (ver figura 29).

La instalación de más ventiladores de los necesarios en una configuración de un único procesador no es una configuración compatible.

Para una configuración de dos procesadores como en este caso, se necesitan seis ventiladores para la redundancia.

En ambos casos si falta un ventilador o se avería, todos los ventiladores giran a una alta velocidad. Si faltan dos ventiladores o se averían, se apaga el servidor de forma ordenada.

El servidor admite diversas velocidades del ventilador. Los ventiladores funcionan a la velocidad mínima hasta que, como consecuencia de un cambio de temperatura, sea preciso un aumento en la velocidad del ventilador para enfriar el servidor.

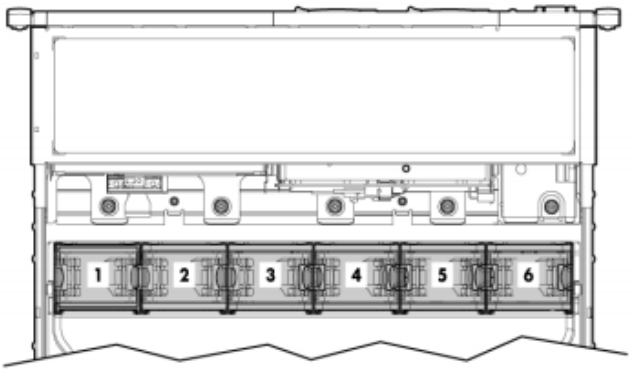


Figura 29 Ubicación de los ventiladores en el servidor

Fuente: (Autor)

Instalación de Memorias RAM.

El subsistema de memoria del servidor admite memorias RDIMM o UDIMM. Ambos tipos de memoria se denominan DIMM cuando la información se aplica a los dos. Todas las memorias instaladas en el servidor deben ser del mismo tipo. El servidor admite las siguientes velocidades de DIMM:

- Memorias DIMM de rango único y rango doble PC3-10600 (DDR-1333) a 1333 y 1066 MHz.
- Memorias DIMM de cuatro rangos PC3-8500 (DDR-1067) a 1066 MHz

El subsistema de memoria de este servidor se divide en dos canales. Cada procesador admite tres canales y cada canal admite tres ranuras DIMM, tal y como se muestra en la tabla 9.

Tabla 9
Arquitectura del subsistema de memoria

Canal	Ranura	Número de ranura
1	G	1
	D	2
	A	3
2	H	4
	E	5
	B	6
3	I	7
	F	8
	C	9

Fuente: (Autor)

Las ranuras DIMM se numeran de forma secuencial (de 1 a 9) en cada procesador. Los modos AMP compatibles utilizan las asignaciones de letras para las indicaciones de ocupación como se observa en la figura 30.

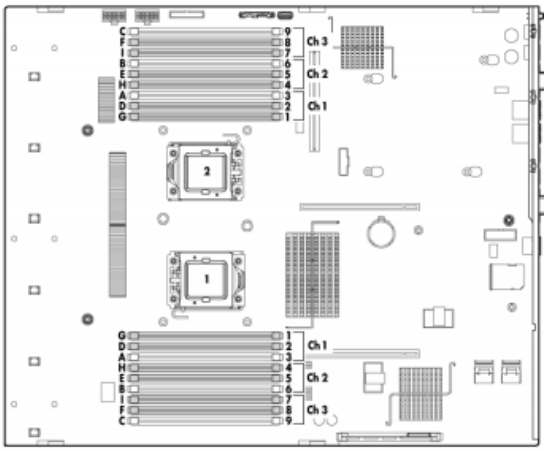


Figura 30 DIMM, ubicación de las ranuras

Fuente: (Autor)

Instalación del servidor en el Bastidor o Rack

El servidor puede montarse en cualquier Rack que cumpla las especificaciones de la norma EIA 310 (Electronic Industries Association 310). El servidor mide 8,6 cm (3,4 pulgadas) de altura, 44 cm (17,5 pulgadas) de ancho y 69 cm (27,3 pulgadas) de profundidad; requiere un espacio vertical de 2U

(unidades de Rack). Con esto se instaló en el Datacenter de Grupo El Comercio C.A. en el Rack denominado DCUIO06 (ver figura 31).

Figura 31 Servidor NAS montado en el rack DCUIO06 de Grupo El Comercio

Fuente: (Autor)

3.4.2. Configuración del Sistema Operativo.

Windows Storage Server 2008 fue desarrollado como un “appliance form-factor”, que significa que los requisitos de hardware y software son pre-configurados para simplificar las tareas de implementación que normalmente se asocian con un nuevo servidor de archivos. Esto también reduce en gran medida la cantidad de tiempo requerido para implementar mediante la eliminación de

varias tareas de administración y minimiza el impacto de la implementación de la Infraestructura en la organización, es decir, la instalación y configuración es mucho más rápida y simple.
A continuación, se detalla el paso a paso para configurar el servidor e instalar el sistema operativo.

Los servidores HP disponen de un servicio de consola remota llamado ILO que nos permite acceder en modo consola a servidores físicos a través de una red local, por lo cual el primer paso será configurar la ILO.
En la parte posterior del servidor se puede encontrar la entrada Ethernet identificada como ILO semejante a la figura 32. Conectamos un cable de red conectado a un switch de la red local.

Figura 32 Puerto Ethernet para ILO

Fuente: (Autor)

Al encender el servidor veremos el arranque del sistema y cuando aparezca el mensaje “Integrated Lights-Out 2 Advanced press [F8] to configure” presionamos F8 para ingresar a configurar la ILO, (ver figura 33).

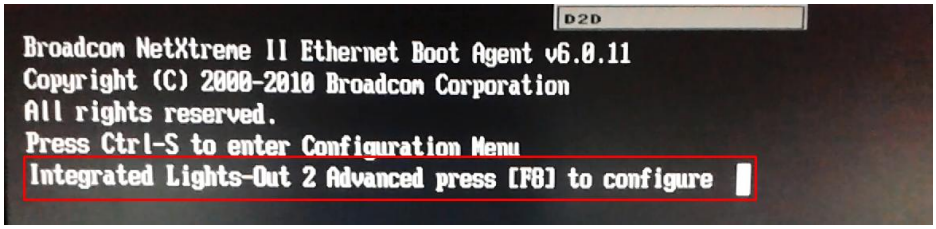


Figura 33 Ingreso a la configuración de la ILO

Fuente: (Autor)

Una vez dentro configuramos la IP, mascara y Gateway, comprobando que el DHCP se encuentre deshabilitado; adicional en caso de ser necesario configuramos el DNS. Normalmente el usuario para la administración es Administrator y el password suele venir en una etiqueta que cuelga del servidor, pero si se desea se puede crear un nuevo usuario en el menú User, (ver figura 34).

Figura 34 Configuración ILO

Fuente: (Autor)

Una vez configurada la iLO, el servidor continuará con el arranque y lo siguiente a configurar es el arreglo de discos, es recomendable e importante realizar este paso para poder garantizar alta disponibilidad del servidor en caso de daños de algún disco, ya que al no realizar esta configuración el sistema operativo se instalará en un arreglo de RAID 0 es decir sin ninguna protección de discos en caso de daños. Para ingresar a la configuración de Array presionamos F8 el momento que se muestre el siguiente mensaje ***"Press F8 to run Option ROM Configuration For Array Utility"*** como se observa en la figura 35.

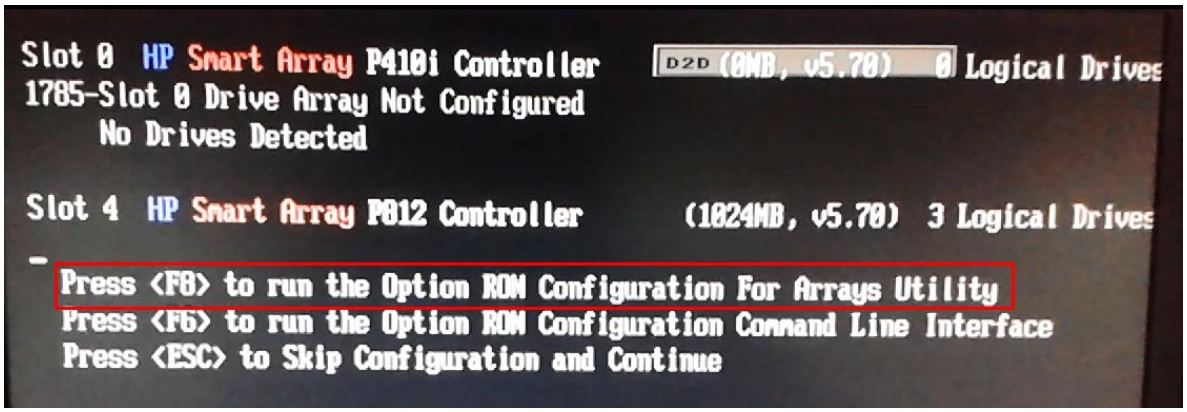


Figura 35 Ingreso a la configuración de arreglo de discos

Fuente: (Autor)

Esta configuración es abierta y se lo realizará según las necesidades que perciba el administrador de Infraestructura, en este caso al tener disponible 16 discos de 300 GB se ha decidido realizar 3 arreglos, (ver figura 36).

1. 2 discos en RAID 1 para la unidad C (Sistema Operativo)
2. 8 discos en RAID 5 para la unidad D (Datos)
3. 6 discos en RAID 5 para la unidad F (Datos)

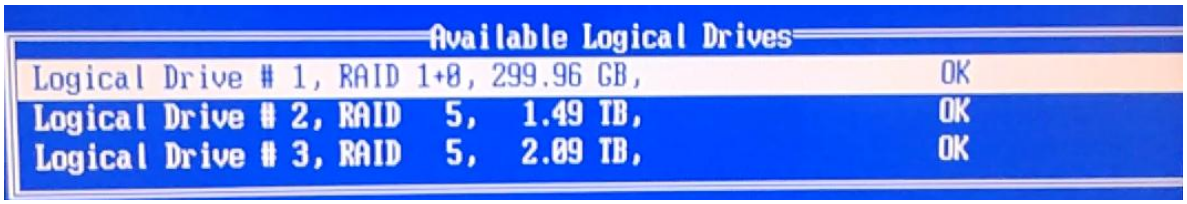


Figura 36 Configuración arreglo de discos

Fuente: (Autor)

En la figura 37 se detalla los arreglos y que discos están configurados en los mismos.

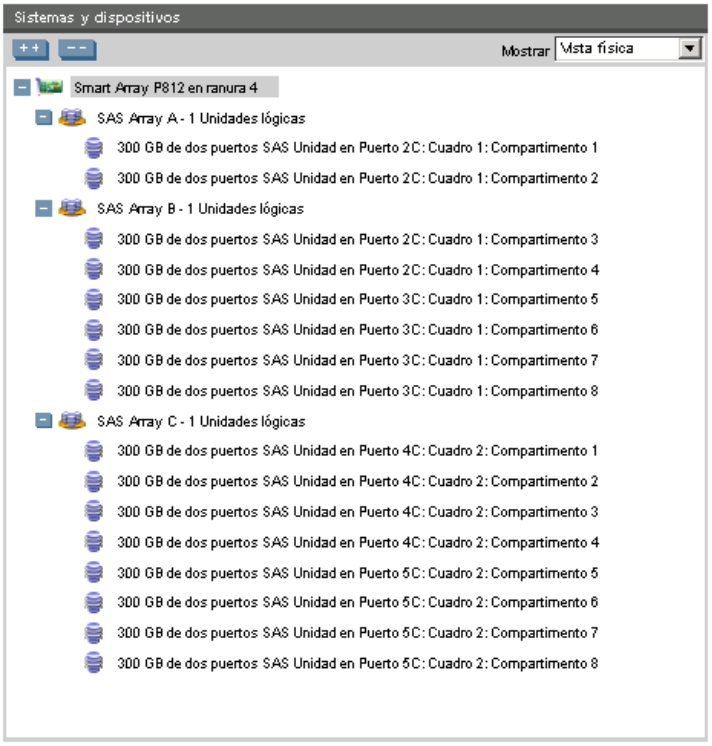


Figura 37 Resumen arreglo de discos

Fuente: (Autor)

Una vez finalizada la configuración del arreglo de discos, el siguiente paso es la instalación del SO, el servidor arrancará el appliance de Windows Storage Server 2008, en la ventana que se despliega escogemos el idioma de instalación y seleccionamos arrancar desde la imagen de fábrica como se observa en la figura 38.

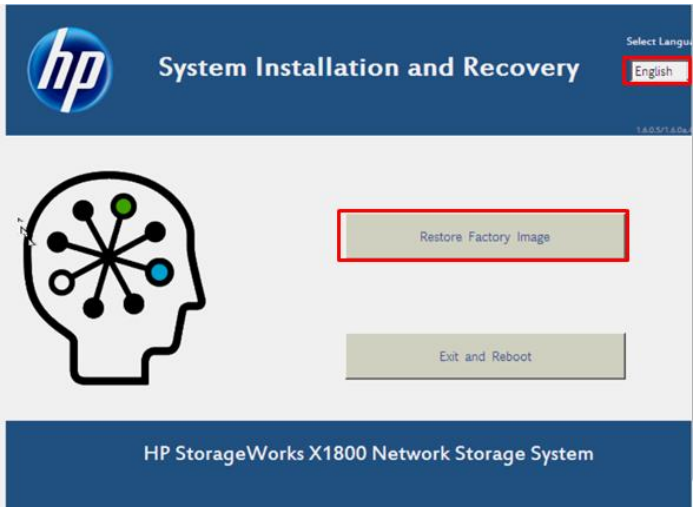


Figura 38 Arranque sistema de instalación WSS 2008

Fuente: (Autor)

Una vez que arranca desde el appliance se muestra una ventana en la cual comienza a descargar y copiar todos los archivos necesarios, (ver figura 39).

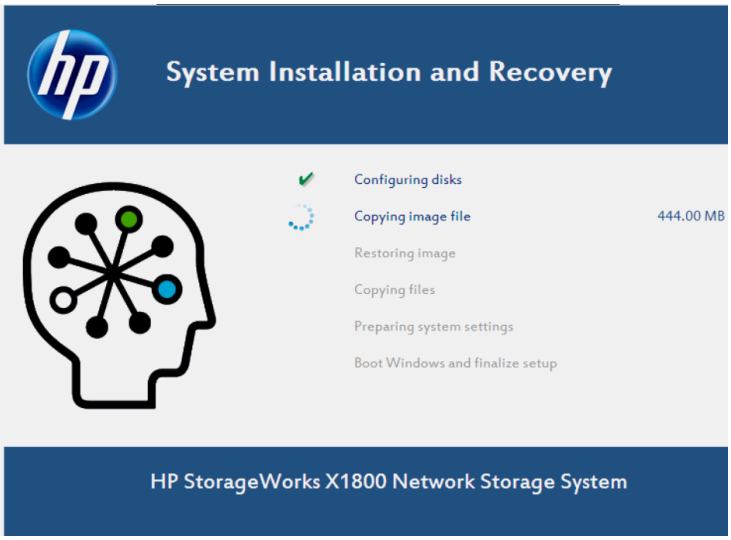


Figura 39 Preparación de la instalación de WSS 2008

Fuente: (Autor)

Una vez que concluya la descompresión de archivos nos mostrará las ventanas para escoger el lenguaje del sistema, la región, y propiedades del teclado como se muestra en la figura 40.

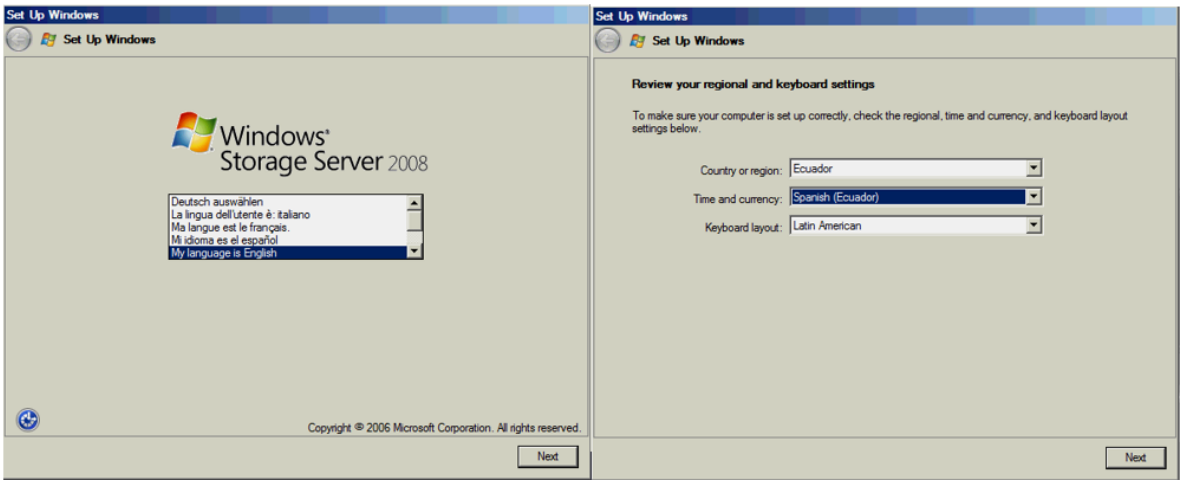


Figura 40 Configuración de idioma y teclado

Fuente: (Autor)

La siguiente pantalla son los términos de licencia de software, la cual debemos aceptar para continuar la instalación.

Figura 41 Términos de licencia WSS 2008

Fuente: (Autor)

Una vez aceptado los términos de licencia arrancará la instalación del sistema operativo como se observa en la figura 42.

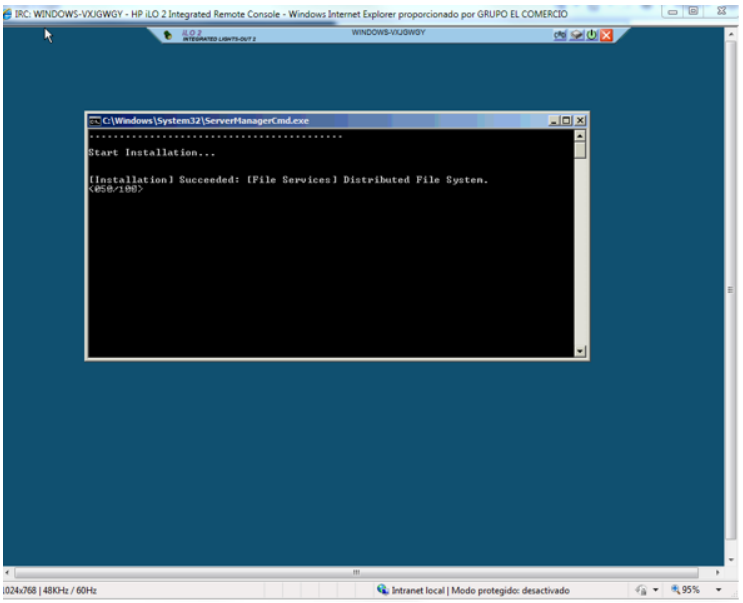


Figura 42 Instalación Sistema Operativo WSS 2008

Fuente: (Autor)

Una vez que se ha instalado el sistema Operativo y al arrancar el mismo se despliega un asistente de configuración inicial, (ver figura 43 y 44), en el cual configuraremos fecha y hora del sistema, red, nombre del servidor y carpetas que queramos compartir.

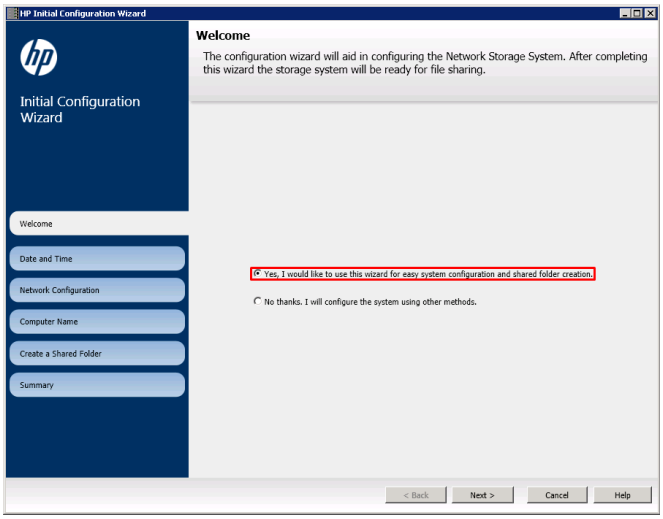


Figura 43 Asistente de configuración inicial

Fuente: (Autor)

Siguiendo con el asistente podemos cambiar la configuración de la fecha y hora del sistema

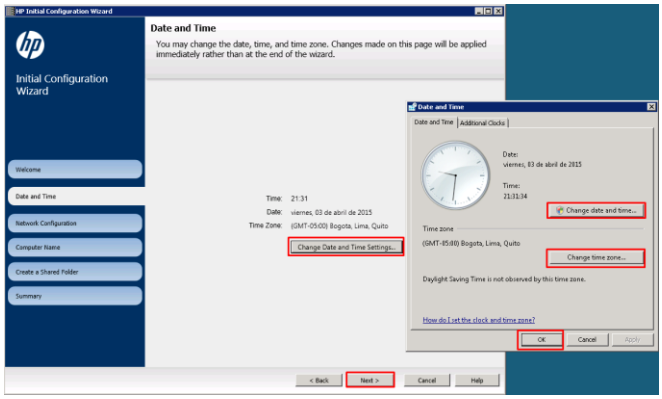


Figura 44 Configuración fecha y hora del sistema

Fuente: (Autor)

Seguidamente se configura los adaptadores de red que se desee, en esta ocasión se conectó dos puertos de red a la LAN, pero se configurará un solo puerto para más adelante realizar un team entre los dos, (ver figura 45). Hay que tomar en cuenta que el objetivo de este servidor es reemplazar a un obsoleto que se encuentra productivo por lo cual debemos configurar una Ip distinta o a su vez dejar que se asigne por DHCP.

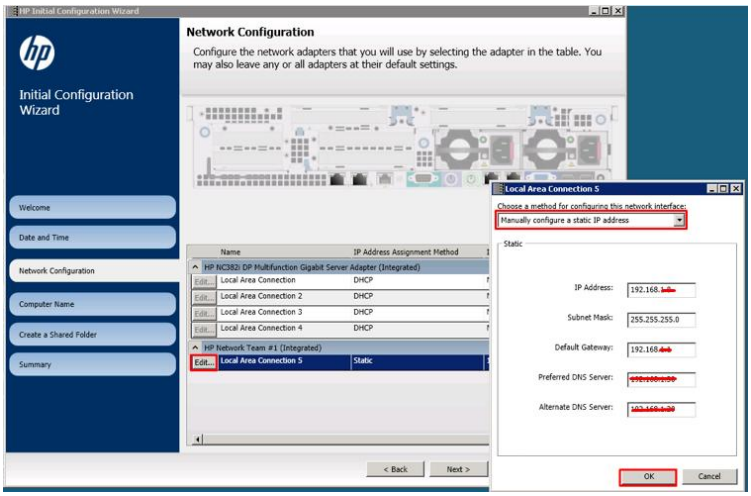


Figura 45 Configuración de red

Fuente: (Autor)

A continuación, configuramos el nombre del servidor, de igual forma se colocó un nombre distinto y no se agregó al dominio de la empresa.

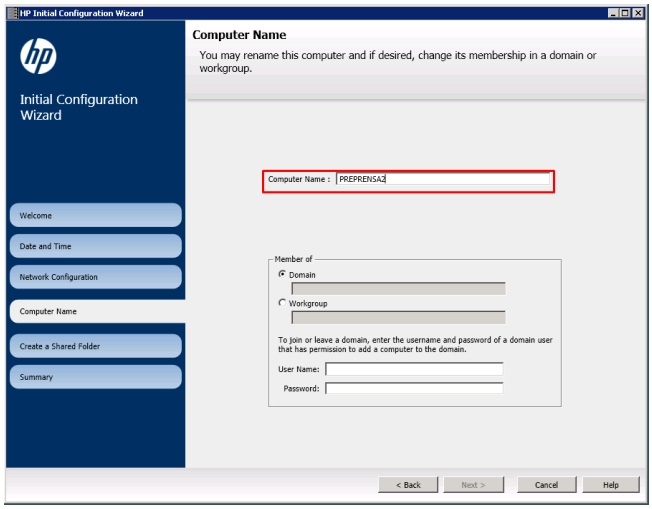


Figura 46 Configuración nombre del servidor

Fuente: (Autor)

Para finalizar configuramos la unidad a ser compartida y reiniciamos el servidor para que los parámetros se hagan efectivos.

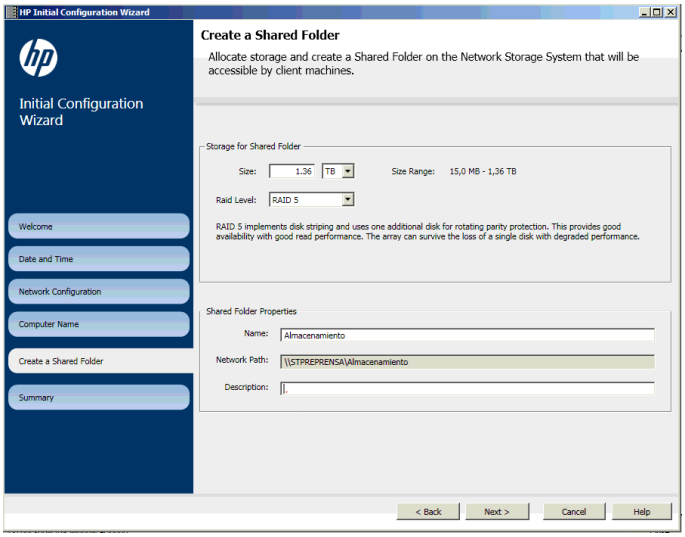


Figura 47 Configuración unidad de disco

Fuente: (Autor)

Con esto el servidor se encuentra listo para ser utilizado y migrar los archivos del servidor original a este.

Cabe recalcar que antes de poner a producción al servidor se configurará el team de la red, se cambiará el nombre del servidor, se ingresará al dominio y se configurará los caminos de fibra para conectar el servidor a la SAN.

3.5. Migración y Sincronización de la Data al nuevo equipo con los permisos y carpetas compartidas que posee el antiguo servidor.

Como se comentó en el apartado 3.2.4 para realizar la migración de los archivos se hará uso del software Uranium Backup, este software permite migrar la información en caliente sin afectar al trabajo de los usuarios y una de las ventajas fundamentales de este sistema es que nos permite migrar con los permisos de seguridad, evitando la engorrosa tarea de ir carpeta por carpeta dando los permisos que tienen en el servidor original.

A continuación, se describe los pasos de instalación y configuración de los Jobs para realizar la tarea de migración, hay que recalcar que para evitar cualquier saturación en el servidor origen se procedió a configurar las tareas de sincronización en el horario de menos flujo de trabajo.

La instalación del software no es compleja, basta con seguir las instrucciones por defecto, (ver figura 48); lo recomendable es realizar la instalación en el servidor origen en una sesión de administrador, con el fin de tener acceso a todos los archivos para evitar errores al momento de realizar la copia.

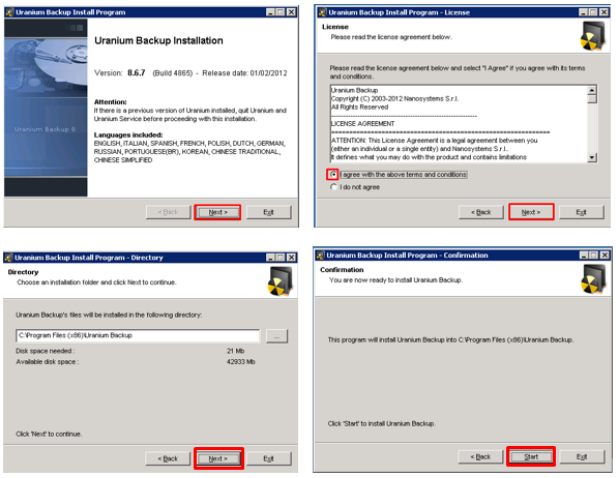


Figura 48 Instalación Uranium Backup

Fuente: (Autor)

Antes de iniciar con la creación de las tareas de respaldo se observó la estructura de carpetas que tiene el servidor original con el fin de dividir las tareas y mantener un orden en la sincronización, (ver figura 49).

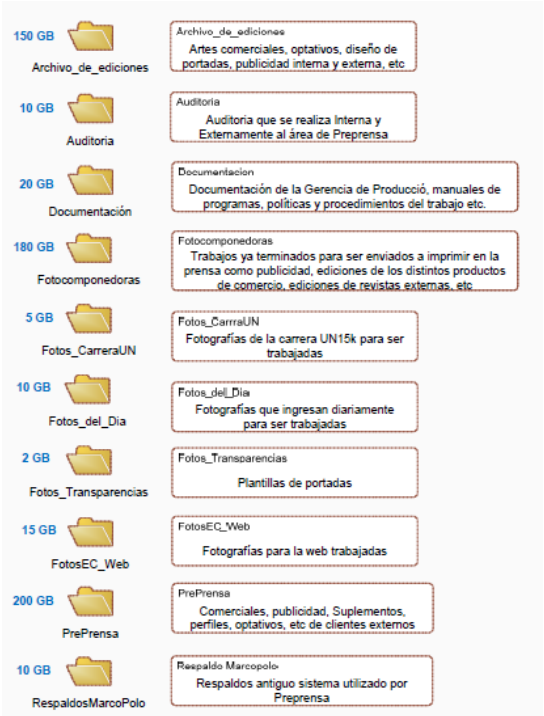


Figura 49 Estructura de carpetas servidor original

Fuente: (Autor)

Una vez analizada la estructura de carpetas e instalado Uranium Backup se procede a crear las tareas de copia y sincronización, en esta ocasión se realizará 8 tareas. A continuación, se detalla paso a paso para crear una tarea de respaldos con sus respectivas configuraciones.

- Abrir el programa y crear una tarea de backup, (ver figura 50).

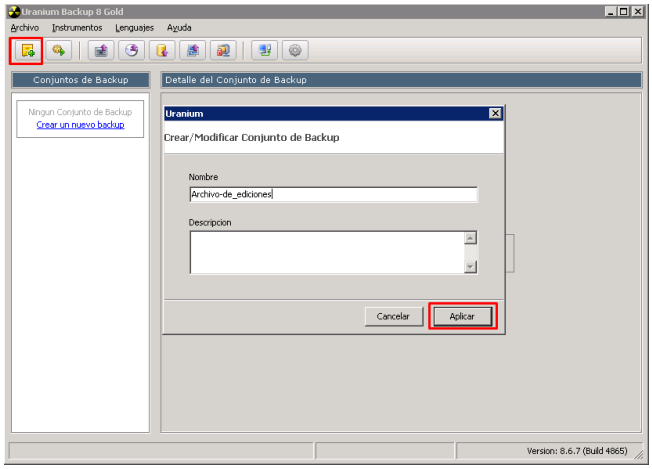


Figura 50 Creación nuevo Backup

Fuente: (Autor)

- Escoger la opción de *Elementos y destinos* para seleccionar la carpeta o carpetas a respaldar, y en Destino escogemos la ruta en la que se copiará la información. En esta ocasión la unidad de destino se encuentra mapeada en el servidor, (ver figura 51 y 52).

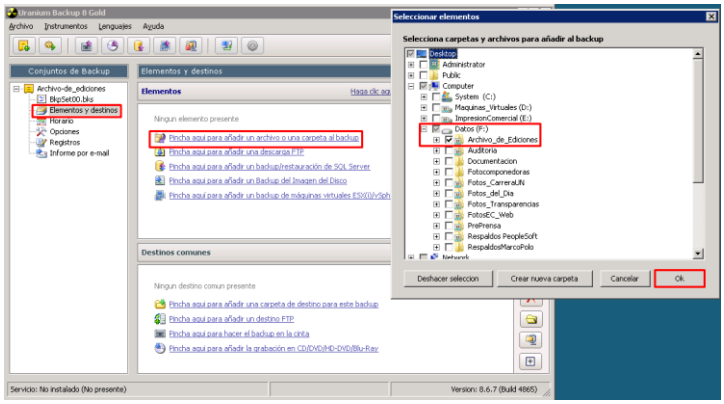


Figura 51 Selección de elementos a copiar

Fuente: (Autor)

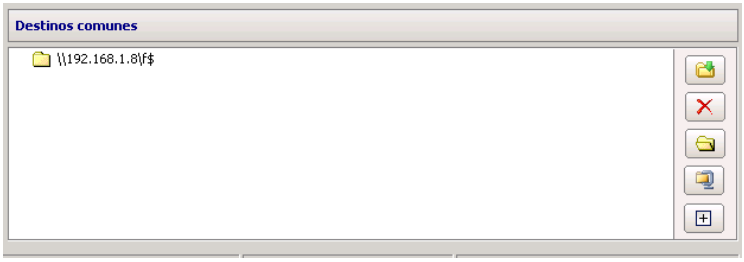


Figura 52 Selección de destino

Fuente: (Autor)

- En el Menú de opciones generales podemos configurar la manera que se desea que se cree la carpeta de destino, copia de archivos ocultos o bloqueados. En este caso se ha escogido que no se cree ninguna ruta en específica y que se realice la copia de archivos ocultos y bloqueados como se observa en la figura 53.

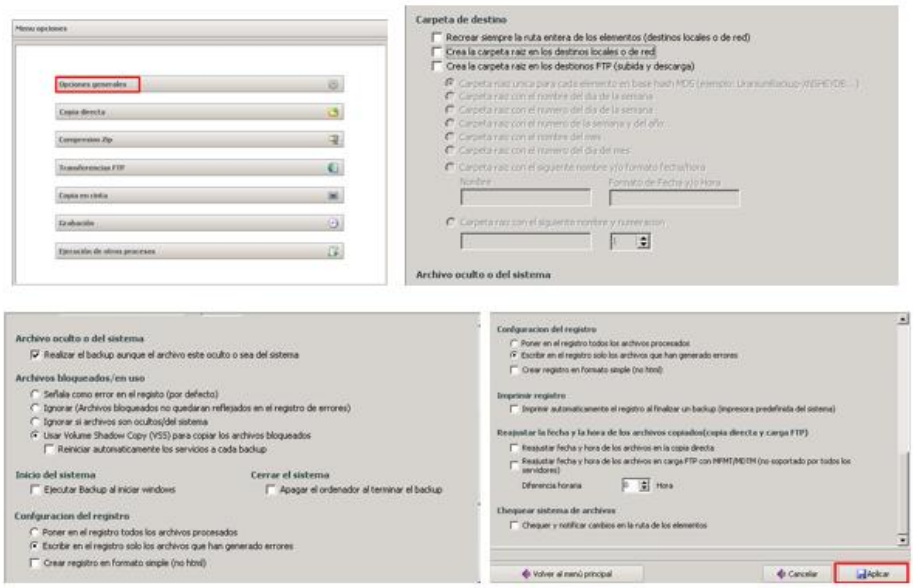


Figura 53 Configuración opciones generales

Fuente: (Autor)

- En el Menú de Copia Directa se configura las opciones de copia, sobre escritura de archivos, copia especial, copia de atributos de seguridad etc. En este caso se seleccionó la sobre escritura de archivos si el archivo

origen ha sido modificado después del último backup, la copia de atributos de seguridad y comparación de fechas y horas de los archivos como se observa en la figura 54.

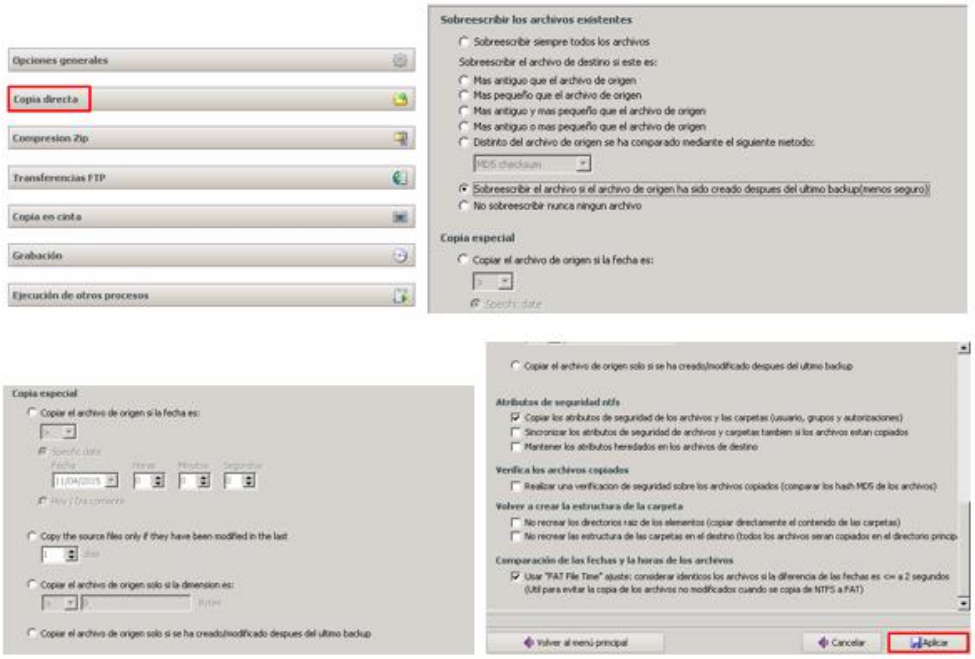


Figura 54 Configuración opciones de copia directa

Fuente: (Autor)

- Con Uranium Backup tenemos la opción de sincronizar el servidor origen con el destino, es decir que, si en el servidor origen eliminan un archivo, al momento de ejecutar la tarea elimina también del destino. Así garantizamos cuando se ponga en producción el servidor destino este similar al origen. Para poder habilitar esta tarea hacemos clic en los elementos de origen y seleccionamos la opción que se muestra en la figura 55.

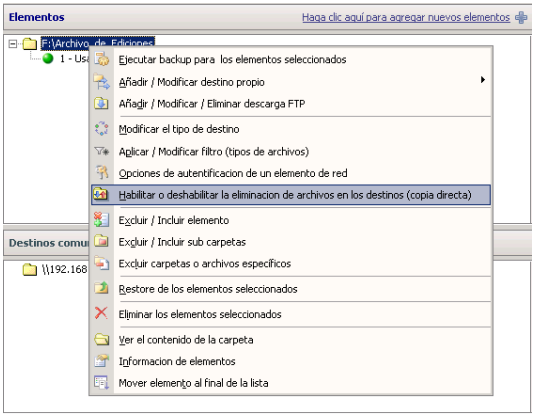


Figura 55 Habilitación de eliminación de archivos en los destinos

Fuente: (Autor)

- Ahora para poder calendarizar la tarea, nos dirigimos a la opción Horario, y calendarizamos la ejecución de la tarea según nuestras necesidades. En este caso calendarizaremos que corra la tarea todos los días a las 2:00 am, (ver figura 56).

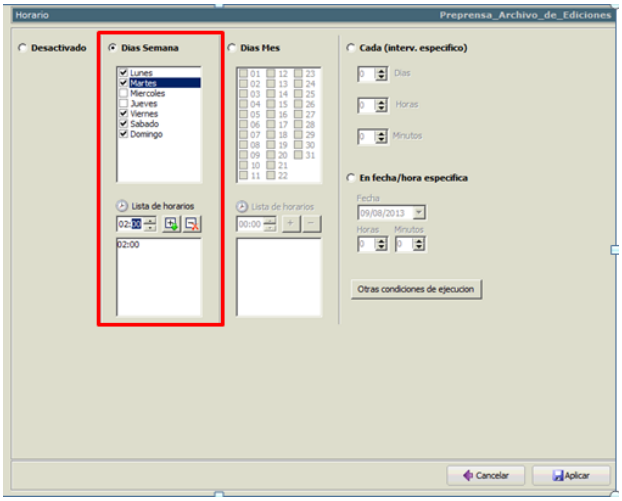


Figura 56 Configuración horario de la tarea

Fuente: (Autor)

- Con este software tenemos la ventaja de que al finalizar una tarea nos envíe un correo indicando la tarea fue satisfactoria o tuvo errores, con esto podemos revisar el inconveniente o a su vez estar seguros de que la

sincronización está correctamente. Para configurar debemos escoger la opción de Informe por mail y configurar según las necesidades, (ver figura 57).

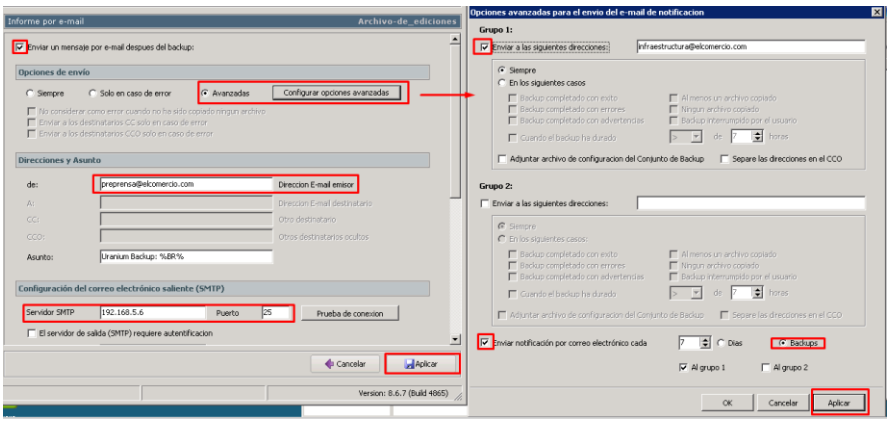


Figura 57 Configuración informe por mail

Fuente: (Autor)

Debido a que la primera vez que se ejecute la tarea tomará su tiempo por la cantidad de archivos a sincronizar se ejecuta manualmente, luego de esto podremos ejecutarlo automáticamente e ir configurando las tareas restantes para calendarizarlos ordenadamente y evitar el cruce de los mismo, provocando así errores en las tareas siguientes.

Finalmente basta por esperar que los dos servidores se encuentren sincronizados con la misma data para ponerlo en producción el nuevo servidor NAS.

3.6. Puesta en Producción del nuevo servidor.

Una vez que la data se ha sincronizado exitosamente, por políticas del área se debe comunicar a la Gerencia de Tecnología y solicitar una ventana de mantenimiento, con el fin de que todos en el área conozcan del evento que se realizará para actuar proactivamente en caso de tener algún inconveniente, (ver figura 58).

De: Centro de Soporte de Tecnologia
Para: Lista-Sistemas
CC:
Asunto: Cerrado: Mantenimiento Programado Servidor Preprensa

Centro de Soporte de Tecnología
GRUPO EL COMERCIO

Estimados Compañeros:

El Centro de Soporte de Tecnología pone en conocimiento el siguiente Mantenimiento Programado:

Servidor Preprensa

Fecha del Evento:	Miércoles 17 de Septiembre de 2014
Hora Inicio:	06:00
Hora y Fecha Fin:	06:55
Tiempo de solución:	55 minutos
Acciones:	Se migró el servidor de Preprensa (cambio de servidor por la NAS)
Servicio Afectado:	File_server de Preprensa
Área afectada:	Usuarios Internos.
Responsable:	Juan Carlos Villacis
Observaciones:	Posterior a la migración todos los servicios se encuentran funcionando correctamente.

Gracias por su comprensión.

Atentamente,

Gerencia de Desarrollo & Tecnología

MESA DE AYUDA
095 41 41 41
4 1 4 1
4141@elcomercio.com

Figura 58 Ventana de mantenimiento programado

Fuente: (Autor)

El cambio de servidor se lo realizó en horas sin flujo de usuarios, debido a que este cambio debe ser transparente para el usuario final. Los pasos que se siguieron son los siguientes.

- Se sacó del dominio elcomercio.news al servidor original.
- Se cambió el nombre del servidor original por *Preprensa_old*
- Se configuró la red habilitando *DHCP* para que nos asigne una nueva IP y liberar la original.
- Se colocó el nombre de *Preprensa* al nuevo servidor.
- Se cambió la IP en el nuevo servidor, colocando una *IP estática* la cual era la que tenía el servidor original.
- Finalmente se ingresó el nuevo servidor al dominio *elcomercio.news*.

Como medida de prevención y mejor uso del ancho de banda se configuró un teaming de red, lo que permite que múltiples conexiones a una red trabajen como un enlace lógico., esto incrementa el ancho de banda global de la conexión al balancear la carga de todo el tráfico de forma igualatoria a través de cada enlace, (ver figura 59).

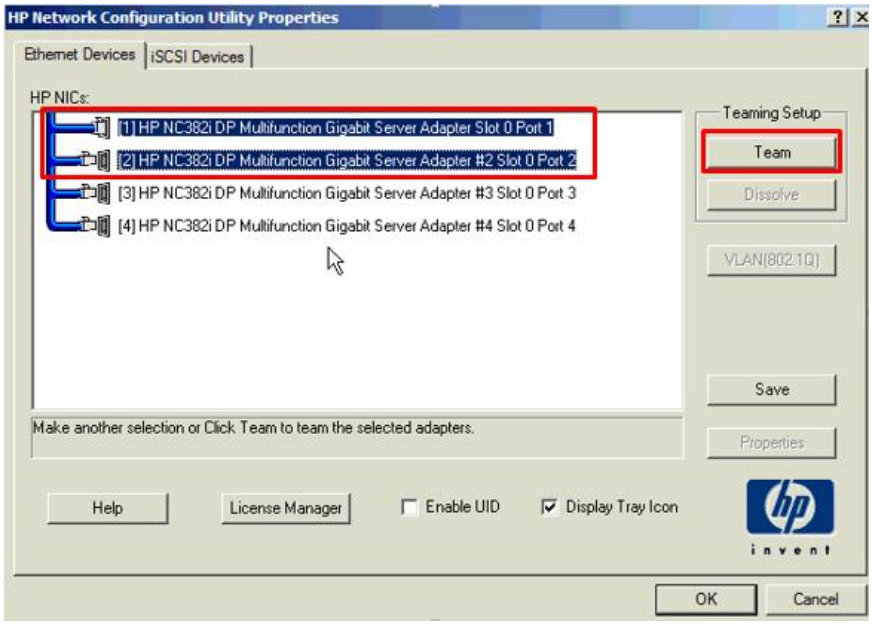


Figura 59 Configuración Teaming de red

Fuente: (Autor)

Luego de realizar estos pasos se probó el acceso al servidor desde varios usuarios y no existió ningún inconveniente.

No solo se logró tener la información en un servidor de nueva generación y con mayor espacio, este servidor se puede conectar a la SAN (Storage Network Área) con lo que se configurará la conexión a las librerías de respaldo y así tener backups de la información en cintas, este tema se lo ampliará más adelante. Adicional al tener conexión a la SAN se puede presentar mayor espacio de otros sistemas de almacenamiento en caso de necesitarlo o a su vez podemos presentar espacio de este servidor a otros más pequeños.

3.6.1. Configuración del servidor en la SAN.

Una SAN es una red de almacenamiento de gran velocidad y estabilidad en la que agrupa varios elementos tales como canales de fibra (SCSI), equipo de interconexión dedicados (Conmutadores, puentes, etc.) y elementos de almacenamiento de red (discos duros, librerías).

Una vez puesto en producción el nuevo servidor y verificado que los usuarios no presenten ningún inconveniente, se realiza la conexión del servidor a la SAN, para esto, antes de comenzar con la configuración en los switchs de fibra, debemos tener claro cómo se encuentra la arquitectura actualmente. En la figura 60 se puede observar la SAN actualmente en la compañía

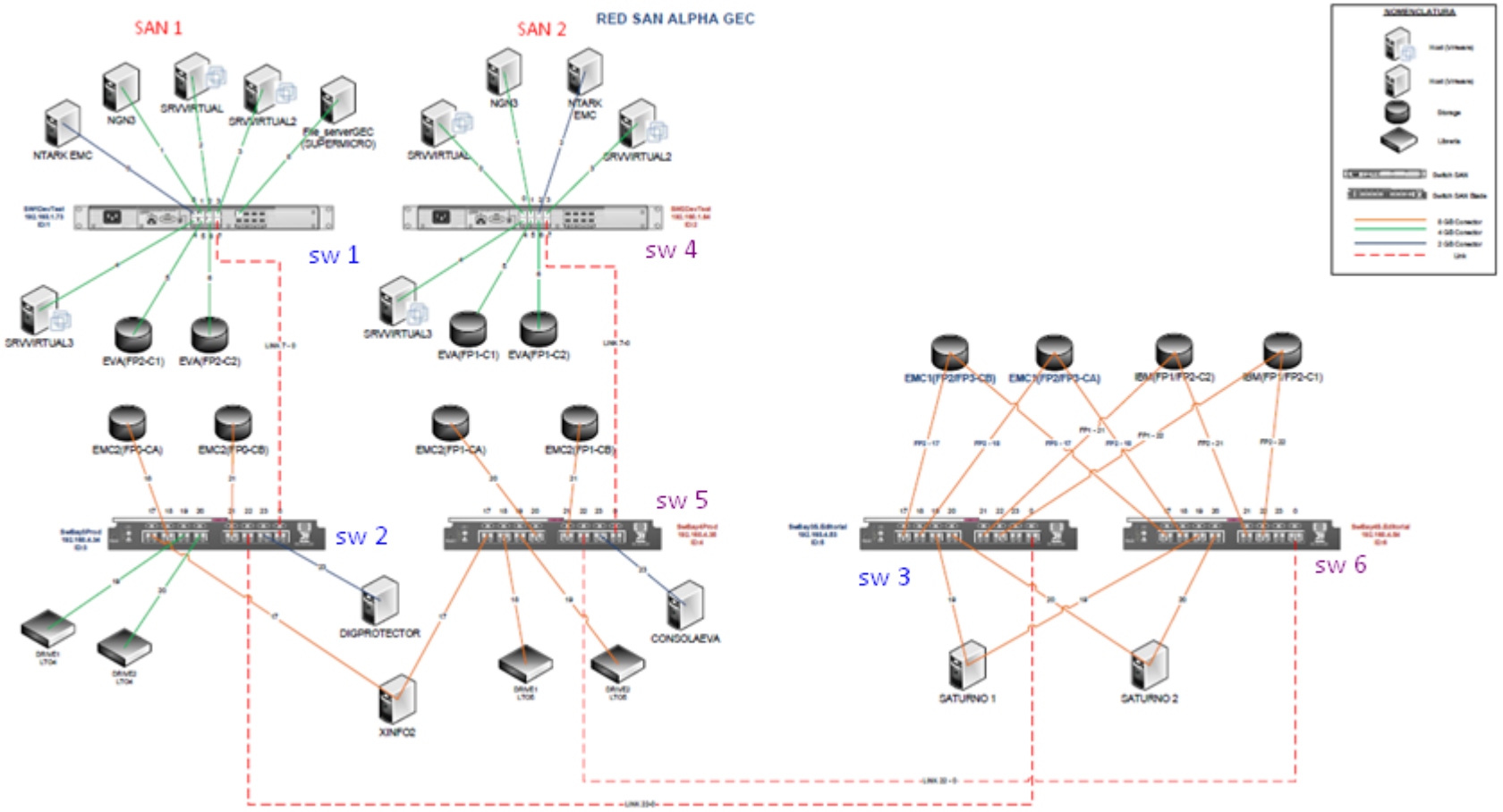


Figura 60 Red SAN GEC

Fuente: (Autor)

Como se pudo observar en la figura anterior se tiene disponible 2 puertos uno en el SW 3 y otro en el SW 6. En esta ocasión se decidió conectar el servidor Preprensa en el Switch 6 puerto 23, realizado esto ingresaremos al switch para configurar las zonas, es decir, indicar que dispositivo podrá ver el servidor preprensa.

Configuración switch SAN

El switch que se configurará es un switch blade de fibra Brocade, la configuración se lo puede realizar completamente por SSH, pero se optó por la configuración basada en entorno gráfico.

1. Accedemos a la Web de gestión (http://192.168.x.x) con User/Password establecidos por el administrador. La pantalla inicial muestra el estado de las comunicaciones de Switch de manera gráfica. Aquí podemos ver que puertos se encuentran libres y cuales en uso, (ver figura 61).

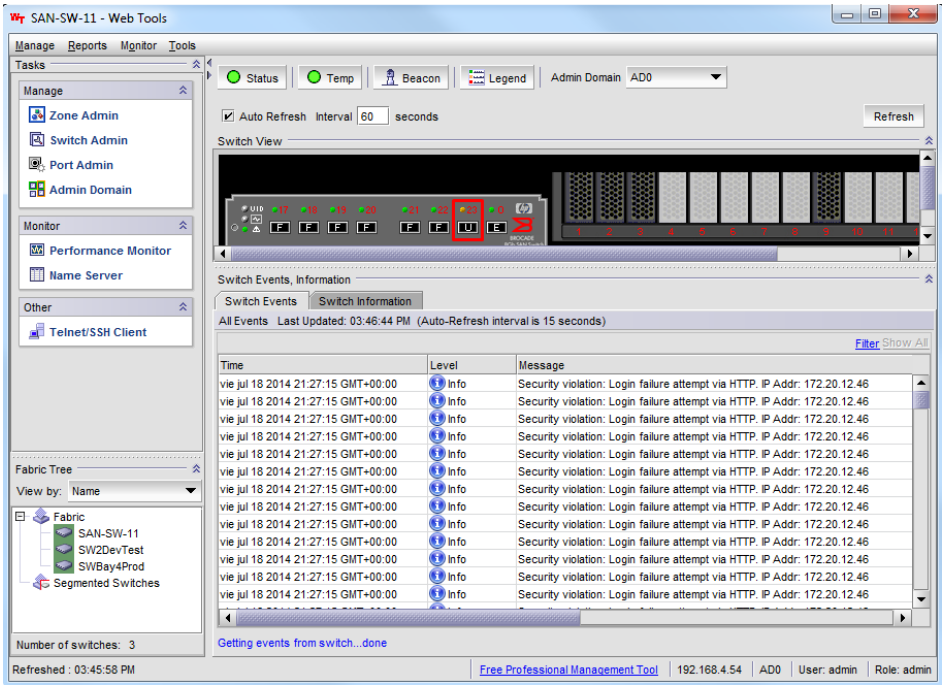


Figura 61 Administración web switch de Fibra

Fuente: (Autor)

2. Lo primero es configurar el puerto del switch que será usado para conectar el servidor Preprensa, dirigiéndonos a la opción de Port Admin. Hay que tomar en cuenta que debemos tener licencias disponibles para poder usar el puerto, caso contrario el puerto no trabajaría, (ver figura 62).

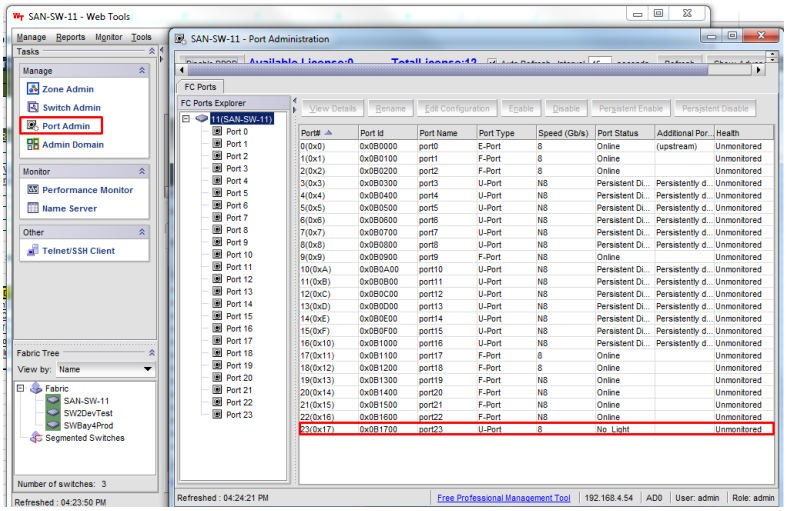


Figura 62 Administración de puertos switch de fibra

Fuente: (Autor)

3. En este caso Seleccionamos el port23, marcamos la opción *Show Advanced Mode* y clicamos sobre *Reserve License* parar agregar la licencia al puerto, (ver figura 63).

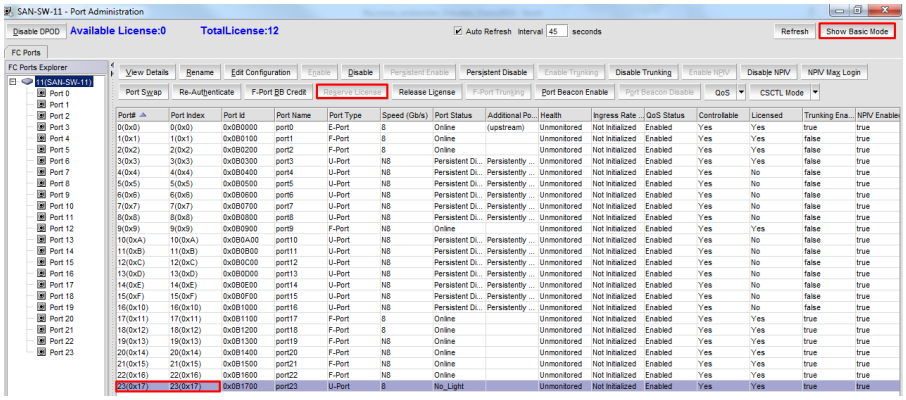


Figura 63 Asignando licencia a un puerto switch de fibra

Fuente: (Autor)

4. Una vez activada la licencia en el puerto, cerramos la ventana y al cabo de unos minutos podemos observar que se ha actualizado el indicador del chasis. El puerto está en verde lo que significa que está activo (ver figura 64).

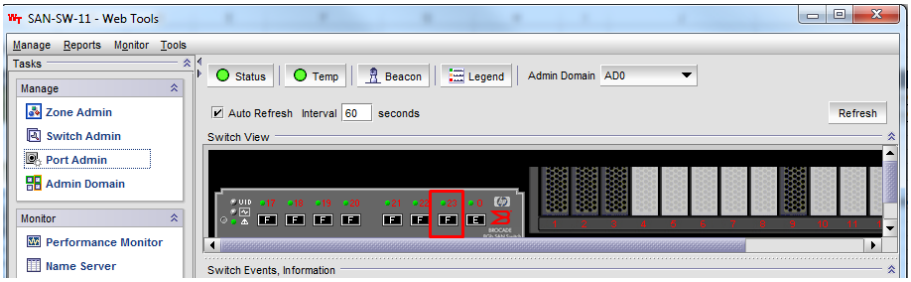


Figura 64 Puerto de fibra activado

Fuente: (Autor)

5. Una vez terminada la configuración del puerto, lo siguiente es configurar la zona, es decir, el camino de comunicación entre un dispositivo y otro. En este caso se realizará una zonificación entre el servidor y la librería de respaldos.

Para configurar la Zona debemos realizar 3 pasos.

- Ingresamos a Zone Admin y lo primero que configuramos es un Alias, el cual es un nombre amigable que se da a los WWN (World Wide Name, identificador único en la red SAN FC) esto para tener identificado el puerto con un nombre específico y tener una mejor administración, en este caso le llamaremos al puerto 23 como Alias_Preprensa, adicional se encuentra configurado los puertos 18 y 19 del SW5 con los siguientes nombres “Alias_MSL_LTO5_Drive1” y ”Alias_MSL_LTO5_Drive2” respectivamente, los cuales están conectados o hacen referencia a la librería de respaldos, (ver figura 65).

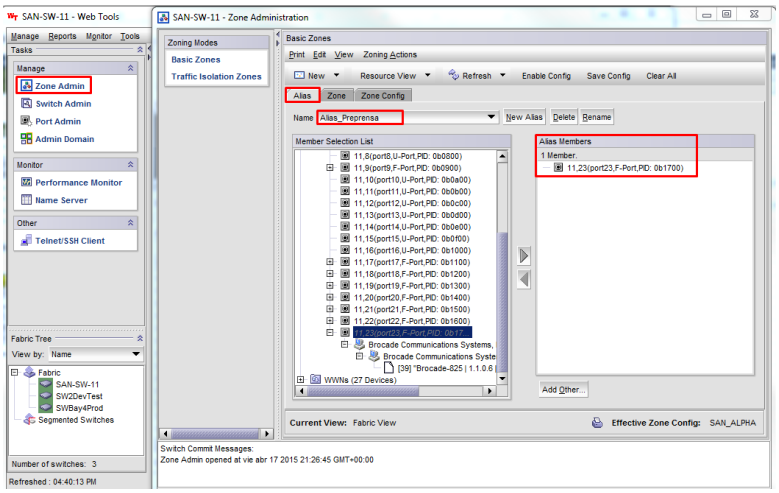


Figura 65 Creando un alias al puerto de fibra

Fuente: (Autor)

- Seguido creamos la Zona, es decir, las conexiones que se permitirá entre los alias, indicamos un nombre de zona, en este caso se lo llama "Zona_Preprensa_Backup", y permite el tráfico entre la HBA del servidor Preprensa y la librería LTO5, (ver figura 66).

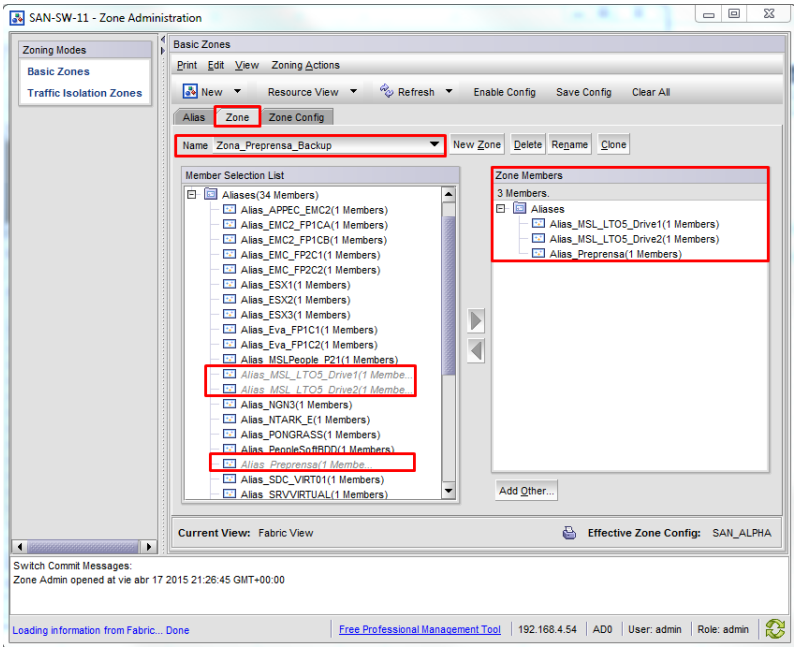


Figura 66 Creación zona de comunicación entre dispositivos

Fuente: (Autor)

- Finalmente, una vez creada la zona, habilitamos la misma en la configuración global. Para ello vamos a la pestaña *Zone Config*, seleccionamos la zona creada anteriormente y agregamos a la configuración, con esto estaría configurado el camino de fibra entre el servidor Preprensa y la librería, (ver figura 67). Guardamos la configuración y habilitamos para que se refleje en toda la red SAN.

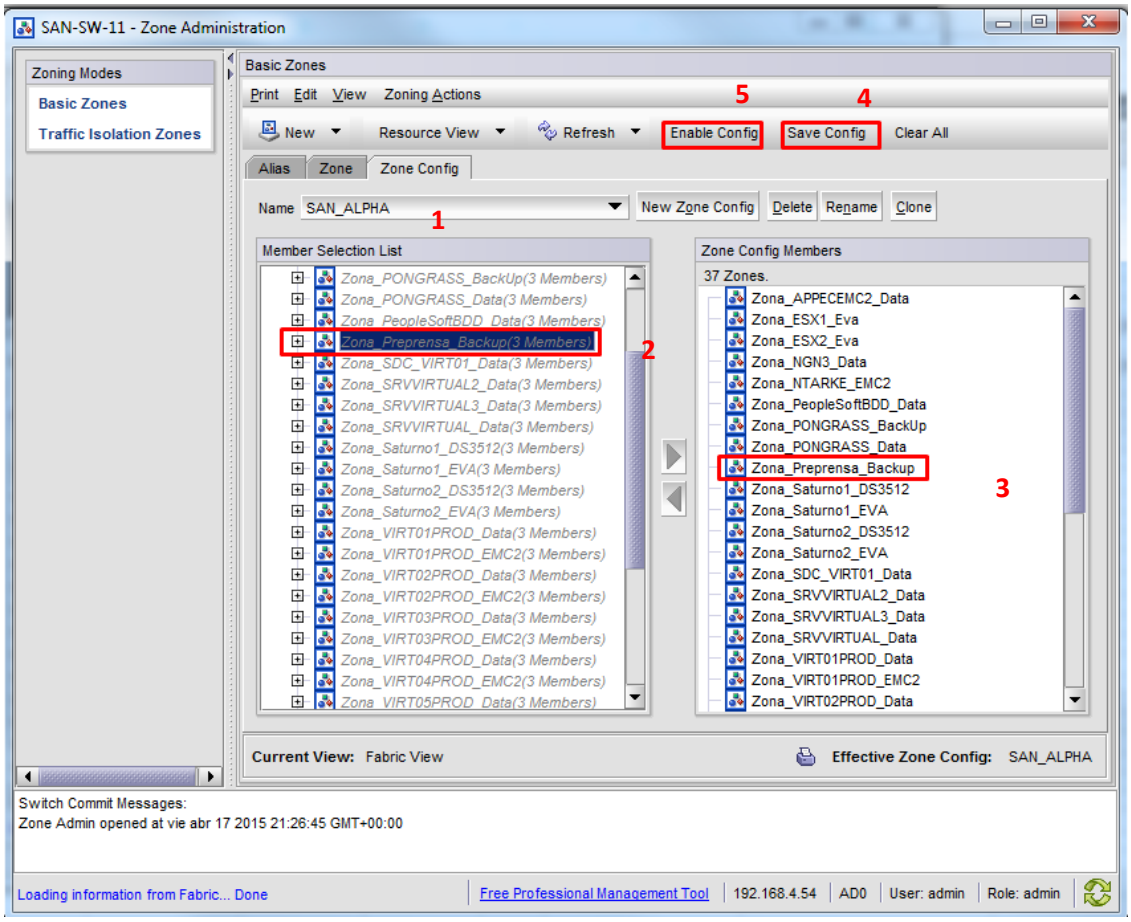


Figura 67 Habilitando la zona en la SAN

Fuente: (Autor)

A diferencia de la situación actual del servidor, en la que solo tenía conexión en la red LAN ahora el servidor se encuentra en la red SAN y LAN. En la figura 68 se puede observar el diagrama red en relación al servidor Preprensa.

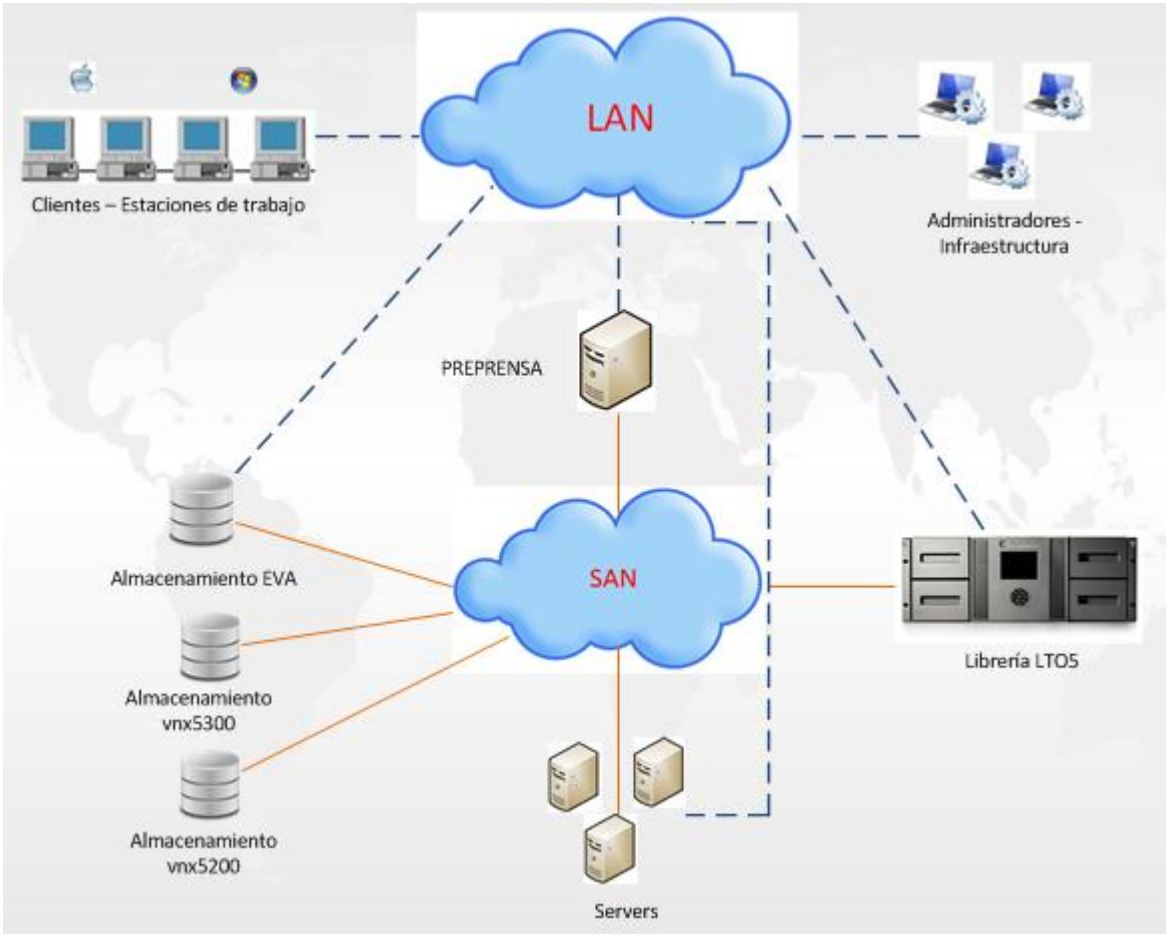


Figura 68 Conexión del servidor Preprensa en la red LAN y SAN

Fuente: (Autor)

CAPITULO IV

ANÁLISIS Y ELABORACIÓN DEL PLAN DE CONTINGENCIA DE LOS SERVICIOS TI SEGÚN LAS NORMAS ISO 27001 E ITIL V3 REFERENTE A LA GESTION DE LA CONTINUIDAD DEL NEGOCIO

4.1. Introducción.

La norma ISO/IEC 27001 que corresponde al Sistema de gestión de Seguridad de la Información, detalla que la información es un activo valioso que puede impulsar o destruir una empresa. Si se gestiona de forma adecuada, le permite trabajar con confianza. La gestión de Seguridad de la Información le ofrece la libertad para crecer, innovar y ampliar su base de clientes sabiendo que toda la información confidencial seguirá siéndolo. La norma específica requisitos para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para prepararse, responder y recuperarse de eventos que generan interrupciones, cuando éstos ocurren. (BSIGROUP, 2014)

Dentro de la administración y la gestión de la seguridad de la información en una compañía es importante tener un plan alterno que asegure la continuidad del negocio, ya que, dependiendo de la forma que se gestione dicho incidente, las consecuencias pueden ser más o menos graves. Un plan de contingencia de servicios TI implica un análisis de los posibles riesgos a los cuales se encuentra expuestos los servidores y sistemas de información.

El plan de contingencia mantiene estrecha relación con la infraestructura informática y con los procedimientos relevantes a este, en donde, la infraestructura informática está conformada por el hardware, software, soporte y transmisión de datos que permiten la funcionalidad del negocio; en tanto que los procedimientos relevantes son todas aquellas tareas que realiza el personal

encargado de la Infraestructura al interactuar con las distintas plataformas generando reportes, consultas, monitoreo, etc.

Al ser la información uno de los bienes más importantes de la empresa al igual que la continuidad de los servicios brindado a los usuarios son los fundamentos primordiales a tomar en cuenta al elaborar un plan de contingencia, además es necesario que el mismo contenga un plan de recuperación con el objetivo de restaurar el servicio informático en forma rápida, eficiente y con la menor inversión monetaria posible.

Con el fin de garantizar la integridad de la información y los servicios se investigará e implementará aplicaciones que permitan recuperarlos en caso de algún evento fortuito, además de impulsar las mejores prácticas para proteger el centro de información.

4.2. Organización del Departamento TI

El departamento a cargo de los servicios TI en la compañía se denomina Desarrollo Digital y Tecnología, cuyos objetivos son, poner en marcha y operación soluciones tecnológicas que apoyen la meta de convertir a la compañía en la mejor empresa de medios de comunicación del país cumpliendo los estándares de calidad y excelencia de la industria. La Gerencia de Desarrollo Digital y Tecnología se encuentra organizada en 3 áreas.

- **Producción y Operación:**
  Responsable de planificar, implementar y mantener la infraestructura tecnológica de la empresa: Hardware, Software y comunicaciones, de tal forma que pueda estar disponible para los usuarios en el momento que sea requerida, aplicando siempre estándares de eficiencia y calidad. El objetivo del área es mantener un uptime de los servicios en un 99,98 %.

- **Desarrollo**

  Cuyos principales objetivos son construir e implementar las nuevas aplicaciones financieras, administrativas, comerciales y digitales-multimedia de acuerdo al plan estratégico de la Empresa. Además, gestionar, negociar y supervisar el trabajo realizado por los proveedores en los proyectos de implementación de nuevas soluciones contratadas

- **Seguridad y Mesa de Ayuda**

  El propósito de la Mesa de Ayuda o Centro de Soporte, es servir como primer punto de contacto entre los usuarios y TI, registrando y dando solución y seguimiento a los requerimientos de los usuarios.

  El área de Seguridad Informática, vela por alcanzar un grado de madurez efectivo en cuestión de Seguridad TI con el fin de minimizar los Riesgos a los cuales estamos expuestos en el mundo de la tecnología de la información.

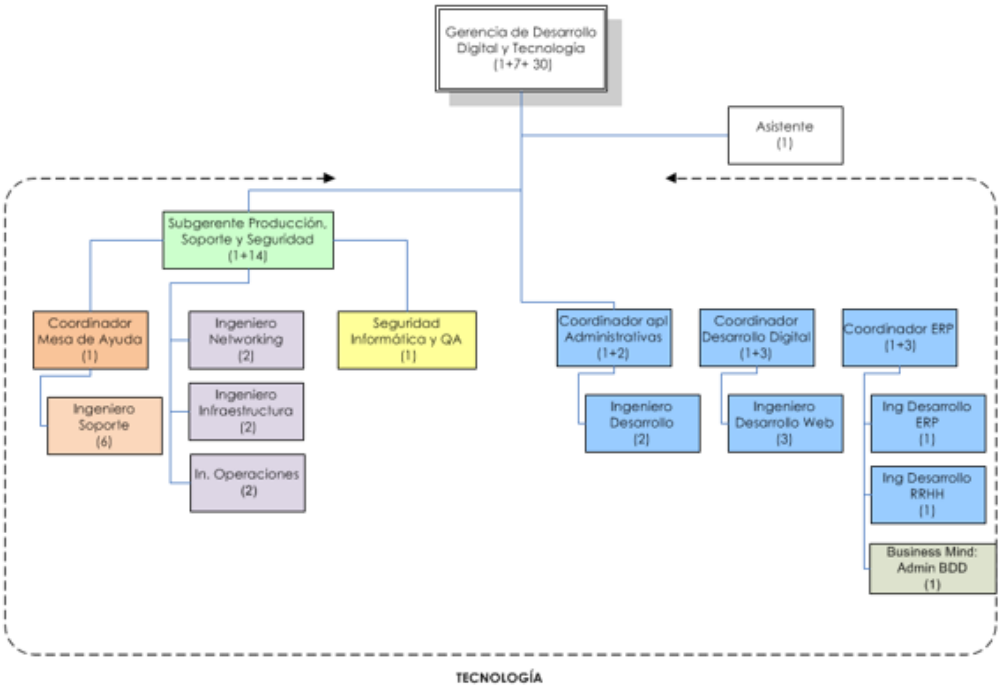


Figura 69 Organigrama Departamento TI de Grupo El Comercio

Fuente: (Autor)

4.2.1. Análisis FODA del Departamento TI

Tomando en cuenta el alcance del presente proyecto de titulación se enfoca el análisis FODA únicamente al Departamento de TI de Grupo El Comercio C.A.

El análisis FODA del Departamento TI ha sido elaborado con la ayuda de los miembros del departamento de Desarrollo Digital y Tecnología el cual se lo describe a continuación.

Fortalezas

- Se cuenta con personal calificado para administrar los servidores físicos y virtuales, así como también los elementos de red y las aplicaciones requeridas por el negocio.
- Se está implementando estándares para los procedimientos que se realizan dentro del área de Desarrollo Digital y Tecnología.
- Cada miembro que labora en el Departamento de Tecnología tiene la facilidad y acceso a capacitación constante sea este presencial o vía online.
- Se tiene la posibilidad de escalar los inconvenientes hacia los proveedores sea nacional o internacional
- Se tiene gran apertura para buscar e implementar nuevas soluciones que permita la mejora del negocio.
- El tener un departamento organizado en varias áreas facilita la atención o soporte hacia los usuarios, lo que permite tener una buena aceptación y percepción por parte de ellos.

Oportunidades

- El Departamento de Desarrollo Digital y Tecnología es partícipe de todos los proyectos que se implementan en la compañía.

- Tener relación con empresas proveedoras líderes nacionales e internacionales que se pueda analizar y tener acceso a tecnología de punta en cuanto a hardware y software.
- Tener acceso a capacitación de nuevas tecnologías con el fin de dar mejores soluciones al Departamento de TI.

Debilidades

- El tener una parte de nuestros servidores en Miami, es un riesgo para el departamento debido a que al ocurrir un daño no se tiene control local sobres estos sistemas para poder gestionar la reparación de forma inmediata.
- Al tener un momento complicado en cuanto a lo financiero hace que los presupuestos se reduzcan, complicando así la adquisición de soluciones y hardware de última generación.
- Falta de conocimiento total del negocio por parte del personal de TI.
- Falta implementar software de monitoreo de hardware y herramientas de respaldo de las aplicaciones.
- Falta comunicación de parte de los demás departamentos cuando se piensa implementar un nuevo proyecto.

Amenazas

- Inestabilidad política del país puede afectar a la organización en general.
- Problemas en tener daños en los equipos sean estos por fallas humanas o tiempo de vida útil de los mismos.
- Problemas al no poder obtener partes de un equipo obsoleto para reemplazar componentes con daño debido a que se encuentran fuera de soporte.
- Plagio de soluciones informáticas, herramientas tecnológicas o métodos para llegar al cliente; por parte de la competencia.
- Problemas en los convenios existentes con los proveedores

- Problemas con hackers que realicen cambios o denegación de servicio en los sitios web de la compañía.

4.3. Identificación y Priorización de Riesgos

4.3.1. Análisis de Riesgo

El Objetivo de un análisis de riesgos es identificar en la compañía los activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado. El análisis de riesgo se centra en los procesos o actividades del negocio que se consideran críticas, aunque también puede extenderse a aquellos que no lo son.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física de los equipos en los cuales se almacena.

La fundación ITIL menciona en su norma itilv3 que al no conocer cuáles son los riesgos reales a los que enfrenta la infraestructura TI es imposible realizar una política de prevención y recuperación ante desastre mínimamente eficaz. La Gestión de la continuidad del servicio debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes riesgos o factores de riesgos.

Gracias a los resultados detallados de este análisis se dispondrá de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio. (Osiatis S.A, 2015)

4.3.2. Probabilidad del Riesgo

La probabilidad es el número de veces que se da un evento, es decir, es el número de veces que una amenaza deja de serlo para convertirse en realidad, a lo largo de un determinado periodo de tiempo.

La probabilidad puede especificarse en términos lógicos, cualitativos o cuantitativos. En definitiva, se trata de establecer un rango con los posibles valores a asignar a cada una de aquellas preguntas de la lista de comprobación de elementos de riesgo. En el caso más extremo, se podría responder a dichas cuestiones con un “si” o un “no”, aunque esta constituiría una solución poco realista. (Sánchez Garreta, Ingeniería de proyectos informáticos: Actividades y procedimientos, 2003)

Para el desarrollo de este proyecto se especificará la probabilidad de riesgo cualitativamente, valorando esta como baja, mediana y alta respondiendo a las siguientes condiciones.

- Baja: Cuando exista condiciones que hacen muy lejana la posibilidad del riesgo
- Mediana: Cuando existen condiciones que hacen poco probable un riesgo ataque en corto plazo, pero no son suficientes para evitarlo en el largo plazo.
- Alta: Cuando el riesgo es inminente.

4.3.3. Impacto del Riesgo

El análisis de impacto es primordial para establecer una estrategia de recuperación, lo cual en principio permitirá la continuidad de las actividades críticas y posteriormente al resto. Esta actividad permite identificar los procesos críticos que permiten el trabajo diario del negocio, las interdependencias entre

procesos y recursos requeridos para operar los procesos en un nivel mínimamente aceptable.

Dentro del análisis de impacto se distinguen las siguientes actividades:

- Obtención de la relación de procesos
- Obtención de la relación de aplicaciones
- Relación de departamentos y usuarios.
- Determinar cuáles son los procesos críticos
- Período máximo de Interrupción.

4.3.4. Exposición del Riesgo

La exposición del riesgo es la frecuencia con que se presenta la situación de riesgo. Siendo tal que el primer acontecimiento indeseado iniciaría la secuencia del accidente. Habitualmente vendrá dado por el tiempo de permanencia en áreas de trabajo, tiempo de operaciones o tareas, de contacto con herramientas, etc. El nivel de exposición se presenta según la tabla 10

Tabla 10
Nivel de la exposición de riesgo

EXPOSICIÓN	INDICE
Continuamente: muchas veces al día	10
Frecuentemente: Aprox. Una vez al día	6
Ocasionalmente: De una vez a la semana a una vez al mes	3
Irregularmente: De una vez al mes a una vez al año.	2
Raramente, cada bastante años	1
Remotamente, no se sabe que haya ocurrido, pero no se descarta	0,5

Fuente: (Autor)

4.3.5. Eventos Controlables y no Controlables

Los riesgos deben estar categorizados en función a las acciones preventivas que pueden estar en manos de la empresa o cuya ocurrencia no puede ser predicha con anterioridad, es así que los eventos pueden ser:

Eventos Controlables: Estos eventos al momento de identificarlos se pueden plantear acciones que eviten la ejecución o reduzca el impacto. Estos pueden ser los que se muestra en la figura 70

Eventos Controlables
Incendio
Elevación de temperatura en el DataCenter
Pérdida de información
Fallo o degradación del hardware de los servidores físicos
Daño de los servidores virtuales
Errores de operación
Caída de sistemas y aplicaciones de la compañía
Fallo en los motores de base de datos
Fallo en la red de datos
Caída de enlaces en las regionales
Ausencia imprevista del personal de soporte técnico
Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático
Acceso no autorizado al DataCenter
Acceso no autorizado a información de los distintos departamentos

Figura 70 Eventos controlables

Fuente: (Autor)

Eventos No Controlables: Cuando la ocurrencia es impredecible y únicamente se pueden plantear acciones que permitan minimizar su impacto, en la figura 71 se observa algunos eventos no controlables.

Eventos No Controlables
Inundaciones por lluvia
Actos de vandalismo
Ataques de denegación de servicios
Sismos
Interrupción del servicio eléctrico
Avería en el servicio telefónico
Avería en la red de datos de los proveedores
Sabotaje

Figura 71 Eventos no controlables

Fuente: (Autor)

4.3.6. Definición de la Matriz de Riesgo

La matriz de riesgo es una herramienta de control y gestión que permite visualizar los riesgos desde la etapa de planificación de un proyecto, facilitando el manejo de riesgos a tiempo y minimizando el impacto negativo en la compañía. Esta matriz contiene los peligros y riesgos propios de cada una de las aplicaciones desarrolladas en la empresa.

El objetivo de la matriz de riesgos es identificar y cuantificar los riesgos para lograr una gestión que permita disminuir la probabilidad y el impacto de los eventos adversos en los servicios TI. En la figura 72 se observa la matriz de riesgo con lo cual se puede establecer prioridades durante la ejecución de las medidas de prevención y mitigación.

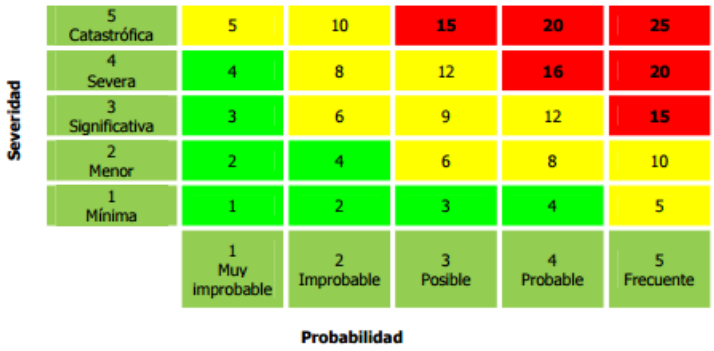


Figura 72 Matriz de riesgo

Fuente: (Ministerio de Energía y Minas Perú, 2015)

En función de las variables severidad o consecuencia y probabilidad se puede obtener el correspondiente Nivel de Riesgo, el cual es el índice de peligrosidad de la actividad evaluada y nos proporciona la información necesaria para adoptar acciones y medidas de control. El nivel de riesgo se calcula multiplicando los valores de consecuencia por los valores de probabilidad.

$$\mathbf{RIESGO = CONSECUENCIA\ X\ PROBABILIDAD}$$

Según el valor que se obtenga en la ecuación anterior, los riesgos se clasifican en Alto, Medio o Bajo; cuanto más alto es el valor más alto es el riesgo. En la figura 73 se explica los criterios de aceptabilidad.

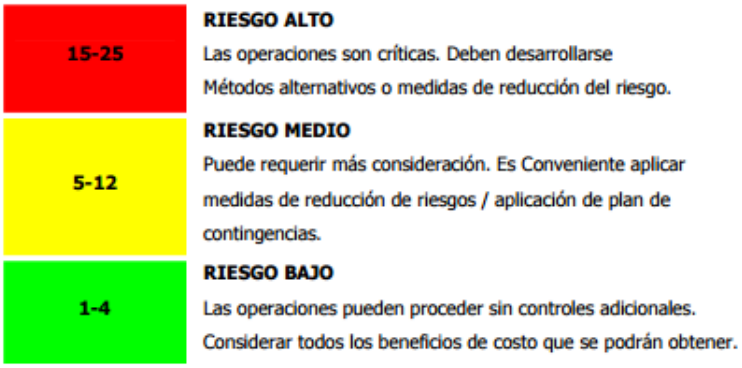


Figura 73 Criterios de aceptabilidad de riesgos

Fuente: (Ministerio de Energía y Minas Perú, 2015)

4.4. Definición de eventos susceptibles de contingencia

El plan de contingencia abarca todos los aspectos relacionados y que forman parte del servicio TI, es por esto que, es importante considerar todos los elementos susceptibles capaces de provocar eventos que activen el plan de contingencia. Los principales elementos que serán considerados para su evaluación son.

- Hardware
    - Servidores físicos
    - Servidores virtuales
    - Almacenamientos o Storages
- Comunicaciones
    - Equipos de comunicaciones switchs SAN y LAN
    - Cableado de red de datos LAN y fibra
    - Enlaces hacia las regionales
- Software
    - Software de Base de datos (Oracle, SQL, PostgresSQL, mysql)
    - Software de aplicaciones
    - Aplicativos utilizados por la compañía
    - Software Base (Sistemas Operativos)
    - Antivirus para protección de servidores.
- Aplicaciones
    - Sistema Editorial
    - Sistema ERP
    - Sitios Web
    - Sistema de RRHH
    - Sistemas para tratar imágenes y pdfs.
    - Sistema Workflow (generación de placas)
    - File_servers

4.5. Etapas de la gestión de continuidad del servicio.

En este punto del proyecto se realizará la elaboración del plan de contingencia de los servicios TI de Grupo El Comercio C.A.

Para el desarrollo del plan se utilizarán las mejores prácticas de ITIL, con el objetivo de asegurar la continuidad de los distintos sistemas de TI ante cualquier eventualidad, basado en el establecimiento de medidas preventivas.

Las etapas que propone ITIL para la gestión de continuidad son las que se observa en la figura 74, adaptadas a las necesidades de la empresa con el fin de que sea aplicable a la realidad del departamento de Tecnología y que sea práctico su implementación.

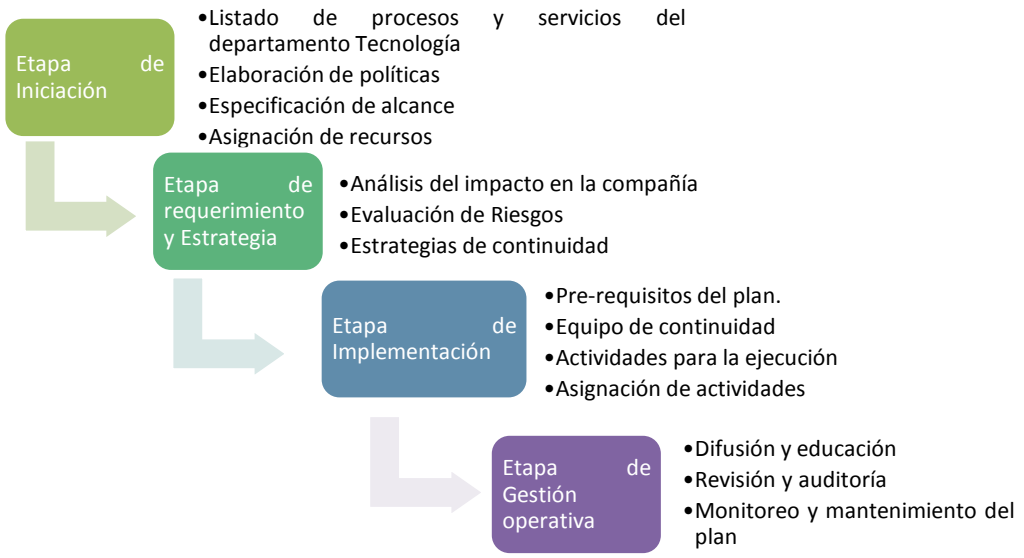


Figura 74 Etapas de la gestión de continuidad del servicio

Fuente: (Autor)

4.5.1. Etapa de Iniciación

Para elaborar el plan de contingencia de los servicios TI se comenzará con la realización de la etapa inicial la cual tiene cuatro aspectos importantes:

- **Los servicios TI:** Se detalla la infraestructura y servicios que tiene a cargo el departamento de tecnología.
- **Las políticas:** Se definen un conjunto de directrices documentadas que establecen normas y procedimientos apropiados para ejecutar las diferentes tareas del plan de una manera ordenada y clara.
- **El alcance:** Se define los temas a tomar en cuenta en el plan de continuidad.
- **Los recursos:** Se define o asignan los recursos tecnológicos, financieros y humanos para lograr un diseño óptimo del plan de contingencia.

4.5.1.1. Infraestructura y servicios TI

La compañía de Grupo el Comercio C.A cuenta con cuatro sitios importantes donde se encuentran los distintos servidores que mantienen la operatividad de la empresa, Quito (Planta y Ed. Aragonés), Guayaquil y Miami. Un total de 214 servidores soportan los ambientes de Producción, Pruebas y Desarrollo, entre servidores físicos y virtuales, los cuales se encuentran distribuidos como se observan en la figura 75.

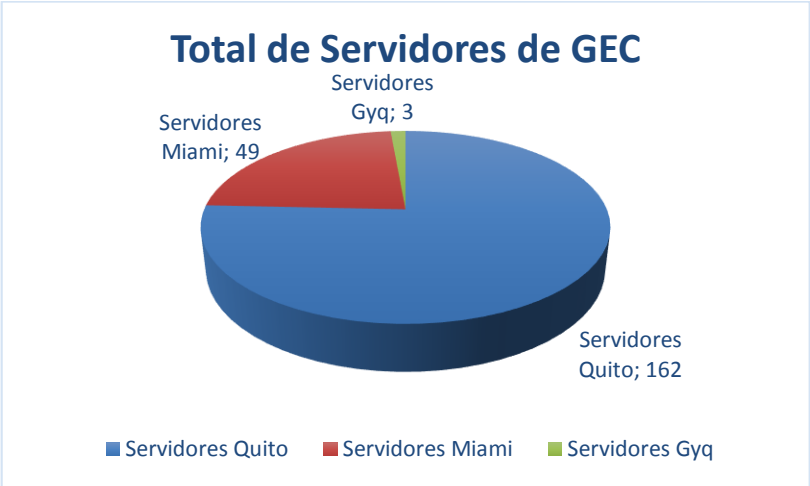


Figura 75 Total de servidores de Grupo El Comercio

Fuente: (Autor)

En las figuras 76 y 77 se describe el número de servidores que se encuentra implementado según el tipo, ya sea estos virtuales o físicos; así como también la distribución de los servidores según su ambiente de operación (producción, test, desarrollo o backup).

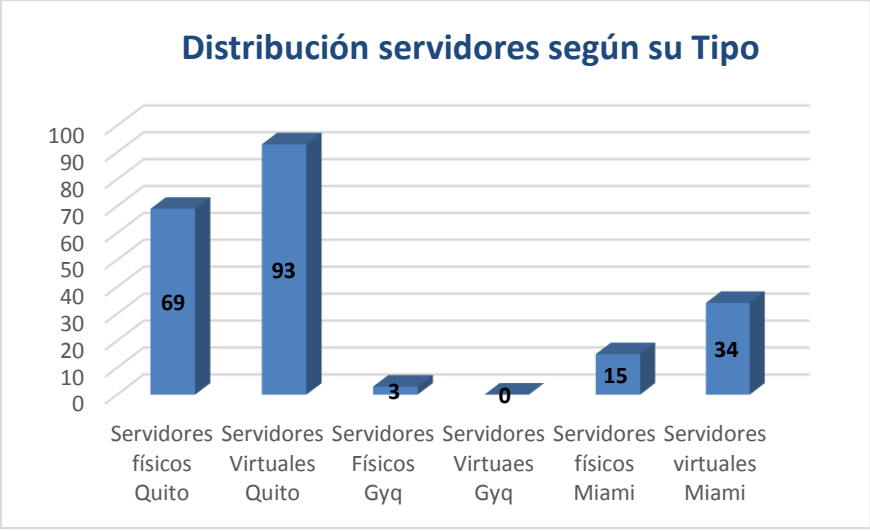


Figura 76 Distribución servidores de GEC según su tipo

Fuente: (Autor)

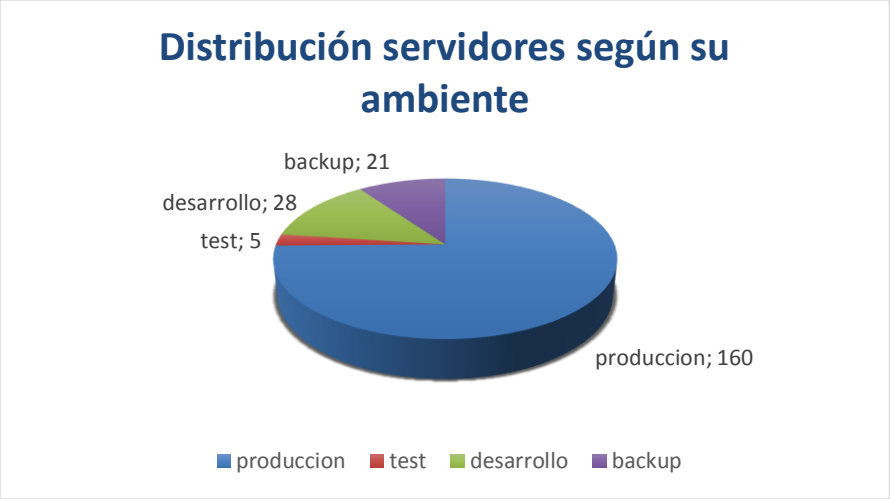


Figura 77 Distribución servidores de GEC según su ambiente

Fuente: (Autor)

Como se puede observar aproximadamente el 75 % de servidores corresponden al ambiente de producción, los cuales brindan los distintos servicios tanto para usuarios internos como para los clientes, es así que es primordial tener un plan de contingencia que permita no tener una caída de los servicios por un tiempo prolongado.

El área de Infraestructura & Operaciones en conjunto con Networking son las encargadas de la producción y operación de los servicios TI, estas áreas se encargan de la parte tecnológica y de brindar soporte de segundo nivel a los usuarios, ´proporcionar la infraestructura informática y de brindar apoyo en las distintas aplicaciones internas y comerciales de GEC.

Al ser una empresa global, muchos de los servicios se necesitan 24 horas al día, 7 días a la semana y 365 días al año, por lo que es indispensable contar con un equipo especializado de profesionales para mantener la operatividad al 100 %. A continuación, con la ayuda del personal de las áreas antes mencionadas se detalla los servicios TI que se tomará en cuenta para la elaboración del plan de contingencia, (ver tabla 11).

Tabla 11
Servicios TI de GEC.

Servicio General	Servicios Específicos	Descripción
Infraestructura	Servidores Producción	Ambiente de producción
	Servidores Test	Ambiente de pruebas
	Servidores Desarrollo	Ambientes de desarrollo
Sistema Editorial	Xalok info	Repositorio archivos históricos de las ediciones publicadas por GEC
	Robots Publicidad	Procesa los archivos de publicidad y multimedia
	Robots Visualización	Genera las previas del temario
	Robot Imágenes	Procesa las imágenes
	Robots Filmación	Genera los pdfs de las páginas trabajadas
	XalokRed	Sistema Editorial
	Xalok Docs	Editor de textos
	Xalok Previsiones	Planificación editorial
	Xalok_Indicadores	Estadísticas del trabajo realizado
Sistemas ERP	PeopleSoft	Sistema Financiero que lleva la contabilidad de la empresa
Facturación y Ventas	AplicacionesEC	Módulo de venta de optativos y publicidad; sistema de facturación, se integra con PeopleSoft
	Pongrass	Sistema de venta de anuncios publicitarios, se integra con AplicacionesEC
	Buxis	Módulo de gestión del área de Recursos Humanos
	RBM	Sistema de venta de anuncios publicitarios vía web, se integra con Pongrass
	Facturación Electrónica	Sistema de facturación electrónica, se integra con PeopleSoft
	Cubos	Sistema estadístico

CONTINÚA ⇨

Procesamiento de Imágenes	Voyager, WorkSpace y Asura	Procesamiento de pdfs de las páginas de las ediciones, procesamiento de artes, clasificados, avisos, publicidad e imágenes en general
Workflow	Trueflow	Sistema para procesar e imprimir placas de las distintas ediciones y archivos comerciales
Sitios Web	www.elcomercio.com	Sitio del Comercio
	www.benditofutbol.com	Sitio de Bendito Futbol
	www.revsitalideres.ec	Sitio de Revista Líderes
	www.revistafamilia.ec	Sitio de Familia
	www.ultimasnoticias.ec	Sitio de Ultimas Noticias
	futbolmania.elcomercio.com	Sitio Futbolmania
	especiales.elcomercio.com	Especiales del Comercio
	especiales.benditofutbol.com	Especiales de Bendito Futbol
	especiales.ultimasnoticias.ec	Especiales de últimas noticias
	www.arteducarte.com	Sitio de arteducarte
	educaccion.elcomercio.com	Sitio de Educaccion
	paper.elcomercio.com	Edición del Comercio y sus suplementos para sistemas inteligentes
	paper.ultimasnoticias.ec	Edición de últimas noticias para sistemas inteligentes
	www.compraya.ec	Sitio de ofertas de Grupo El Comercio
	inmuebles.elcomercio.com	Venta de Clasificados de inmuebles vía web
	www.artepatiosquito.com	Sitio Arte patios Quito
	www.club.elcomercio.com	Sitios de promociones exclusivo para suscriptores
	www.ecuadoradio.ec	Sitio Web de las radios Quito y Platinum
	File_server	Servidor de archivos de Redacción
	Preprensa	Servidor de archivos Preprensa

CONTINÚA ⇨

Servidor de Archivos	File_servergec	Servidor de archivos general
	Admin_sus	Servidor de archivos gerencias
	Srv_ecuadoradio	Servidor de archivos administrativo ecuadoradio
	Srvbackupradios	Servidor de respaldos radio Quito y Platinum
	srv_backupradios	Servidor de archivos Ag. Guayaquil

Fuente: (Autor)

4.5.1.2. Elaboración de Políticas

Las políticas se elaboran con el fin de tener estándares y mejores prácticas a la hora de realizar procedimientos o actividades relacionas con los servicios TI; estos deben tener aplicación a largo plazo además de guiar el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas deben ser aprobadas por las directivas de una organización.

El desarrollo de las políticas debe iniciar priorizando los temas que deben abordarse, la identificación de los servicios y activos a proteger, para esto se puede realizar las siguientes actividades.

- Seleccionar las áreas que utilicen información que deba ser protegida por alguna ley.
- Identificar información utilizada para la toma de decisiones críticas dentro de la organización.
- Definir la sensibilidad de la información.
- Especificar un esquema de clasificación de información.

Las políticas del plan de continuidad del Departamento de Desarrollo Digital y Tecnología definirán los elementos necesarios para asegurar los activos y servicios de la empresa, por lo cual es necesario la participación de miembros

del Departamento directamente relacionados con las aplicaciones. Es importante contar con un equipo que se encargará de autorizar cambios y actualizaciones de los documentos relacionados, en este caso se establecerá el equipo según la aplicación o servicio. A continuación, en la figura 78, se detalla el flujo de validación y aprobación de una política dentro del Departamento.

Figura 78 Flujo de validación y aprobación de las políticas

Fuente: (Autor)

4.5.1.3. Especificación de Alcance.

El Plan de continuidad del negocio para el Departamento TI busca establecer los pasos y lineamientos a seguir para garantizar la continuidad de la operación de los servicios TI a pesar de ocurrir algún desastre.

Se desarrollará el ciclo de vida del plan de continuidad, cumpliendo con las cuatro etapas que menciona ITIL, tomando en cuenta los servicios y procesos críticos del Departamento TI. El alcance del plan depende de la investigación y de los recursos disponibles para su inversión.

4.5.1.4. Asignación de Recursos.

Para que el plan de continuidad tenga resultados positivos es necesario contar con recursos necesarios para salir de una emergencia. Se debe tomar en cuenta que en una emergencia no es el mejor momento para investigar en documentación o manuales como solventar el inconveniente.

Es importante y necesario adelantarnos a un problema, estar preparados para solventar el inconveniente conociendo las herramientas a utilizar y el personal responsable de cada función. En este apartado se detallará los recursos que dispone actualmente el Departamento de TI de GEC, conociendo esto y conforme se realice los estudios para elaborar el plan de contingencia se implementará los recursos necesarios para garantizar la seguridad de la información y servicios TI.

Los recursos con los que se cuenta en el Departamento de TI son:

- **Recursos Financieros:** Se tiene un presupuesto anual que se asigna al departamento de tecnología para invertir en recursos informáticos.
- **Recursos Humanos:** Al momento existen 28 personas en el departamento de Tecnología, de los cuales 6 personas se encargan de la producción y operación de los distintos servicios TI.
- **Recursos Tecnológicos:** Debido a la situación económica que atraviesa la empresa es difícil disponer de todos los recursos que se requiere, así como el soporte, es por esto que se debe buscar las mejores alternativas tecnológicas para que la inversión no sea muy costosa.

4.5.2. Etapa de requerimiento y Estrategia.

4.5.2.1. Análisis de impacto en la compañía

El análisis de impacto en la compañía consiste en identificar el impacto de la interrupción de los servicios TI en el negocio y determinar los requerimientos

necesarios para recuperar los procesos críticos del negocio una vez ocurrido el desastre.

El área de Infraestructura & Operaciones durante los últimos años ha realizado un esfuerzo para levantar información y documentar los servicios que soportan a la compañía, así como los componentes tecnológicos que soportan los mismos.

Para la selección de los servicios críticos nos ayudaremos de la tabla de valoración de impactos, la cual muestra la siguiente escala, (ver tabla 12).

Tabla 12
Valoración de Impactos

CALIFICACIÓN	CRITERIO	VALOR
Crítico	El proceso es fundamental para el cumplimiento de los objetivos de la empresa	4
Alto	El proceso aporta de manera importante para el cumplimiento de los objetivos de la empresa	3
Medio	El proceso aporta de una manera menor para el cumplimiento de los objetivos de la empresa	2
Bajo	El proceso no afecta para el cumplimiento de los objetivos de la empresa	1

Fuente: (Autor)

Tabla 13
Análisis de criticidad del Sistema Editorial

Servicio General	Servicio específico	# Servidores	Área Afectada	Criticidad
	Xalok info	1	RIM, Centro de Documentación	3
	Robots Publicidad	1	Preprensa	3
	Robots Visualización	4	RIM	2

CONTINÚA

Sistema Editorial	Robot Imágenes	1	RIM Preprensa	3
	Robots Filmación	2	RIM Preprensa	2
	XalokRed	3	RIM Preprensa	4
	Xalok Docs	1	RIM	1
	Xalok Previsiones	1	RIM	2
	Xalok_Indicadores	1	RIM Administrativo	1

Fuente: (Autor)

Tabla 14
Análisis de criticidad del Sistema Financiero, Facturación y Ventas

Servicio General	Servicio específico	# Servidores para el servicio	Área Afectada	Criticidad
Sistemas ERP	PeopleSoft	3	Financiera, Administrativa, Tecnología, Distribución, Preprensa, PostPrensa Optativos y Suscripciones Mercadeo y Ventas.	4
Facturación y Ventas	AplicacionesEC	1	Financiera, Administrativa, Tecnología, Distribución, Preprensa, PostPrensa Optativos y Suscripciones Mercadeo y Ventas	3
	Pongrass	1	Call Center, Aras	4
	Buxis	1	Recursos Humanos	2
	RBM	2	Call Cener, Aras Usuarios Externos	2
	Facturación Electrónica	1	Administrativa Financiera	4
	Cubos	1	Administración Comercial	1

Fuente: (Autor)

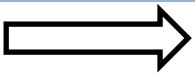
Tabla 15
Análisis de criticidad del Sistema de Imágenes y Workflow

Servicio General	Servicio específico	# Servidores para el servicio	Área Afectada	Criticidad
Procesamiento de Imágenes	Voyager, WorkSpace y Asura	3	Ventas, Preprensa, Diseño, CallCenter Clientes externos	4
Workflow	Trueflow	1	Preprensa Post Prensa	4

Fuente: (Autor)

Tabla 16
Análisis de criticidad de los Sitios Web

Servicio General	Servicio específico	# Servidores para el servicio	Área Afectada	Criticidad
Sitios Web	www.elcomercio.com	6	RIM, usuarios externos	4
	www.benditofutbol.com	4	RIM, usuarios externos	4
	www.revsitalideres.ec	5	RIM, usuarios externos	4
	www.revistafamilia.ec	1	RIM, usuarios externos	4
	www.ultimasnoticias.ec	1	RIM, usuarios externos	4
	futbolmania.elcomercio.com	1	RIM, usuarios externos	1
	especiales.elcomercio.com	1	RIM, usuarios externos	3
	especiales.benditofutbol.com	1	RIM, usuarios externos	3
	especiales.ultimasnoticias.ec	1	RIM, usuarios externos	3

CONTINÚA 

	www.arteducarte.com	1	RIM, usuarios externos	2
	educaccion.elcomercio.com	1	RIM, usuarios externos	2
	paper.elcomercio.com	1	RIM, usuarios externos	4
	paper.ultimasnoticias.ec	1	RIM, usuarios externos	2
	www.compraya.ec	1	Unidad digital usuarios externos	4
	inmuebles.elcomercio.com	1	Call Center, Aras Clientes externos	2
	www.artepatiosquito.com	1	RIM, usuarios externos	2
	www.club.elcomercio.com	1	Suscripciones Usuarios externos	2
	www.ecuadoradio.ec	1	Usuarios externos	3

Fuente: (Autor)

Tabla 17
Análisis de criticidad de los servidores de archivos

Servicio General	Servicio específico	# Servidores	Área Afectada	Criticidad
Servidores de Archivos	File_server	1	RIM, Unidad Digital, Optativos y Suscripciones, Call Center, Aras,	3
	Preprensa	1	Preprensa, Diseño Editorial	4
	File_servergec	1	Todas las áreas	3
	Admin_sus	1	Todas las áreas	4
	Srv_ecuadoradio	1	Usuarios Ecuadoradio	3
	Srvbackupradios	1	Usuarios Radio Quito y Platinum	3
	srv_redacgyq	1	Usuarios Regional Guayaquil	3

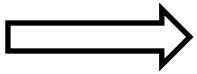
Fuente: (Autor)

4.5.2.2. Componentes Tecnológicos que soportan los servicios

GEC tiene 3 ambientes de trabajo como se detalló anteriormente, en este caso el plan de contingencia es desarrollado únicamente para el ambiente de producción en donde se encuentran alojados los servicios anteriormente detallados. A continuación, se describe unos ejemplos de los componentes que soportan los servicios, (ver tabla 18), la tabla completa se encuentra detallada en el ANEXO 1.

Tabla 18
Inventario recursos tecnológicos para el ambiente de producción

INVENTARIO RECURSOS TECNOLOGICOS PARA EL AMBIENTE DE PRODUCCIÓN											
UBICACIÓN	TIPO DE COMPONENTE	Detalle	Marca	Sistema Editorial	Sistema ERP	Facturación y Ventas	Procesamiento Imágenes	WorkFlow	Sitios Web	Servidor de Archivos	Criticidad
MIAMI	Enlace	Enlace UIO - Miami	MojoHost						X		4
PLANTA	Enlace	Enlace UIO - Regionales	Telefónica / Level 3	X	X	X	X	X	X	X	4
PLANTA	Enlace	Enlace de datos	Telefónica / Level 3	X	X	X	X	X	X	X	4
PLANTA	Enlace	Enlace de internet	Telefónica / Level 3	X	X	X	X	X	X	X	4
PLANTA	Router	6500	Cisco	X	X	X	X	X	X	X	4
PLANTA	Switchs	Switchs para red de servidores y usuarios	Cisco	X	X	X	X	X	X	X	4
PLANTA	Storages	Almacenamiento para servidores virtuales y físicos	EMC / HP / IBM	X	X	X	X	X	X	X	4
PLANTA	Access Point	Access Point Wifi		X	X	X	X	X	X	X	3
PLANTA	FISICO	Firewall Quito	HP						X		4
PLANTA	FISICO	Directorio Activo 1	HP	X	X	X	X	X	X	X	4
DATACENTER	VIRTUAL	DCUIO02 (Directorio activo secundario)	Vmware								1

CONTINÚA 

PLANTA	FISICO	File_servergec	Supermicro							X	3
PLANTA	FISICO	Servidor 1 ambiente virtual editorial	HP	X							3
PLANTA	FISICO	Servidor 2 ambiente virtual editorial	HP	X							3
PLANTA	FISICO	Servidor 3 ambiente virtual editorial	HP	X							3
PLANTA	FISICO	Vcenteruio (Administración MV)	HP	X	X	X			X		4
PLANTA	FISICO	(PeopleSoft Application	HP		X	X					4
PLANTA	FISICO	PeopleSoft Process	HP		X	X					4
PLANTA	FISICO	PeopleSoft Base de datos	HP		X	X					4
PLANTA	FISICO	File_server	HP							X	3
PLANTA	FISICO	Compra Ya	HP						X		4
DATACENTER	VIRTUAL	Web server Sistema Editorial	Vmware	X							4
DATACENTER	VIRTUAL	Base de datos Sistema Editorial	Vmware	X							4
DATACENTER	VIRTUAL	Application del Sistema Editorial	Vmware	X							4
DATACENTER	VIRTUAL	BuxisProd (Sistema de Nómina)	Vmware			X					2
DATACENTER	VIRTUAL	Sistema de tickets de soporte	Vmware								1

CONTINÚA ⇨

DATACENTER	VIRTUAL	Antivirus	Vmware	X	X	X	X	X	X	X	4
MIAMI	FISICO	BDD EC.com	HP						X		4
MIAMI	FISICO	Middle1 EC.com	HP						X		4
MIAMI	FISICO	Storage EC.com	Supermicro						X		4
MIAMI	VIRTUAL	Backend EC.com	Vmware						X		4
MIAMI	VIRTUAL	Front EC.com	Vmware						X		4
MIAMI	VIRTUAL	Middle 2 EC.com	Vmware						X		4

Fuente: (Autor)

4.5.2.3. Tiempo máximo de recuperación de los servicios.

Una vez que se determinó los servicios críticos del negocio, se define el tiempo máximo de recuperación y se los clasifica de acuerdo a sus prioridades de recuperación. Se debe analizar cada caso, ya que no será lo mismo la aplicación que da servicio a la elaboración de las distintas ediciones, que la aplicación para el cálculo de la nómina que se ejecuta cada mes.

Para recuperar las aplicaciones y los datos en una contingencia se puede realizar varios pasos dependiendo del problema que se presente, ya sea desde restaurar copias de seguridad hasta restaurar un servidor, todo esto puede tomar minutos, horas o días.

Al revisar con el personal encargado de cada aplicación se establecieron los tiempos máximos de recuperación, los cuales siguiendo la tabla 19 correspondiente a la valoración de la criticidad se detalla el TMR por cada servicio.

Tabla 19
Valoración del TMR

Criticidad	TMR	Detalle	Simbología
4	0-24 horas	Recuperación inmediata	**A**
3	1 - 2 días	El proceso debe ser recuperado entre el primer día y el segundo día	**B**
2	1-5 días	El proceso debe ser recuperado antes del quinto día	**C**
1	1 - 7 días	El proceso debe ser recuperado antes del séptimo día	**D**

Fuente: (Autor)

A continuación, se especifica el TMR para el servicio del Sistema editorial, (ver tabla 20), los detalles para el resto de servicios se pueden encontrar en el ANEXO 2

Tabla 20
Análisis del TMR del Sistema Editorial

Servicio General	Servicio específico	Criticidad	TMR
Sistema Editorial	Xalok info	3	B
	Robots Publicidad	3	B
	Robots Visualización	3	B
	Robot Imágenes	3	B
	Robots Filmación	3	B
	XalokRed	4	A
	Xalok Docs	1	D
	Xalok Previsiones	2	C
	Xalok_Indicadores	1	D

4.5.2.4. Análisis del daño que causa la interrupción de un servicio.

Cuando se produce la interrupción de un sistema, aplicación o servicio soportado por el Departamento de TI, es importante determinar las consecuencias de la interrupción, con el fin de tener idea del impacto que se produce en el negocio si hay una paralización de operaciones. En la tabla 21 se da una breve descripción de las consecuencias de la detención de los servicios de TI.

Tabla 21
Análisis del daño en una interrupción

Servicio TI	Consecuencia
Sistema Editorial	Si se suspende el Sistema Editorial, se detiene el principal negocio de la empresa que es la generación de ediciones del Comercio, Líderes, Revista Familia, etc. No se podría trabajar en las ediciones diarias.ni adelantos.
Sistema ERP	Si se suspende el sistema de PeopleSoft, se detiene la facturación, la planificación de recursos empresarial, la generación de reportes de veta y compras; es decir se detiene el proceso contable de la empresa dado que varias áreas utilizan distintos módulos esenciales para el Core del negocio
AplicacionesEC	Si se suspende este servicio, se detiene la facturación de las ventas de optativos y publicidad, al igual que PeopleSoft varias áreas serán afectadas ya que utilizan distintos módulos
Pongrass	Si se suspende Pongrass, se detiene la venta de anuncios publicitarios vía telefónica o en las distintas Aras que tienen distribuido la empresa
RBM	Si se suspende este servicio, no se podrá realizar venta de anuncios publicitarios vía web
Buxis	Si se suspende este servicio, se detiene el módulo de gestión de Recursos Humanos
Facturación Electrónica	Si se suspende este servicio, se detiene el proceso de facturación electrónica, lo cual impediría generar y enviar los documentos electrónicos para los clientes.
Asura, WorkSpace y Voyager	Si se detienen estos servicios, se suspende el procesamiento de las imágenes y pdfs; tales como anuncios, artes, avisos, páginas de ediciones, etc.
Trueflow	Si se detiene el Sistema Trueflow, no se podrá generar las placas impresas con las páginas de las distintas ediciones, lo cual provocaría el no poder imprimir el diario y suplementos en la prensa.
Sitios Web	Si se suspende algún servicio web, dependiendo del tiempo provocaría una penalidad a nivel internacional por tener abajo el servicio, además de que afectaría a clientes ya que sus banners aparecen en cada sitio según lo contratado
Servidores de archivos	El no tener acceso a las unidades de red provoca que los usuarios no puedan ni guardar ni acceder a sus datos
Intranet	El daño de la intranet provoca que los usuarios no puedan ver y utilizar información publicada, formularios, datos financieros, aplicaciones de GEC.

CONTINÚA

Internet	El enlace a Miami permite la conexión hacia nuestros equipos en CoreSite y que las distintas aplicaciones puedan ser usadas por nuestros clientes, si se cae el enlace perderíamos la administración y se caerían los servicios webs alojados allí
	El enlace local permite la navegación rápida en el internet sin que sea necesario entrar a la red de la empresa, por lo tanto, si no se tiene este servicio no se podría acceder de manera rápida al internet.
Firewall	Si no se tiene disponible el Firewall, se perdería la comunicación con Miami y las distintas regionales, además de que personal de la empresa no podría acceder a la red interna desde fuera de ella
Cableado	El daño o interrupción de la red de cableado estructurado provoca que los usuarios no puedan acceder a varios servicios como Internet, Intranet, unidades de red, etc.

Fuente: (Autor)

4.5.2.5. Análisis de riesgos en GEC

El objetivo del análisis de riesgo es el de identificar los riesgos que puede afectar a la compañía, identificando las amenazas y sus consecuencias, de tal manera que en base a estos datos se pueda establecer las opciones de recuperación para mitigar los riesgos.

El análisis de estos riesgos es importante en el desarrollo de un plan de continuidad del negocio, por lo cual los puntos esenciales del análisis son:

- Identificar las amenazas potenciales que podrían causar interrupciones en las operaciones, (ver tabla 22).
- Establecer medidas preventivas para minimizar la ocurrencia del desastre.
- Proveer de un lugar seguro que no sea en las mismas instalaciones para respaldar el activo en caso de alguna contingencia.

Tabla 22
Amenazas relacionadas a la continuidad del negocio

ORIGEN DE LAS AMENAZAS		
TIPO	**AMENAZAS**	**POSIBILIDAD**
Amenazas Naturales	Incendio	x
	Terremoto/temblor	x
	Erupción volcánica	x
	Inundaciones	x
	Deslizamiento de tierra	
Amenazas Humanas	Hackers	x
	Accesos no autorizados a la planta	x
	Robo de equipos	x
	Virus	x
	Robo de datos o documentos	x
	Vandalismo	X
	Terrorismo	x
	Accidentes en el trabajo	x
	Violación de reglas en el trabajo	x
	Desastres provocados intencionalmente	x
	Huelgas o manifestaciones	
Amenazas Tecnológicas	Interrupción de energía eléctrica	x
	Daño de discos y componentes de servidores	x
	Falla de los servidores	x
	Virus en las aplicaciones de software	x
	Fallas del aire acondicionado	x
	Fallos o daños en la red	x
	Denegación de servicio	x

Fuente: (Autor)

Probabilidad de Ocurrencia de la amenaza.

Una vez identificado las amenazas, es importante valorar cada una de estas a fin de estimar una probabilidad de ocurrencia; se analiza dos factores, el ambiente o entorno donde se encuentra las instalaciones de la compañía y el histórico de los desastres suscitados. El nivel de probabilidad se calcula al realizar el producto del factor histórico con el factor actual teniendo como resultado los siguientes niveles e interpretación, (ver figura 79).

Nivel de probabilidad (h*a)	Interpretación
Nulo * Nulo	**Impensable**, No se cree que ocurra (Desestimar)
Bajo * Bajo	**Improbable**, con probabilidad de ocurrencia muy baja (Desestimar)
Bajo * Medio	**Posible**, con probabilidad de ocurrencia intermedia (Sin prioridad)
Medio*Medio	**Probable**, con probabilidad de ocurrencia alta (Prioridad)
Medio * Alto	**Casi Seguro**, con probabilidad de ocurrencia extrema (Urgente)
Alto * Alto	**Casi Seguro**, con probabilidad de ocurrencia extrema (Urgente)

Figura 79 Probabilidad de ocurrencia de amenazas en GEC

Fuente: (Autor)

A continuación, en la tabla 23, luego de realizar un análisis, se detalla el nivel de probabilidad de ocurrencia de las amenazas expuestas anteriormente dentro de la compañía Grupo El Comercio.

Tabla 23
Cálculo de nivel de probabilidad de una amenaza

AMENAZAS	HISTORICO (h)	PERCEPCION ACTUAL (a)	NIVEL DE PROBABILIDAD (p=h*a)
Incendio	Bajo	Bajo	**Improbable**
Terremoto/temblor	Nulo	Nulo	**Impensable**
Erupción volcánica	Bajo	Medio	**Posible**

CONTINÚA ⇨

Inundaciones	Medio	Bajo	**Posible**
Deslizamiento de tierra	Nulo	Nulo	**Impensable**
Hackers	Medio	Bajo	**Posible**
Accesos no autorizados	Medio	Medio	**Probable**
Robo de equipos	Medio	Bajo	**Posible**
Virus	Medio	Medio	**Probable**
Eliminación de datos o documentos	Alto	Medio	**Casi seguro**
Vandalismo	Nulo	Nulo	**Impensable**
Accidentes en el trabajo	Medio	Bajo	**Posible**
Violación de reglas en el trabajo	Medio	Bajo	**Posible**
Desastres provocados	Bajo	Bajo	**Improbable**
Huelgas o manifestaciones	Nulo	Nulo	**Impensable**
Bloqueos de vías prolongadas	Nulo	Nulo	**Impensable**
Interrupción de energía eléctrica	Medio	Bajo	**Posible**
Daño de discos y componentes	Alto	Alto	**Casi Seguro**
Falla de los servidores	Alto	Alto	**Casi seguro**
Virus en las apps de software	Medio	Bajo	**Posible**
Fallas del aire acondicionado	Alto	Medio	**Probable**
Fallos o daños en la red	Medio	Bajo	**Posible**
Denegación de servicio	Bajo	Medio	**Probable**

Fuente: (Autor)

Evaluación de riesgos

A partir de las amenazas antes expuestas se calcula el riesgo tomando las amenazas con nivel de probabilidad “probable” y “casi seguro”, con el fin de proponer recomendaciones o contramedidas para mitigar los mismos y llegar al nivel de lo posible, (ver tabla 24).

Tabla 24
Evaluación de riesgos

AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
Accesos no autorizados	MEDIA	MEDIO	**MEDIO**
Virus	MEDIA	MEDIO	**MEDIO**
Eliminación de datos o documentos	ALTA	MEDIO	**ALTO**
Daño de discos y componentes de servidores	ALTA	MEDIO	**ALTO**
Falla de los servidores	ALTA	ALTO	**ALTO**
Fallas del aire acondicionado	MEDIA	ALTO	**ALTO**

Fuente: (Autor)

Como se pudo observar varios de los riesgos involucran a los servidores y al activo principal de la empresa que es la información, lo cual pone en riesgo los servicios que administra el departamento de desarrollo y Tecnología.

Es importante mitigar estos riesgos implementando un sistema de seguridad para acceso a las distintas áreas, herramientas de monitoreo de hardware, de uso de recursos y enlaces, realizar una mejor administración de los servidores de archivos otorgando los permisos adecuados a las diferentes carpetas que maneja cada área previa autorización de los jefes superiores, implementando políticas de respaldo, etc. Cabe recalcar que la empresa se encuentra pasando un proceso de transición o cambio de dueños por lo que es complicado adquirir nuevos equipos de última generación para reemplazar los servidores obsoletos, es así que se debe implementar alternativas para garantizar la continuidad de los servicios que se encuentra montados en los distintos servidores de GEC.

4.5.2.6. Estrategias de continuidad

En este proyecto se ha analizado los procesos y servicios que tiene a cargo el departamento de Tecnología, los cuales son indispensables tenerlos siempre disponibles para no afectar el trabajo diario de las personas y el servicio hacia

nuestros clientes. Es por esto que es importante establecer las estrategias de continuidad, las cuales están diseñadas para determinar en forma razonable las soluciones para recuperar un sistema o servicio que se encuentre caído y que puede afectar al negocio.

Después de haber analizado las amenazas y riesgos más probables, se establecerá las estrategias a seguir en cada escenario.

Escenario 1: Acceso no autorizado al DataCenter

En varias ocasiones personal de limpieza, técnicos de AC, etc, han ingresado al Dataceter sin autorización de la Gerencia de Tecnología o supervisión de algún ingeniero de Infraestructura, poniendo así en riesgo la operación de los equipos que se encuentran allí.

El ingreso de personal no autorizado ha puesto en riesgo la operación de los servicios en varias ocasiones, como, por ejemplo, cuando deshabilitaron el AC principal y no habilitaron el backup, provocando un incremento en la temperatura llegando a los 40 °C dentro del Datacenter, esto generó daños en discos de servidores y fuentes de poder del almacenamiento EVA.

La estrategia en este escenario es definir una norma y política de ingreso al Datacenter, la cual se encuentra redactada en el ANEXO 3; adicional y lo más importante es habilitar el acceso únicamente con tarjeta magnética. A continuación, en la figura 80 se define el procedimiento de acceso al Datacenter.

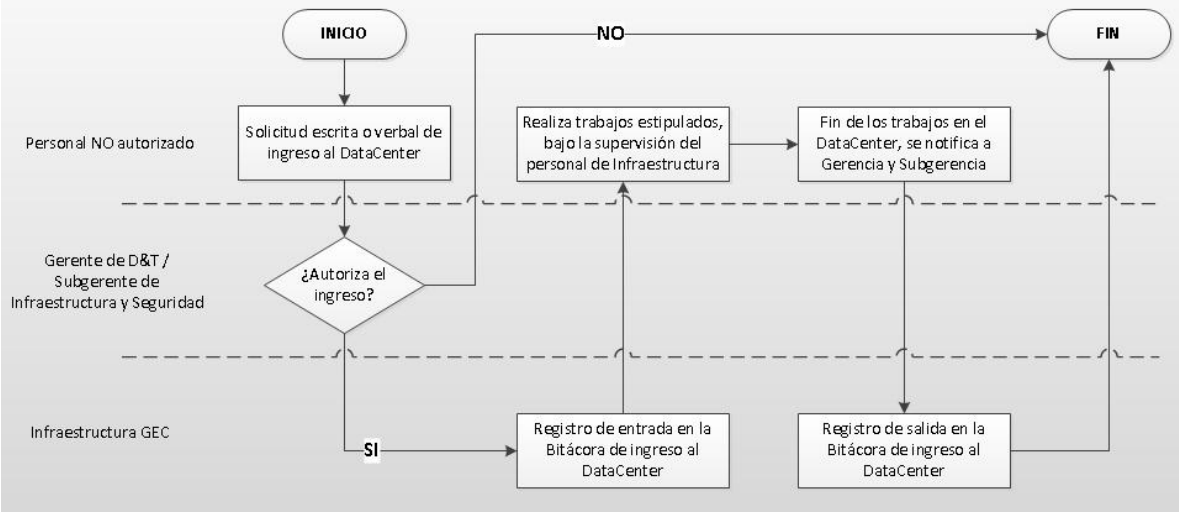


Figura 80 Procedimiento de acceso al Datacenter

Fuente: (Autor)

Una vez habilitado el ingreso al DataCenter por medio de la tarjeta magnética se define el personal que tendrá acceso, los cuales son los siguientes.

- Gerente de Desarrollo y Tecnología
- Subgerente de Infraestructura y Seguridad
- Ingeniero de Infraestructura
- Ingeniero de Operaciones
- Ingeniero Networking

Escenario 2: Virus en los servidores o estaciones de trabajo

Un virus informático es un programa computacional que se propaga de un computador a otro el mismo que interfiere con el normal funcionamiento de los equipos, incluso eliminando o dañando información del computador. En la compañía se tiene implementado un servidor de antivirus “Kaspersky”, el mismo que controla todos los servidores Windows y las estaciones de trabajo de los usuarios; no se ha instalado el agente en los servidores Linux debido a que

consume demasiados recursos, provocando así lentitud en las aplicaciones instaladas en esta plataforma.

En varias ocasiones se ha tenido inconvenientes con los servidores Linux, ya que la mayoría de estos brindan el servicio de páginas Web y han sido víctimas de hackeo, introduciendo troyanos, archivos php con código malicioso, provocando así que las páginas web muestren contenido inapropiado.

El personal de Infraestructura es el encargado de la supervisión de los servidores tanto Windows como Linux, en tanto que, el personal de seguridad es el encargado de administrar la consola de antivirus y detectar las amenazas en los servidores y equipos con sistema Operativo Windows. Para la revisión de archivos infecciosos en los servidores Linux se ha decidido hacer uso de la herramienta ClamAv.

Las estrategias en este evento son:

- Establecer políticas de seguridad para prevenir la instalación de aplicaciones maliciosas en las estaciones de trabajo, haciendo que los usuarios no puedan instalar ninguna aplicación si no es con la cuenta de administrador la cual maneja el personal de mesa de ayuda, infraestructura y seguridad.
- Restringir el acceso a internet en las estaciones de trabajo que por su uso no es necesario
- Deshabilitar los puertos USB en las estaciones de trabajo que no son requeridos
- Mantener actualizado en estaciones de trabajo y servidores Windows el antivirus Kaspersky
- Personal de Infraestructura analizará mensualmente mediante la herramienta ClamAv si existe archivos maliciosos en los servidores Linux.

A continuación, en las figuras 81 y 82 se define el procedimiento de análisis de virus en un sistema Linux y en sistemas Windows

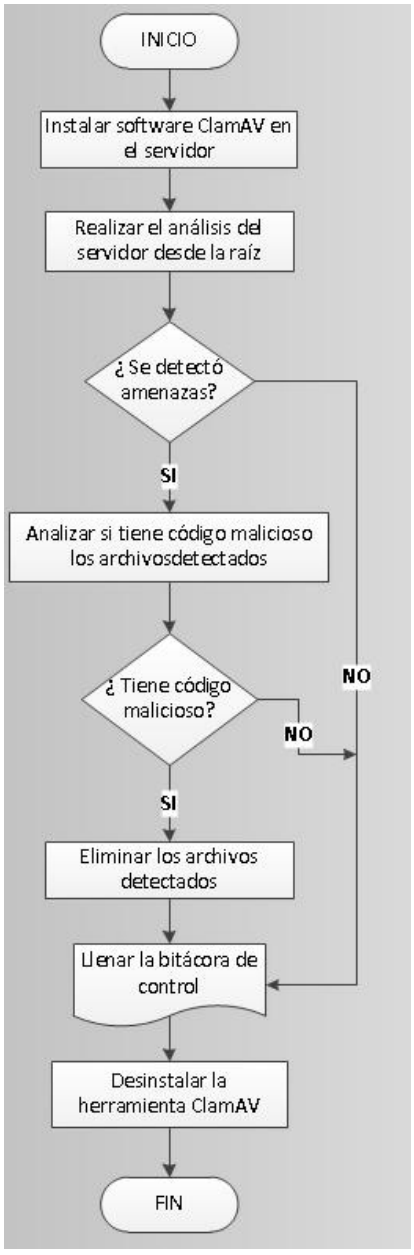


Figura 81 Procedimiento de análisis de virus en un sistema Linux

Fuente: (Autor)

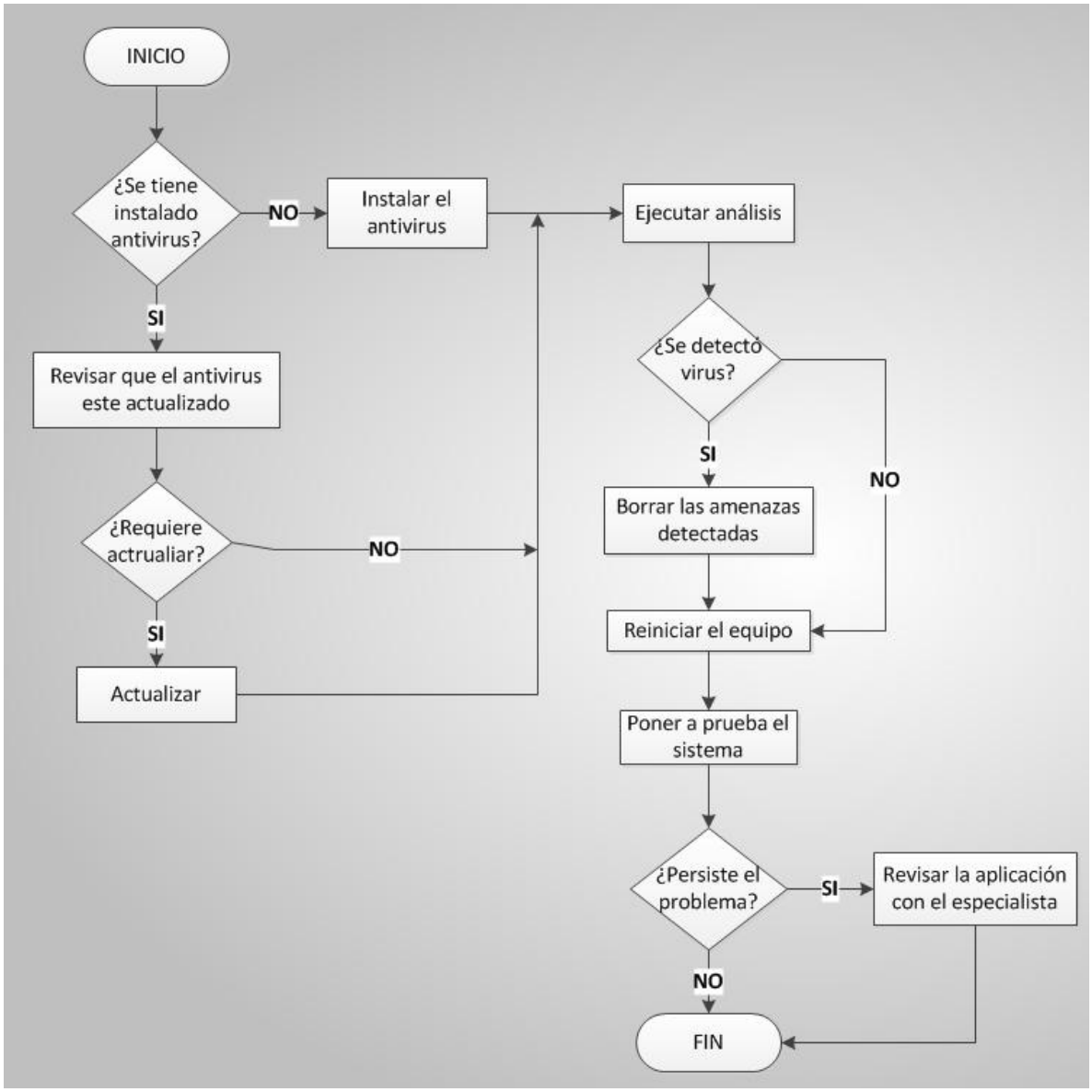


Figura 82 Procedimiento de análisis de virus en un sistema Windows

Fuente: (Autor)

Escenario 3: Eliminación de datos o documentos

La eliminación de datos o documentos es muy común en la compañía, varios usuarios pierden información de los file_servers o de las bases de datos ya sea que estos sean eliminados por equivocación o por daños en los mismos. El no

tener una política de backups provocaría pérdida importante en la empresa, así como tiempo valioso que los usuarios invierten al momento de realizar su trabajo.

Es por esto que se ha implementado una estrategia que garantizará tener backups de los archivos que se encuentran en los file_servers, configuraciones y bases de datos montadas en Windows y Linux, configuraciones de aplicaciones críticas como el ERP, Trueflow y aplicaciones propias de la compañía. La herramienta que se usará para obtener backups es el DataProtector los mismos que serán almacenados en cintas usando librerías de respaldo; más adelante se detallará el uso de esta herramienta.

El área de Infraestructura y Operaciones es la encargada de generar las políticas de respaldo y recuperación de datos, en la cual se detallará los servicios que se respaldarán, el tiempo de retención, el horario de backups, etc. Adicional se debe tener bitácoras de control, errores, revisión de backups y un formulario de recuperación que será llenado por el usuario cuando este necesite recuperar información. Dicho formulario puede ser encontrado en el ANEXO 4.

A continuación, en la figura 83 se puede observar el procedimiento implementado para obtener archivos, documentos, base de datos cuando estos han sido eliminados o dañados.

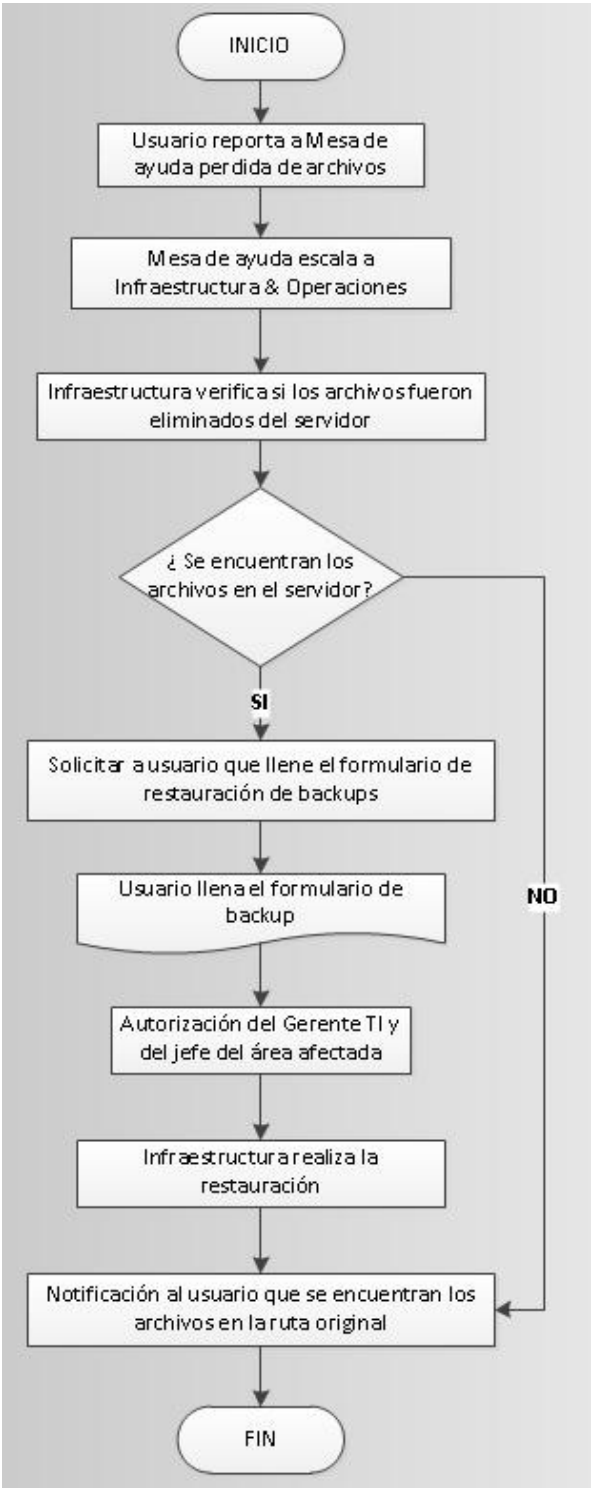


Figura 83 Procedimiento de obtención de backup

Fuente: (Autor)

Escenario 4: Daños de discos o componentes de servidores

Dado el caso que los componentes de los servidores como son discos, memorias, controladores, baterías, fuentes de poder tienen un tiempo de vida útil, estos pueden presentar fallas críticas que no pueden ser reparadas. En varias ocasiones se ha tenido inconvenientes con los discos duros, memorias, fuentes y baterías; lo cuales ha provocado lentitud en los servidores y tiempo de indisponibilidad en lo servicios al no detectar de manera oportuna alguna falla,

Es así que observando la criticidad de este evento se ha implementado varias estrategias para minimizar el riesgo de indisponibilidad.

Es importante configurar los servidores con Raid 1 o Raid 5 con lo cual podemos mantener al aire el servidor hasta reponer algún disco defectuoso, así también instalar con más de una fuente de poder para tener el equipo con alta disponibilidad.

El área de Infraestructura & Operaciones es la encargada de estar pendiente que ningún servidor presente alarmas en el hardware, pero es difícil tener una persona a cargo que este pendiente las 24 horas observando que no se presente ninguna alarma en los servidores o enlaces de red; es por esto que se ha implementado herramientas de monitoreo tales como HPSIM y WHATS UP GOLD que permiten monitorear los servidores físicos y los enlaces de red enviando un correo alertando sobre algún inconveniente en cualquier equipo. Con esto la persona de turno de mesa de ayuda y la persona de soporte remoto podrá alertar sobre el inconveniente para tomar acción sobre el evento de una manera más proactiva y eficiente siguiente el procedimiento detallado en la figura 84.

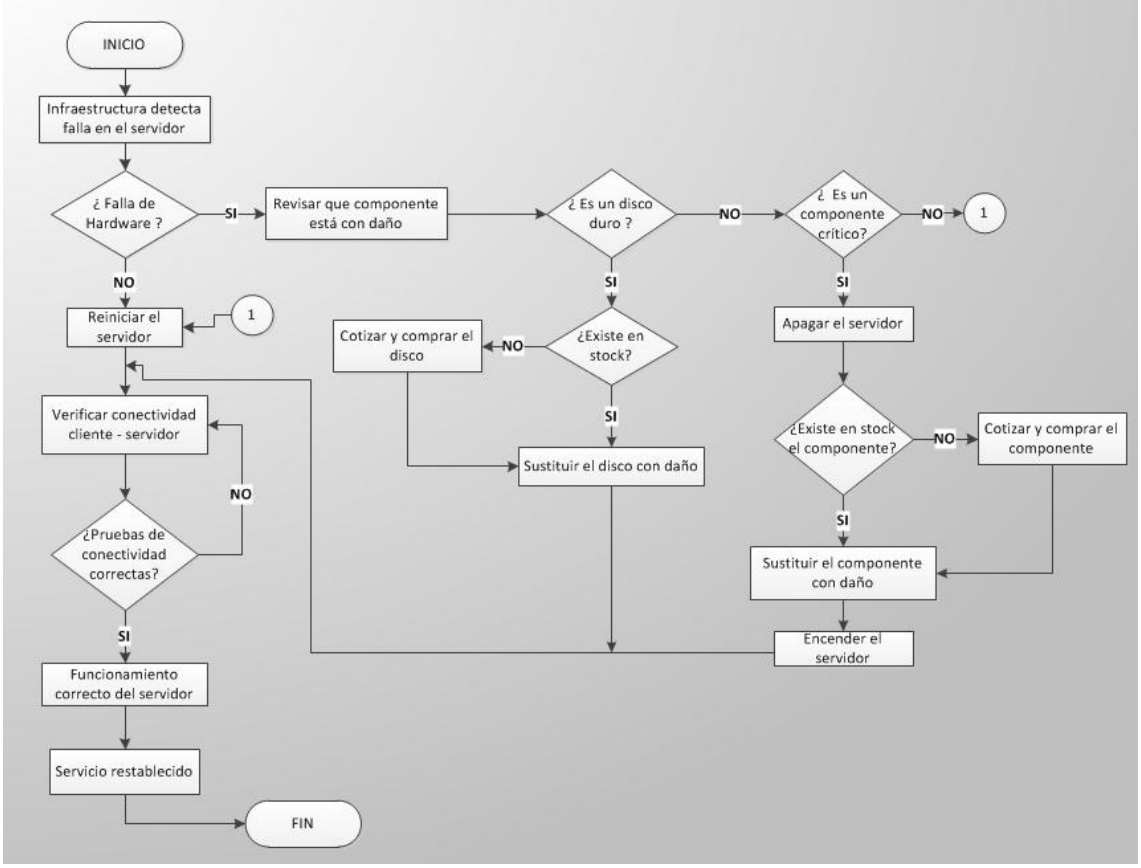


Figura 84 Procedimiento con daños de discos o componentes

Fuente: (Autor)

Como se ha mencionado anteriormente se ha implementado herramientas de monitoreo para mitigar el riesgo o gestionar de manera oportuna algún inconveniente.

- **HP SIM (System Insight Manager)**

HP Systems Insight Manager permite gestionar el hardware de los servidores HP y dispositivos de almacenamiento. Esta herramienta es de mucha utilidad en la compañía debido a que el 98 % de servidores implementados en GEC son de la gama de HP.

HP SIM reporta a una ubicación centraliza todos los eventos en los que se establecen para reaccionar como base para los informes de sucesos SIM de HP

(Dispositivo en el que se produjo el evento, Fecha/Hora de ocurrencia, gravead de evento, nombre del evento, descripción del evento). Es así que los servicios de HP SIM monitorean varios eventos del sistema (CPU, discos, Array Drive, ventiladores, NIC, fuente de alimentación, temperatura, etc).

El software HP SIM presenta varias ventajas a los administradores TI, como proporcionar una notificación proactiva de los fallos de componentes reales o inminentes, permite configurar políticas para ejecutar secuencias de comandos, reenviar eventos y notificar fallos a los usuarios.

Instalación y Configuración HP System Insight Manager

La herramienta de monitoreo y administración de infraestructuras HP SIM podemos obtener de manera gratuita de la página http://www8.hp.com/us/en/products/server-software/product-detail.html?oid=489496, en esta ocasión se obtuvo la versión 7.3. Una vez descargado procedemos con la instalación en un servidor Windows server 2008 previamente instalado el servicio SNMP.

1. Creamos una carpeta en la unidad C llamada HPSIM en donde se descomprimirá los archivos a instalar, (ver figura 85)

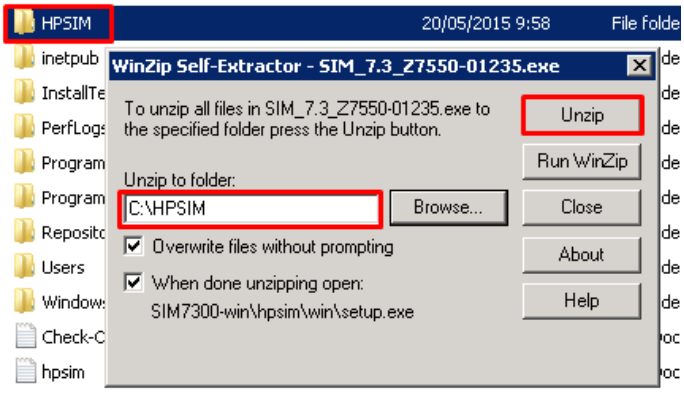


Figura 85 Obtención de instalador HPSIM

Fuente: (Autor)

2. Una vez descomprimido los archivos ejecutamos el setup de instalación que se encuentra en la ruta C:\HPSIM\SIM7300-win\hpsim\win y seguimos hasta la pestaña donde configuraremos la base de datos, (ver figura 86)

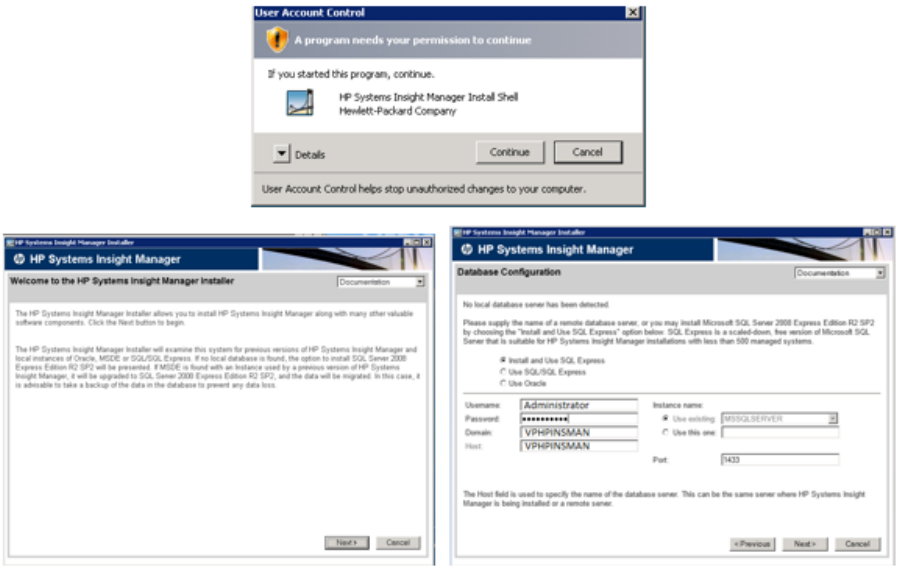


Figura 86 Configuración de instalación HPSIM

Fuente: (Autor)

3. Seguido escogemos el modo de instalación típica, con lo cual se instalará todos los paquetes necesarios, adicional sesteamos las credenciales de la cuenta que administrará los servicios de HPSIM, con esto procedemos con la instalación de la herramienta, (ver figura 87).

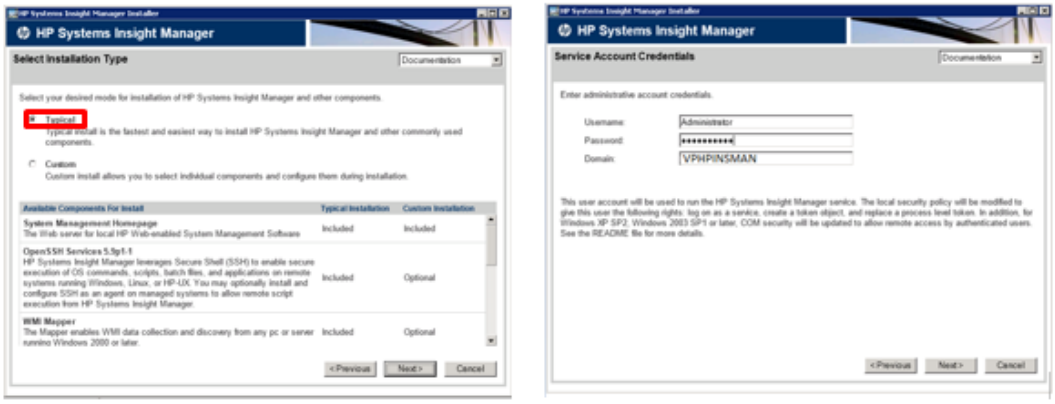


Figura 87 Instalación Típica de HPSIM

Fuente: (Autor)

4. Una vez instalado la herramienta podemos conectarnos desde cualquier equipo que se encuentre en la LAN haciendo uso de preferencia el navegador Firefox, digitando la siguiente dirección https://nombre_servidor:50000 e ingresando con las credenciales de Administrator, (ver figura 88).

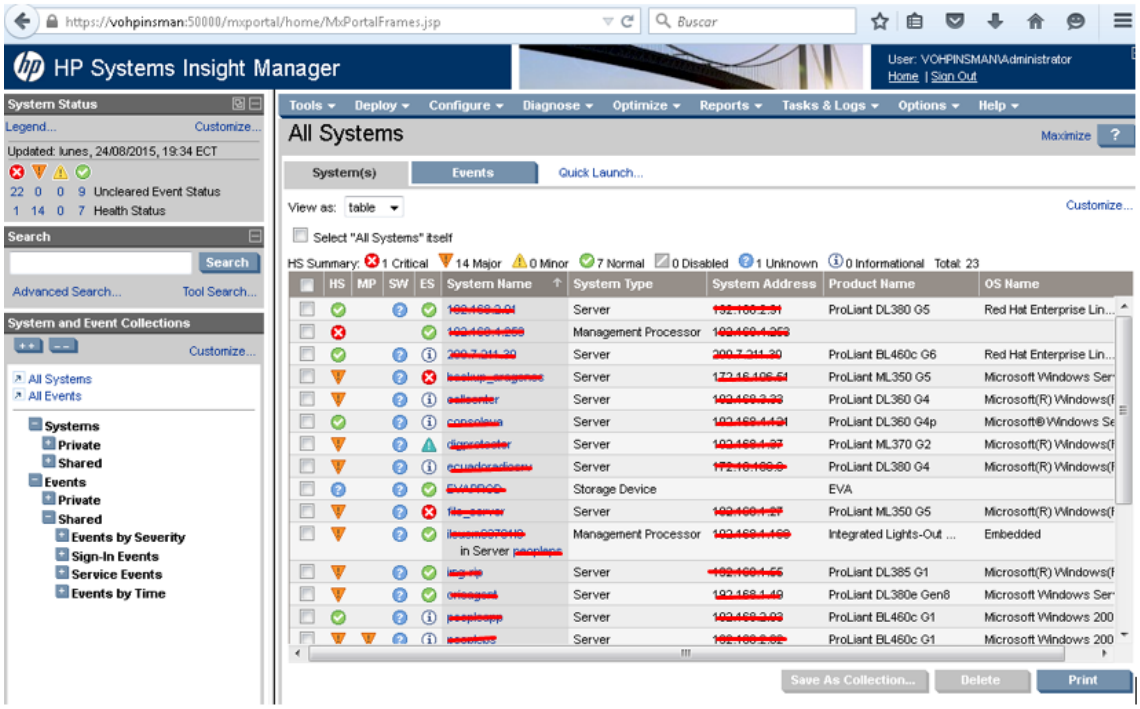


Figura 88 Interfaz HPSIM

Fuente: (Autor)

5. El siguiente paso es ingresar los servidores que se van a monitorear, se pueden ingresar individualmente o escogiendo un rango de red para que el sistema los descubra, en este caso ingresamos los servidores individualmente, escogiendo la opción de “Discovery” e ingresando el nombre e Ip del servidor, adicional para que se ejecute el agente colocamos las credenciales de administrador o un usuario que tenga permisos de administrador, (ver figura 89).

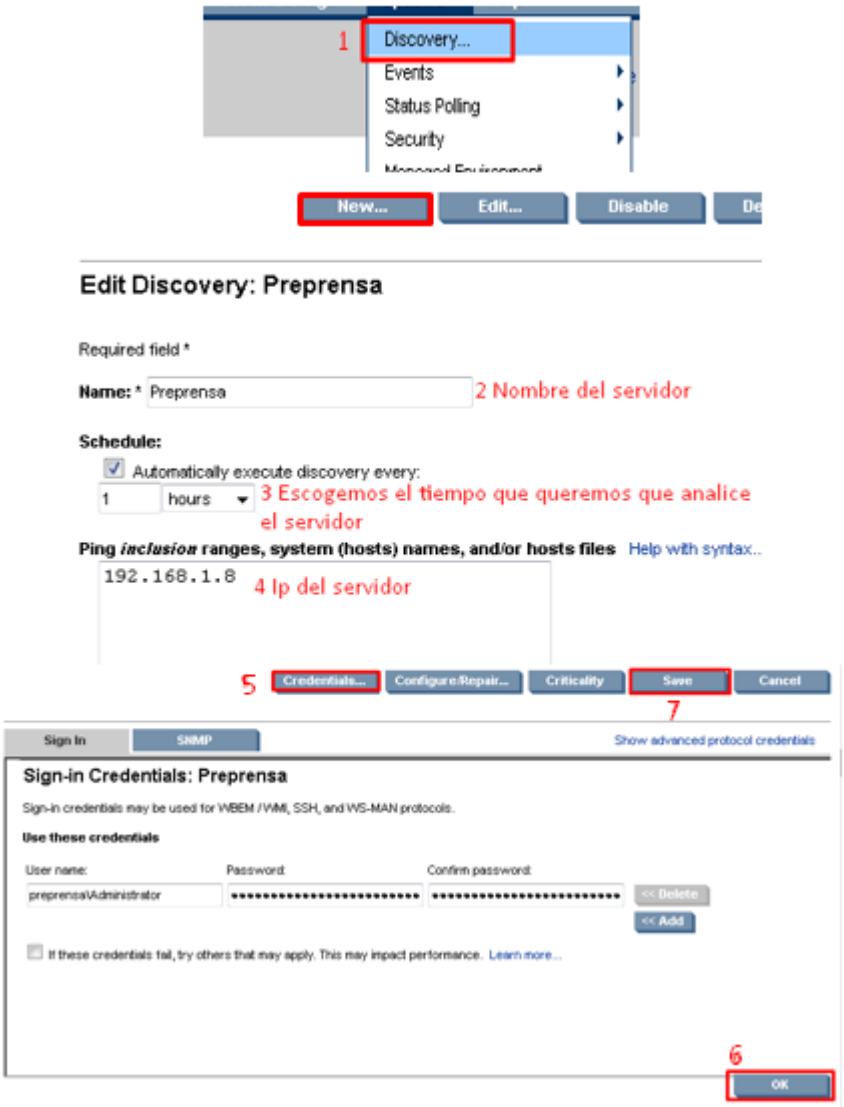


Figura 89 Ingreso de servidores a monitorear

Fuente: (Autor)

6. Para una mejor administración se crearon diferentes colecciones en las cuales se colocaron los servidores dependiendo su sistema operativo. Con esto se creará las diferentes alertas de manera ordenada y clara como se observa en la figura 90.

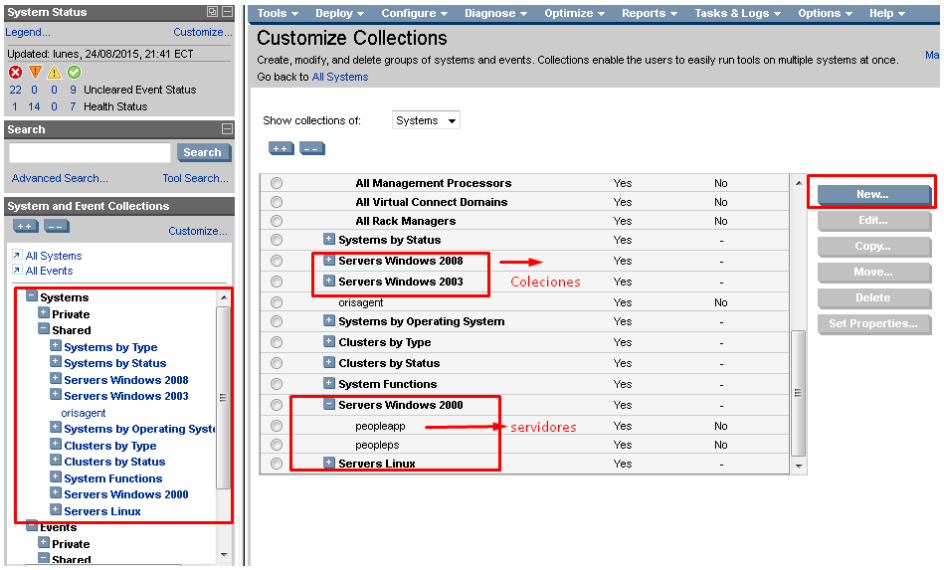


Figura 90 Creación de colecciones de sistemas

Fuente: (Autor)

7. Por último, se crea las alertas que deseamos que lleguen por correo dependiendo el evento ya sea este crítico, mayor, menor o satisfactorio. Para los fines del área se ha creado tareas que monitoreen y alerten cuando un dispositivo de los servidores tenga algún inconveniente lo cual nos alertará por correo electrónico y permitirá gestionar el evento de manera proactiva, (ver figuras 91, 92 y 93).

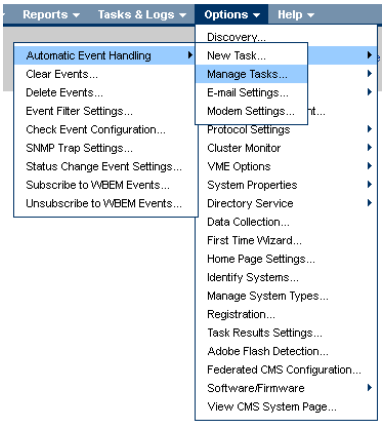


Figura 91 Administrador de eventos y tareas

Fuente: (Autor)

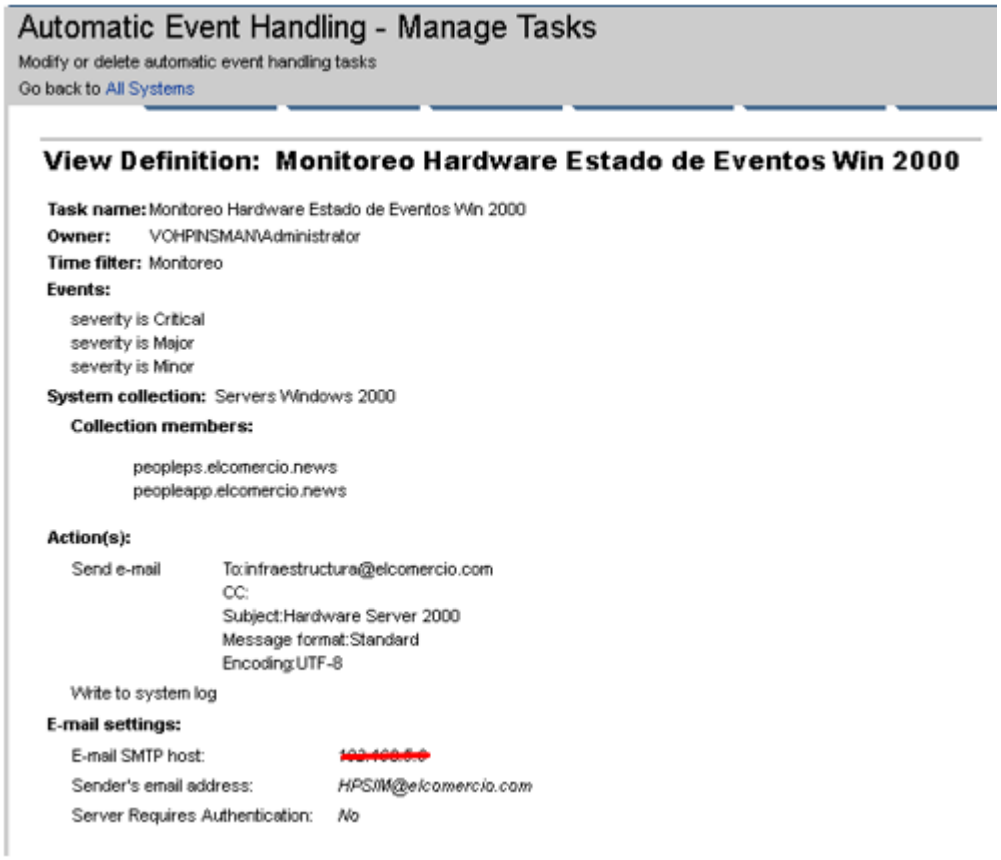


Figura 92 Configuración de una alerta

Fuente: (Autor)

	Name	Page	E-mail	CMS Tool	Forward	Assign	Clear	Log	Last Run
○	example - all desktop informational events						✓		Disabled
○	example - all linux MIB updates						✓	✓	Disabled
○	example - all server failed sign-in events							✓	Disabled
○	Monitoreo HardwareEstado de Eventos Linux		✓					✓	8/21/15 7:45 AM
◉	Monitoreo Hardware Estado de Eventos Win 2000		✓					✓	7/31/15 5:55 AM
○	Monitoreo Hardware Estado de Eventos Win 2003		✓					✓	8/19/15 12:20 PM
○	Monitoreo Hardware Estado de Eventos Win 2008		✓					✓	8/20/15 3:24 AM
○	Monitoreo Hardware - informacional Linux		✓					✓	8/15/15 12:04 AM

Figura 93 Alertas creadas para monitorear el hardware

Fuente: (Autor)

- **WhatsUp Gold**

WhatsUp Gold es una herramienta licenciada que permite el monitoreo unificado de disponibilidad de redes y servidores, lo cual permite evitar el tiempo de inactividad, realizar inventarios y monitorear automáticamente todos los dispositivos en las redes cableadas e inalámbricas.

Con esta herramienta se monitoreará los enlaces de datos e internet, además de los switches que se encuentran instalados en las distintas áreas de GEC, esto permitirá agilitar de manera inmediata el soporte y reducir el tiempo de indisponibilidad.

Instalación y Configuración WhatsUP Gold

El instalador de esta herramienta se puede obtener de la siguiente dirección http://www.whatsupgold.com/free-trial/whatsupgold.aspx, lamentablemente este software es licenciado, pero se puede obtener de forma gratuita por 1 mes, con lo cual se realizó pruebas y se validó su funcionamiento, es así que se aprobó la compra y se licenció para monitorear hasta 300 dispositivos. Una vez descargado la herramienta procedemos con la instalación la cual no es compleja, pero se puede seguir el manual de instalación que se encuentra en la dirección http://docs.ipswitch.com/NM/79_WhatsUp%20Gold%20v15/06_Languages/Spanish/Install_Config/index.htm?32253.htm?toc.htm. Como recomendación es aconsejable no escoger las opciones avanzadas de instalación y escoger la opción de instalar una nueva base de datos express.

Una vez instalado el software se abrirá la interfaz Web de WhatsUp Gold como la que se observa en la figura 94.

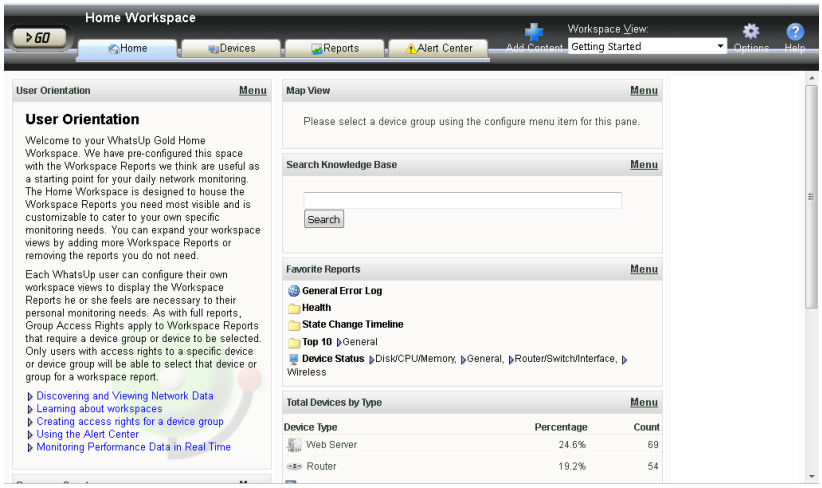


Figura 94 Interfaz Web de WhatsUp Gold.

Fuente: (Autor)

Para ingresar dispositivos podemos hacerlo desde la interfaz web o desde el servidor donde se encuentra instalada la herramienta, en este caso se va ingresar desde el servidor ya que se puede diseñar la interfaz web colocando imágenes, planos, líneas, cuadros, etc.

1. Crear un nuevo grupo dentro de *mi red*, en este caso se llamará MonitoreoII, (ver figura 95). Dentro del grupo podemos crear varios grupos para tener una mejor administración.

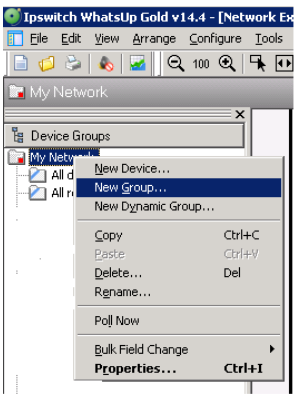


Figura 95 Creación Grupo de monitoreo - WhatsUp Gold.

Fuente: (Autor)

2. Ingresamos los dispositivos a monitorear, ingresando la Ip del dispositivo, somo se observa en la figura 96. Una vez ingresado el dispositivo podemos poner el nombre que identifica al mismo, el tipo de dispositivo, etc.

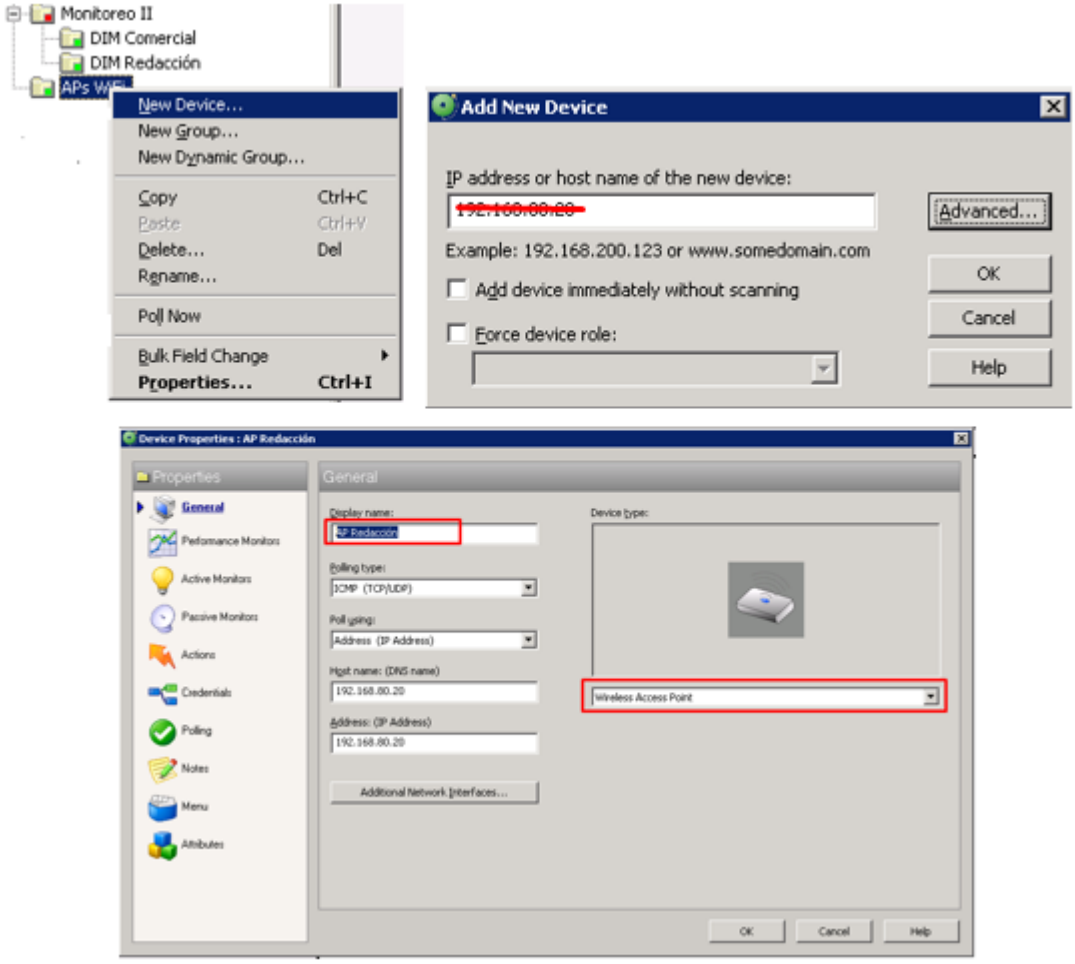


Figura 96 Ingreso de dispositivo a monitorear - WhatsUp Gold.

Fuente: (Autor)

3. La herramienta permite enviar alertas por mail según la acción y estado que configuremos, para este caso Se configuró las alertas para que lleguen por correo cuando un dispositivo se encuentre en estado “Down” o “UP”, (ver figura 97).

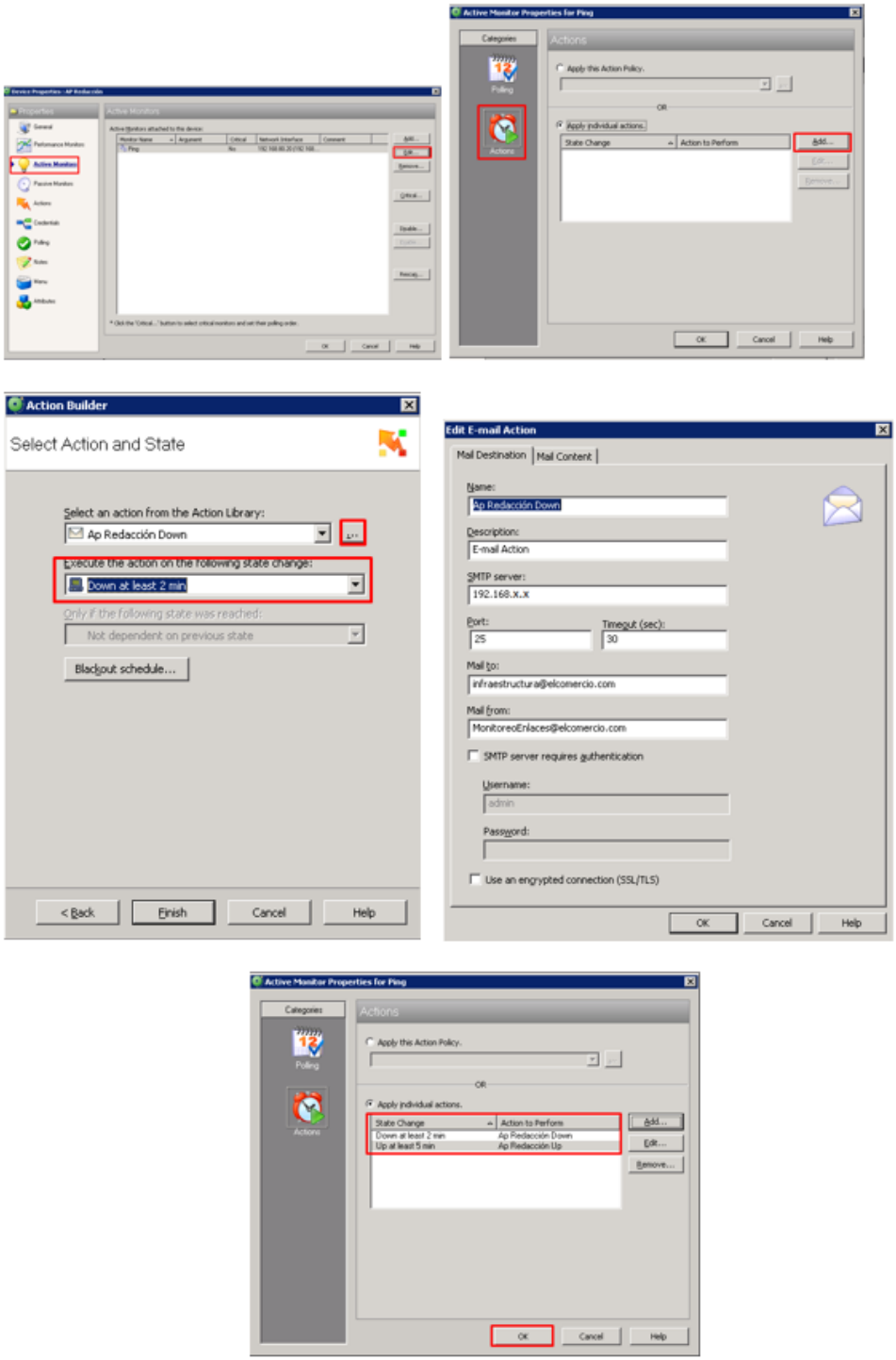


Figura 97 Creación de acciones y alertas - WhatsUp Gold.

Fuente: (Autor)

4. Una vez ingresado los dispositivos podemos diseñar nuestra vista de interfaz web ingresando planos, títulos, cuadros, imágenes. etc. como se muestra en la figura 98 la cual es la pantalla de monitoreo de GEC, en esta podemos divisar que se encuentran creada grupos la cual al hacer clic en esta nos lleva a otra pantalla donde se encuentra detallado los dispositivos correspondientes, como se observa en la figura 99.

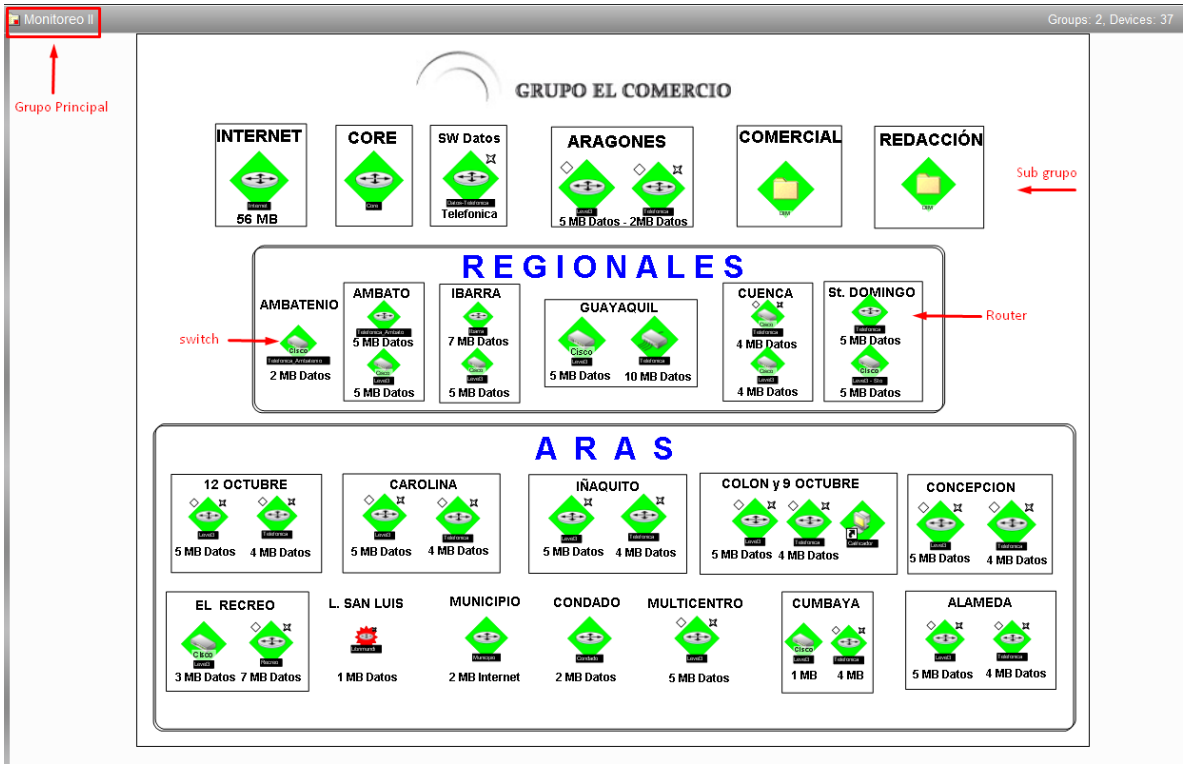


Figura 98 Diseño interfaz Web del grupo de Monitoreo GEC - WhatsUp Gold

Fuente: (Autor)

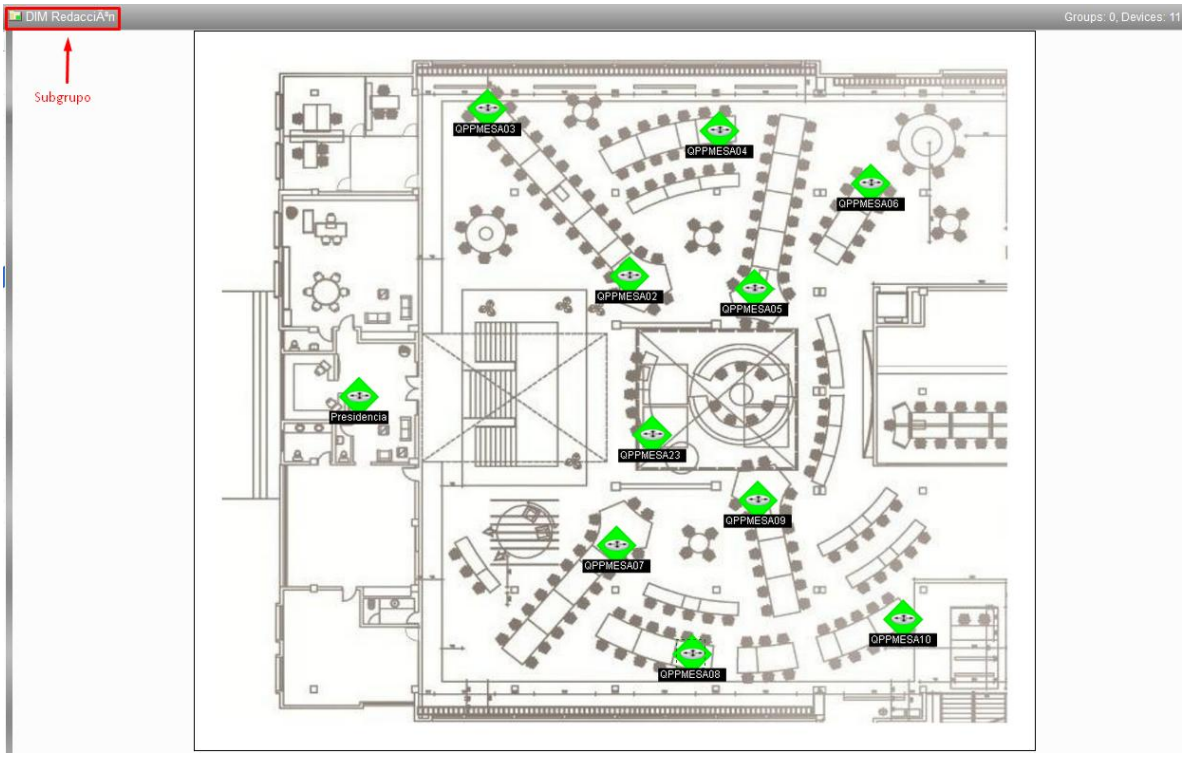


Figura 99 Diseño interfaz Web de un Sub Grupo de Monitoreo - WhatsUp Gold.

Fuente: (Autor)

Escenario 5: Falla de los servidores

Como se mencionó anteriormente GEC posee servidores físicos y virtuales, los cuales al ser máquinas corren el riesgo de algún momento fallar. En ocasiones se ha presentado este inconveniente, un servidor a colapsado y no ha sido posible ponerle productivo inmediatamente, provocando así indisponibilidad del servicio para el usuario y cliente por varios días, la solución para ese momento fue preparar un nuevo servidor y configurar el aplicativo lo cual demanda tiempo.

El hecho de tener servidores obsoletos pone en riesgo mayor la falla de estos, no obstante, el Departamento de TI debe garantizar la continuidad del servicio, por lo cual se ha implementado varias estrategias para garantizar la continuidad de los mismos.

- Los servidores a diferencia de los equipos terminales, trabajan todo el tiempo y prácticamente no tienen descanso. Es por esta razón, que cada cierto tiempo es necesario realizar mantenimiento preventivo para mantener el funcionamiento de los servidores lo más óptimo posible y evitar errores o situaciones que puedan mermar el funcionamiento de la compañía. El mantenimiento preventivo se lo realizará cada año y consta en actualizar el firmware, revisión de partes y limpieza de hardware. Al final de cada mantenimiento se realizará un informe que servirá para presentar a las auditorías externas. Como fase inicial de este proyecto y garantizar la funcionalidad de los equipos de GEC se realizó el mantenimiento de la infraestructura tanto de Miami, Quito y Guayaquil, el informe del mantenimiento puede encontrase en el ANEXO 5.
- Para garantizar la operatividad de un servidor virtual se implementó una herramienta que permite respaldar servidores virtuales los cuales podemos restaurar poner productivo al servidor en menos de 10 minutos. La herramienta se llama VeeamBackup la cual se explicará más adelante.
- Para servidores físicos que son críticos se ha visto la opción de virtualizarlos con la herramienta VirtualConverter con el fin de tener un backup del servidor, pero en virtual y así ponerlo productivo cuando ocurra algún desastre, en servidores que son imposibles virtualizarlos debido a que se conectan físicamente a otros dispositivos se ha visto la necesidad de colocar otro con similares características y tener una sincronización de los archivos para poner operativo en caso de una emergencia.

A continuación, en la figura 100 se puede observar el procedimiento a seguir cuando nos encontremos en este escenario.

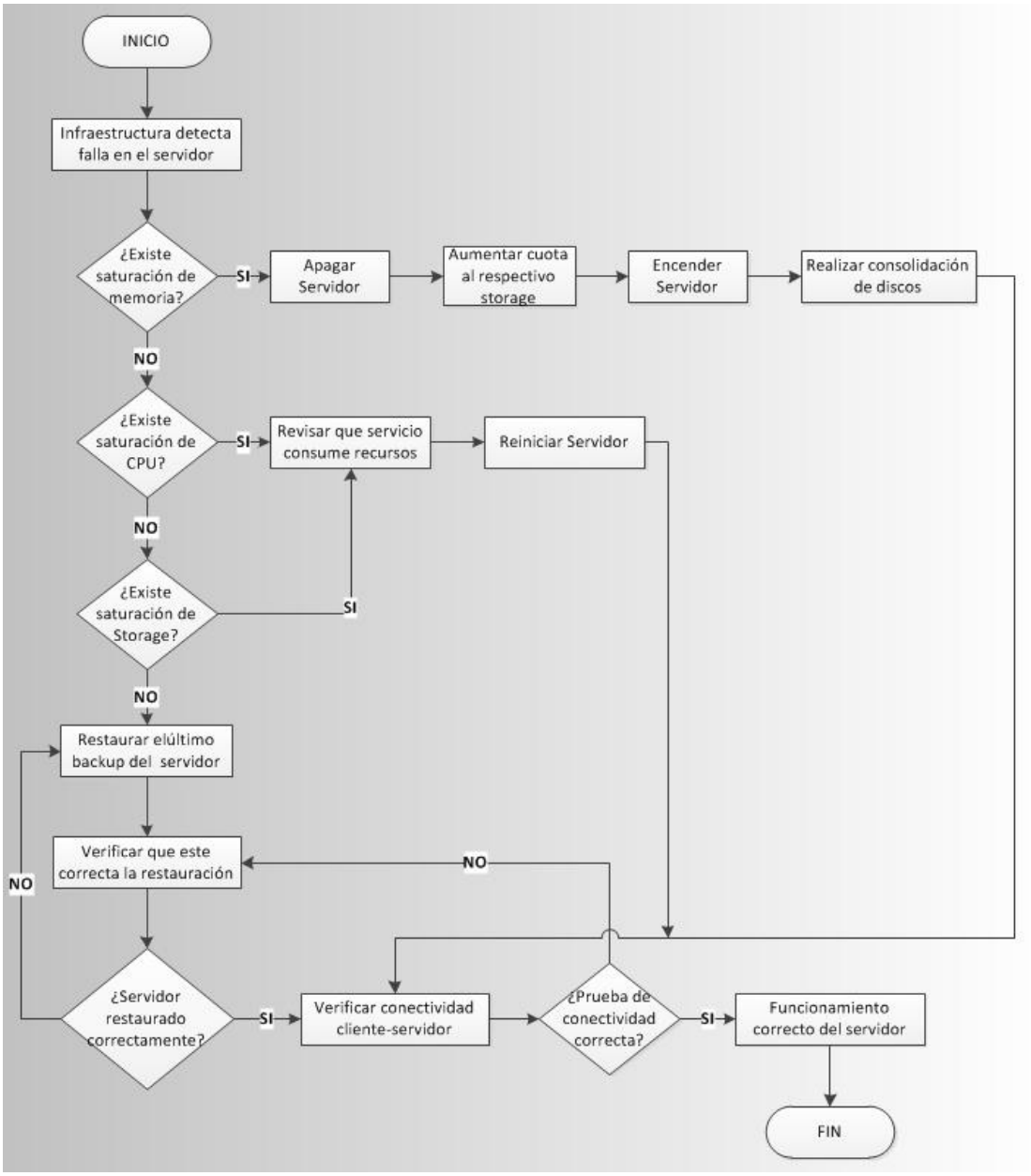


Figura 100: Procedimiento cuando existe fallas en un servidor

Fuente: (Autor)

Como se detalló anteriormente se ha visto la necesidad de implementar herramientas que permitan recuperar de manera rápida el servicio que brinda un servidor, es por esto que se ha implementado las herramientas VeeamBackup &

Replication y VirtualConverter los cuales permiten tener un backup virtual de los servidores.

- **VeeamBackup & Replication V8.**

Veeam Backup & Replication es un software que ofrece una recuperación rápida, flexible y fiable de las aplicaciones y datos virtualizados, alcanzando objetivos de tiempo de recuperación (RTOs) menores a 15 minutos. Este software es fiable ya que evalúa automáticamente cada backup y replica de vSphere y Hyper-V sin excepción, (ver figura 101). La herramienta se puede descargar desde el siguiente enlace http://www.veeam.com/es-lat/vm-backup-recovery-replication-software.html la cual es una versión gratuita valida por 30 días.

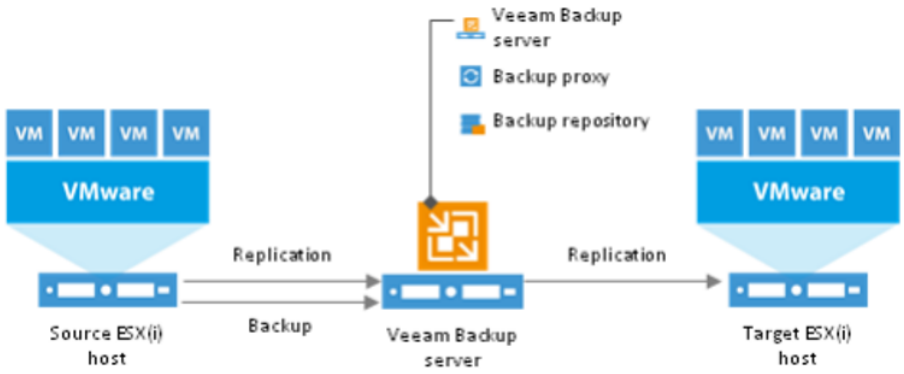


Figura 101 Diagrama de flujo Veeam Backup & Replication

Fuente: (Autor)

Instalación y Configuración de VeeamBackup & Replication

La instalación de este sistema se realizó en un servidor Windows Server 2008 con Netframework 4.0.

1. Para iniciar con la instalación insertamos el medio donde se encuentre el instalador, el cual es el archivo “setup.exe”, al abrir el ejecutable nos

aparecerá la siguiente ventana, donde daremos clic en la opción señalada, (ver figura 102).

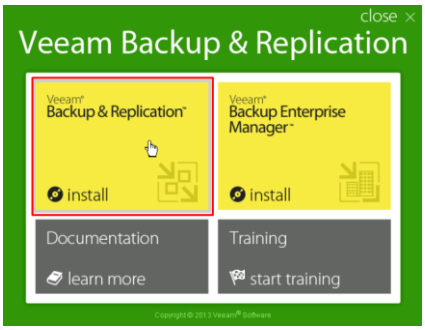


Figura 102 Inicio de instalación Veeam Backup & Replication

Fuente: (Autor)

2. Avanzamos las pantallas de bienvenida y de contrato, hasta la opción de cargar el archivo de licencia, el cual nos genera la página de Veeam y nos envía al correo de suscripción. Cargamos el archivo .lic y avanzamos con la instalación como se observa en la figura 103.

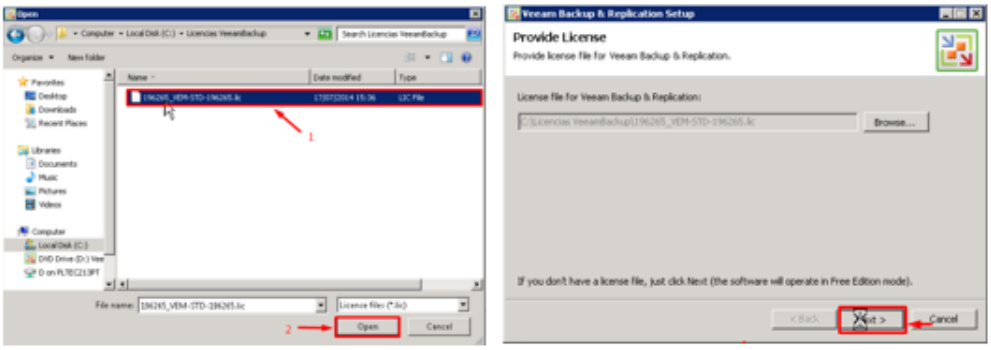


Figura 103 Cargando licencia de Veeam Backup & Replication

Fuente: (Autor)

3. Seguido escogemos por defecto los componentes a instalar, adicional el instalador verificará el sistema, en el cual tendremos que instalar los programas que son necesarios para que trabaje la herramienta.

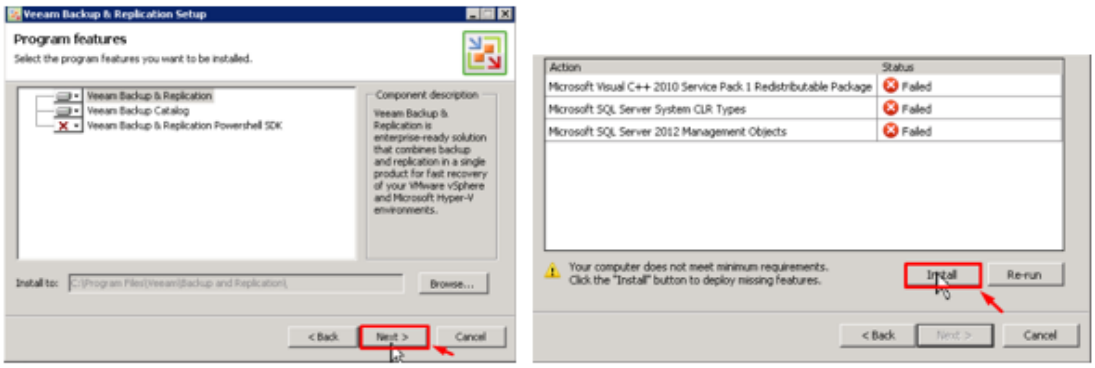


Figura 104 Instalación de componentes y programas necesarios para Veeam Backup & Replication

Fuente: (Autor)

4. A continuación, nos pedirá seleccionar o crear la BDD, en este caso instalaremos una nueva instancia de SQL server para crear la BDD en nuestro propio equipo, tal como se observa en la figura 105.

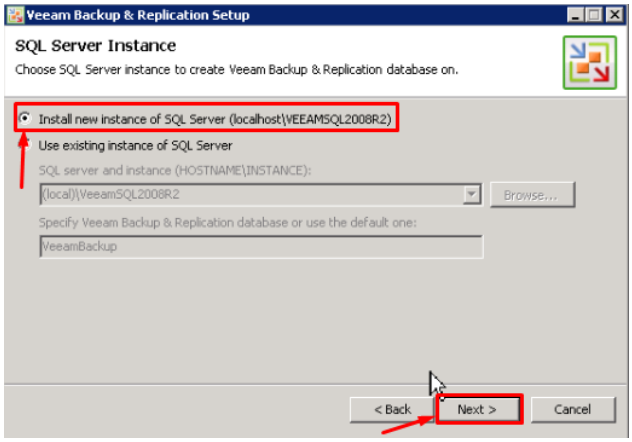


Figura 105: Instalación de SQLServer para Veeam Backup & Replication

Fuente: (Autor)

5. Finalmente se escoge los puertos que usará el software y los directorios donde se crearán el vPower NFS y el Guest file system catalog, lo cual de preferencia dejaremos por defecto, (ver figura 106). Con esto finalizamos la instalación de Veeam Backup & Replication.

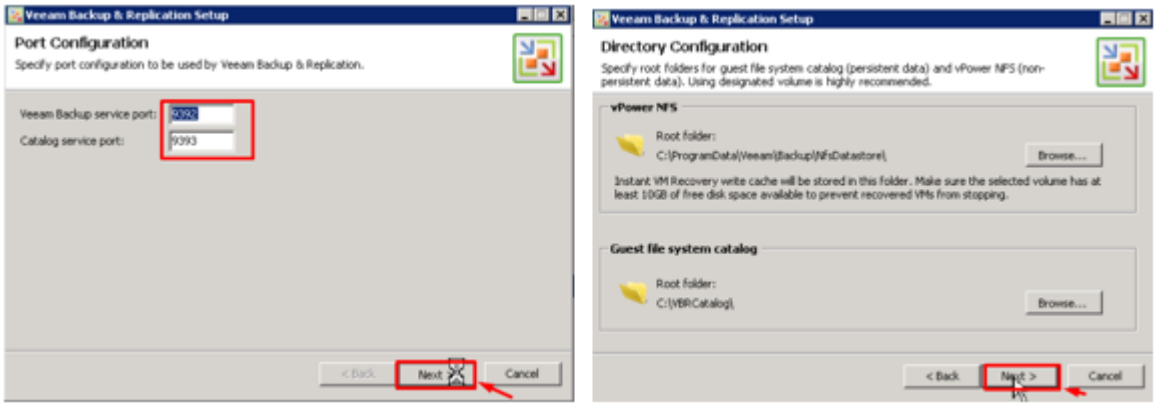


Figura 106: Configuración de puertos y directorios para Veeam Backup & Replication

Fuente: (Autor)

6. Una vez terminada la instalación, ingresamos por primera vez a la interfaz, donde se muestra una pantalla similar a la figura 107.

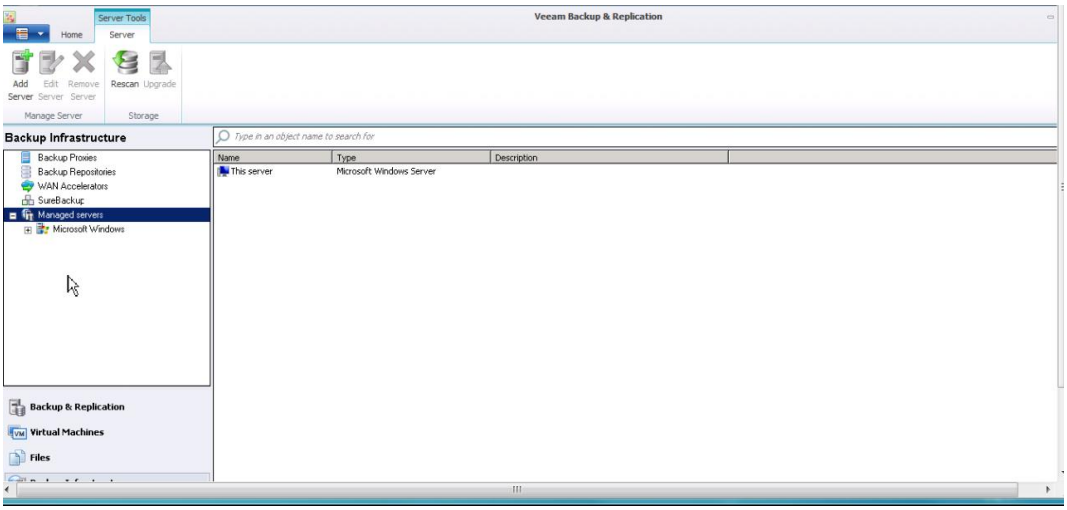


Figura 107 Interfaz Veeam Backup & Replication

Fuente: (Autor)

7. Una vez lista la herramienta, lo primero a realizar será agregar los servidores físicos que conforman los ambientes virtuales digitando el nombre o Ip del servidor y sus credenciales de administrador. En nuestro caso ingresaremos servidores Vmware vSphere, (ver figura 108).

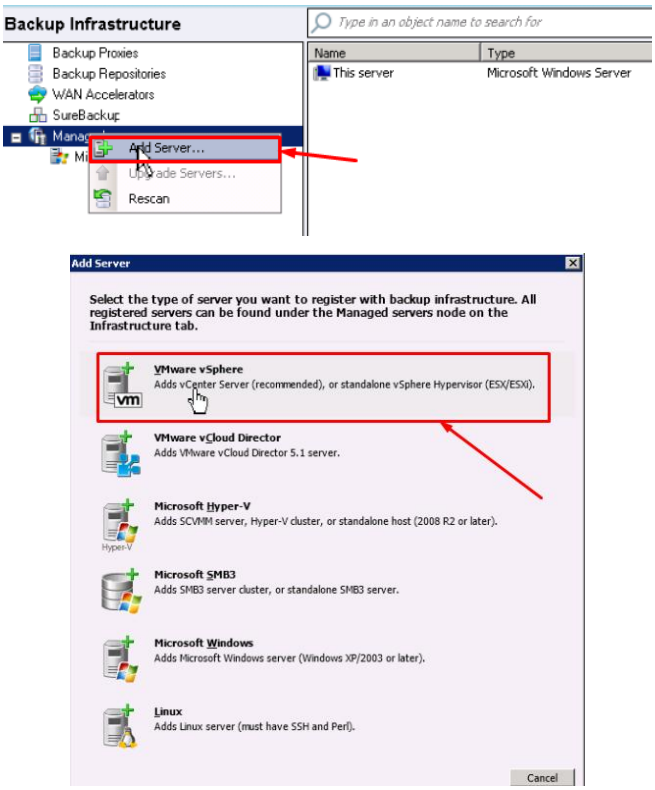


Figura 108 Ingreso servidores físicos a Veeam Backup & Replication

Fuente: (Autor)

8. Luego de unos segundos, nos aparecerá la ventana de confirmación de que el servidor fue creado. Y en el panel principal observaremos los servidores ingresados.
9. Para una mejor administración de los backups se puede crear repositorios en donde pueden ser almacenados los backups de las máquinas virtuales, en este caso crearemos repositorios de desarrollo, test y producción en un servidor que tiene mayor espacio de almacenamiento, (ver figura 109). Los repositorios pueden ser de un servidor Windows, Linux o una carpeta compartida mapeada en el servidor local. Una vez configurado los repositorios se procederá a crear los trabajos de backup

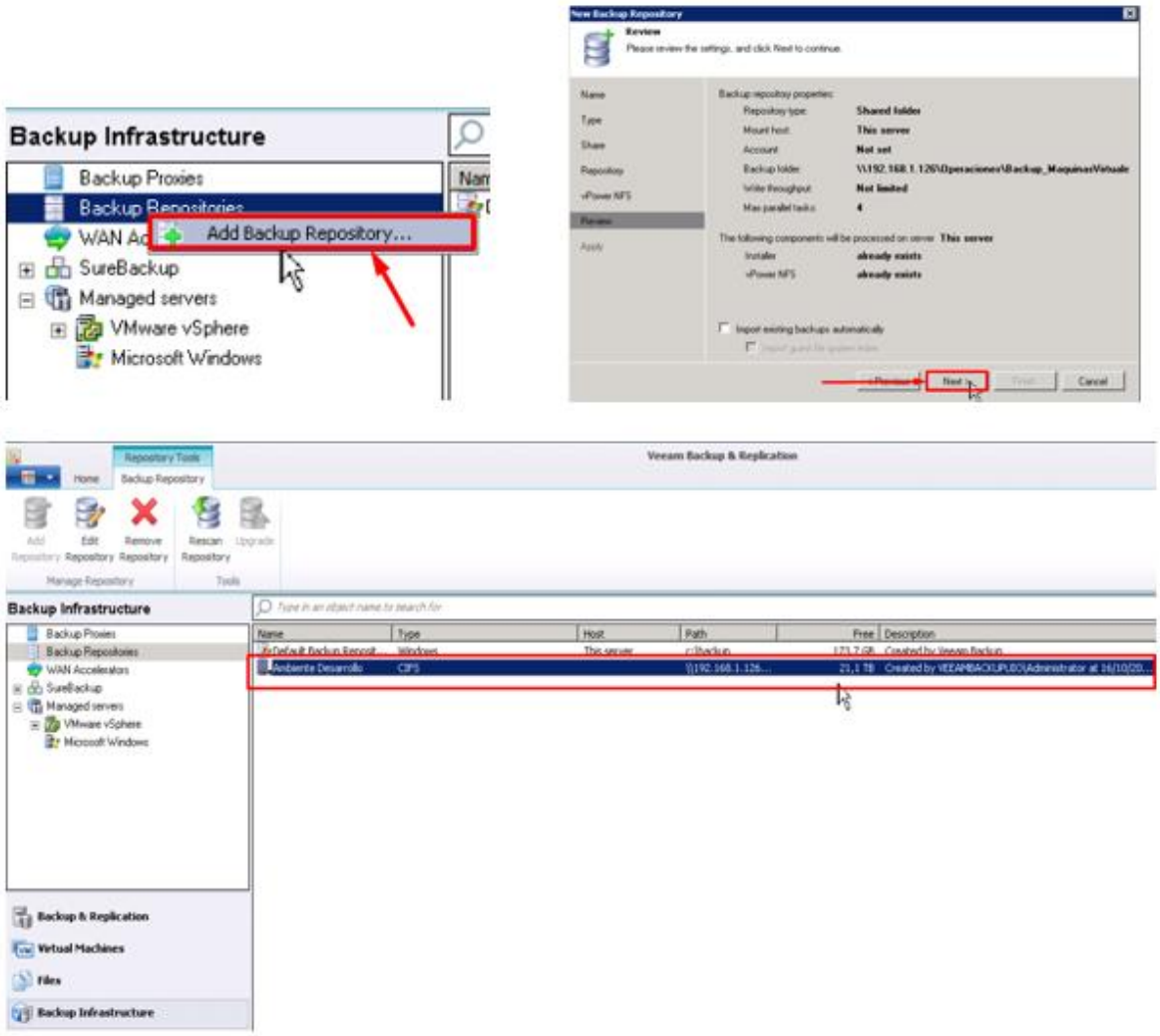


Figura 109 Creación repositorios de almacenamiento de backups

Fuente: (Autor)

- **VMWare vCenter Converter**

VMware vCenter Converter es una solución sencilla que permite automatizar el proceso de convertir una Máquina física hacía una virtual, esté corriendo bajo Windows o Linux, otros formatos de máquinas virtuales e incluso formatos de imagen de máquinas de terceros, y lo mejor, sin tiempo de indisponibilidad, es decir, se puede realizar la tarea en caliente, (ver figura 110).

Virtual Converter permite una gestión centralizada de conversiones de máquinas virtuales o físicas, así se puede gestionar desde una única consola la migración de varias máquinas al mismo tiempo, además agrega una fiabilidad máxima al realizar la copia mediante un snapshot del sistema operativo de la máquina de origen, antes de empezar a migrar.

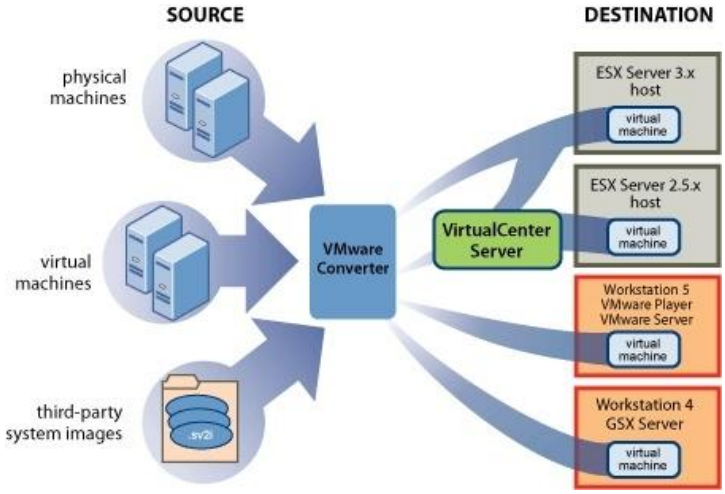


Figura 110 Flujo de trabajo Vmware Converter

Fuente: (Autor)

Para poder obtener el software debemos registrarnos en el portal de Vmware https://my.vmware.com/web/vmware/evalcenter?p=converter, con esto obtendremos el instalador y procederemos a instalar la aplicación la cual es sencilla, basta con seguir todo por defecto. Al final de la instalación se levantará una interfaz como se observa en la figura 111 en la cual configuraremos los servidores a virtualizar.

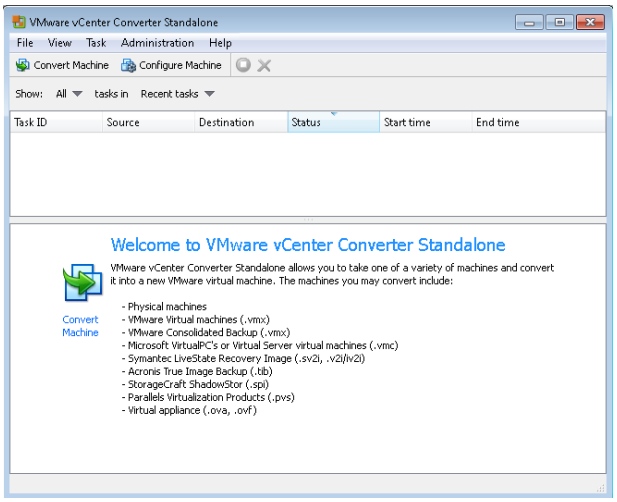


Figura 111 Interfaz de inicio Vmware Converter

Fuente: (Autor)

4.5.2. Etapa de Implementación

4.5.2.1. Fase de Prerrequisitos para implementación del Plan

4.5.2.1.1. Equipo de Recuperación Inicial

Una vez que ha ocurrido un evento o desastre la persona encargada de liderar la recuperación del departamento de TI es el Gerente de Desarrollo Digital & Tecnología, es quien convoca inicialmente al equipo mínimo del departamento para evaluar el daño ocurrido en el sitio, la comunicación debe ser de forma efectiva y oportuna ante cualquier crisis o evento adverso a la operación normal de los procesos de GEC, sean internos o externos. Una vez realizada la evaluación se procederá a decidir si es necesario comunicar a todo el departamento haciendo uso de la cadena de Comunicación.

4.5.2.1.2. Centro de reunión alternativo en caso de desastre

Dependiendo el tipo de desastre se ha definido los siguientes puntos de encuentro para reunión del equipo mínimo de TI, dados los siguientes casos.

- Si el sitio de desastre es accesible, reunirse en:
    - Matriz – Área de tecnología
    - Matriz – Sala de reuniones tercer piso
- Si el edificio es inaccesible, reunirse en.
    - Sucursal – Ed. Aragonés
- Si el desastre afecto a toda la ciudad, reunirse en.
    - Regional Guayaquil
    - Regional Cuenca

4.5.2.1.3. Acuerdos con proveedores

Se asume que el departamento de Tecnología de GEC ya tiene implementado acuerdos con proveedores para tener disponible los recursos necesarios en caso de desastre en los tiempos pre-acordados.

4.5.2.1.4. Requerimientos Tecnológicos

Los backups se encuentran trasladando fuera de la matriz del Departamento de Tecnología, mismos que serán entregados a las personas autorizadas en el momento que se requiera, o en su defecto, que sean entregados a personas de GEC con autorización de los representantes legales para realizar estas actividades.

4.5.2.2. Equipo de Continuidad de negocio

Cualquier situación (natural o provocada, propia o ajena) que amenace la imagen y ponga en riesgo la continuidad del negocio de GEC, alterando las operaciones normales, es necesario estar instruidos adecuadamente en la comunicación, para evitar que el impacto sea menor.

Para proceder con la implementación del plan de continuidad del negocio para el Departamento de Tecnología se debe definir el equipo mínimo que se encargará de la recuperación y del retorno a operaciones normales de las actividades de los usuarios.

En el Departamento de Tecnología de GEC se ha definido 11 personas en el equipo mínimo para garantizar la continuidad del negocio, (ver figura 112), adicional se definió que cada persona tenga un suplente en caso de no estar disponible el miembro principal. En este documento no se ha publicado la información de personal de los miembros del equipo mínimo, debido a que este tipo de información se lo maneja de manera confidencial y dentro de la empresa. En la cadena de comunicación debe estar registrada la información de cada miembro que la conforma.

Es necesario mantener la Cadena de comunicación de equipo mínimo siempre actualizada debido a la variabilidad de las personas en sus cargos y para tener una comunicación efectiva.

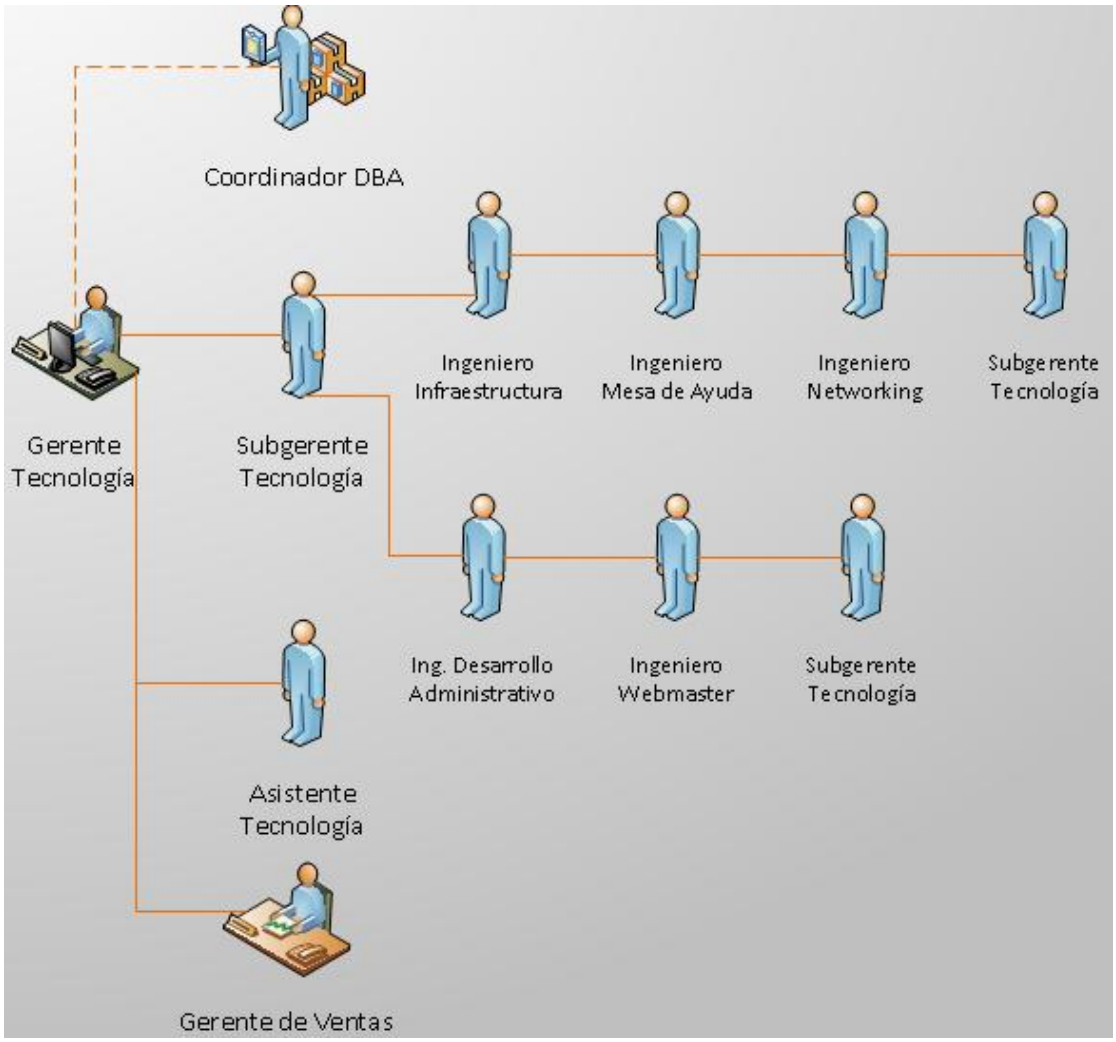


Figura 112 Equipo mínimo del Departamento de Desarrollo Digital y Tecnología

Fuente: (Autor)

4.5.2.3. Actividades para la ejecución del plan de contingencia

El plan de continuidad del negocio tiene como objetivo minimizar el impacto y el riesgo de la operación normal de GEC, el equipo mínimo deberá actuar de forma rápida y ordenada para recuperar y retornar a la normalidad las actividades del negocio, en este caso restablecer lo antes posible los recursos de computación y comunicaciones, para que los usuarios puedan operar de forma

normal, dentro de lo que dependa del Departamento de Desarrollo Digital y Tecnología.

En la Gerencia de Desarrollo Digital y Tecnología, existen dos tipos de equipos de comunicación.

- Equipo mínimo
- Cadena de comunicación.

La comunicación tiene efecto entre los integrantes de cada grupo y en el orden especificado en los documentos. La cadena la inicia el responsable y a él debe llegar la última llamada lo más pronto posible, se debe seguir los siguientes pasos una vez que se haya notificado sobre un desastre o inconveniente.

1. Proceder a llamar a la siguiente persona que se encuentra en la cadena de comunicación y pasarle el mismo mensaje recibido.
2. Si no se consigue ubicar en los siguientes 3 minutos, llamar a la persona suplente o la segunda persona en la cadena, y pasarle el mismo mensaje.
3. De la misma manera, si no contesta, seguir a las siguientes personas hasta que se contacte algún integrante de la cadena.

El mensaje que se dirá en la cadena de comunicación es semejante al que se muestra en la figura 113

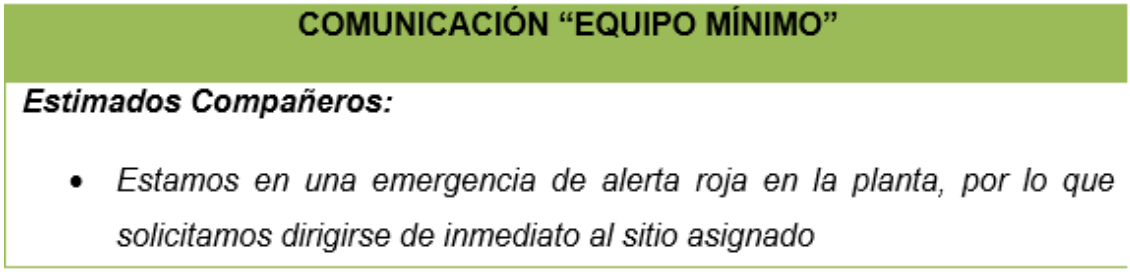


Figura 113 Mensaje de emergencia para el Equipo mínimo

Fuente: (Autor)

4.5.2.4. Asignación de Actividades

Después de sucedido el desastre, se evalúa el impacto de los daños, todos los miembros del equipo mínimo son notificados y el plan es activado. Para llevar un orden se ha definido las siguientes actividades.

1. Reunirse en el lugar asignado
2. Notificar a los proveedores acerca del daño, en caso de ser necesario
3. Acceder a la documentación del plan de continuidad del negocio
4. Si el desastre es en horas no laborables, trasladarse a la planta inmediatamente.
5. Evaluación de los daños preliminares
6. Evaluación del impacto del desastre.
7. Preparar un reporte preliminar del desastre y sus problemas.
8. Inspeccionar el sitio del desastre para evaluar detalladamente el impacto causado por la interrupción
9. Evaluar la interrupción de los procesos y daños en los recursos en general.
10. Estimar el impacto del desastre basado en los registros del plan, catalogando al desastre como bajo, medio o alto.
11. Si no afecta a los procesos críticos se debe continuar monitoreando las aplicaciones hasta mantener la estabilidad.
12. Preparar un informe detallado del problema.

Una vez analizado el desastre el equipo de Infraestructura & Operaciones revisará las opciones de recuperación disponible y decidirá la mejor opción de recuperación, en tanto que Networking analizará y gestionará con los proveedores de red para establecer a la normalidad los enlaces de datos e internet en la planta o en el área afectada según sea el caso o la necesidad.

Dentro de las operaciones diarias, es la realización de respaldos tanto de base de datos, servidores virtuales, archivos de configuración y data; el área de operaciones genera los respaldos mediante procesos batch o sistemas de

backup y son copiados en dispositivos de almacenamiento externo. El orden de recuperación de las funciones se realizará según la criticidad de los sistemas.

Una vez establecido el servicio el equipo mínimo evaluará las aplicaciones y se comunicará a los usuarios para que continúen con la operación del negocio; es importante monitorear el comportamiento de los aplicativos por un tiempo prudente con el fin de garantizar que todo vuelva a la normalidad.

4.5.3. Etapa de Gestión Operativa

En esta etapa se analiza aspectos importantes tales como la difusión y educación del plan de continuidad, poner en práctica auditoria y revisión del plan cada cierto tiempo y realizar pruebas sobre el plan.

4.5.3.1. Difusión y educación

Una vez culminado la elaboración del plan de continuidad se debe informar a todos los miembros del departamento TI con el fin de hacerles conocer las estrategias y pasos a seguir para que los sistemas vuelvan a operar con normalidad en caso de un inconveniente. La forma que se difundirá el plan de continuidad en el departamento de TI son:

- Charla de concientización para que todos se involucren y colaboren activamente en el plan de continuidad
- Publicación del plan de continuidad en un servidor compartido por toda el área
- Publicación del plan en la Intranet
- Taller de simulación para probar el plan.

Es importante que cada miembro del departamento TI conozca el plan ya que son participantes activos del plan, es por esto, que más que una difusión del plan se requiere una capacitación y que conozcan los procesos de recuperación.

4.5.3.2. Revisión y Auditoria

Es necesario hacer una revisión del plan de continuidad periódicamente con el fin de mantenerlo vigente y actualizado en las situaciones reales de la empresa. Una de las prioridades principales del Departamento TI es mantener actualizado periódicamente el plan de continuidad.

Se recomienda realizar auditorías cada 6 meses con el fin de mantener el plan eficaz y que ayuden a todos mediante una visión global a identificar las falencias encontradas.

Adicional se recomienda verificar que los backups obtenidos, se puedan restaurar y que sean almacenados fuera del sitio principal de la empresa, que documentación de red e infraestructura se encuentre actualizada y que los contratos de soporte con los proveedores se en encuentren vigentes y con todos los requerimientos necesarios.

4.5.3.3. Monitoreo y mantenimiento del plan de continuidad

Una vez finalizado el plan de continuidad se recomienda realizar pruebas al menos cada 6 meses con el fin de verificar la validez de los procedimientos. Para realizar las pruebas se debe montar un simulacro, donde se apliquen los procedimientos necesarios para la recuperación, en los simulacros se debe seguir los siguientes pasos.

1. Definir un escenario con determinadas condiciones
2. Definir fecha y hora para realizar el simulacro, previa autorización del Gerente de TI.
3. Llegada la fecha y hora, iniciar las actividades del plan, siguiendo los procedimientos anteriormente establecidos.
4. Registrar los tiempos que tomo la recuperación total del servicio afectado.
5. Registrar inconvenientes detectados durante el proceso de recuperación.

6. Una vez terminado el simulacro, se debe realizar una reunión con todos los miembros para analizar los inconvenientes encontrados e inconsistencias del plan que no se adecuan a la realidad
7. Realizarlos cambios en el plan de continuidad siempre y cuando sea necesario

4.6. Generación de políticas de respaldo.

4.6.1. Introducción y estudio del Dataprotector

HP Data Protector es un software automatizado de backups y recuperación en un solo servidor para ambientes empresariales, que proporciona protección fiable y alta accesibilidad en el crecimiento de los datos empresariales.

La estructura de Data Protector trabaja en un entorno de red que contiene un Administrador (cell manager), clientes y dispositivos de respaldo como se observa en la figura 114. El administrador tiene el software Data Protector instalado y es el punto central a partir del cual se administra la herramienta, los clientes, backups y operaciones de restauración.

HP Data Protector soporta almacenamiento en disco o almacenamiento en cinta, y es posible obtener backups en línea de los sistemas operativos Windows, Unix y Linux.

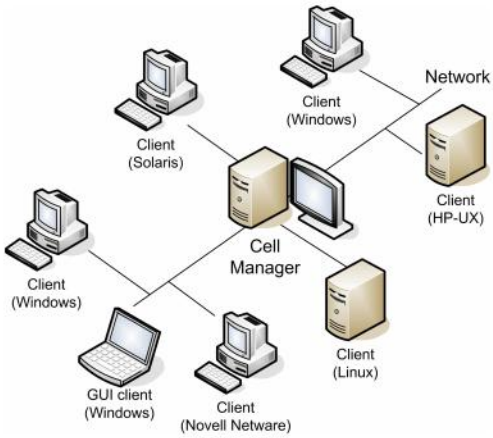


Figura 114 Entorno de red Data Protector

Fuente: (Autor)

Un backup es un proceso que crea una copia de los datos en los medios de respaldo, el cual se almacena y se mantiene para su uso futuro en caso de que se destruya o se corrompe el original. En tanto que la restauración es un proceso que recrea los datos originales desde la copia de backup, (ver figura 115).

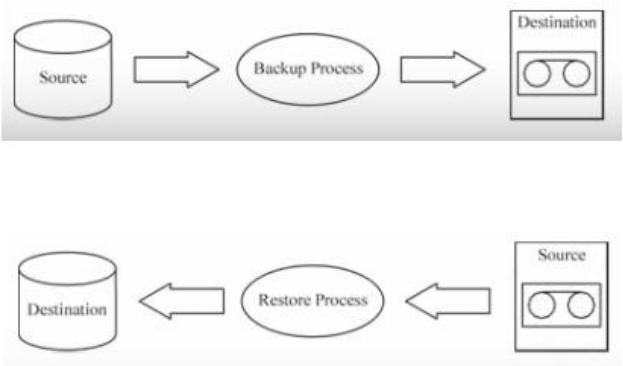


Figura 115 Proceso de Backup y Restauración

Fuente: (Autor)

Data Protector tiene una base de datos integrada llamada IDB, la cual está ubicada en el Administrador, que mantiene información sobre los datos respaldados y que medios contiene los respaldos para restaurar. Adicional el DP contiene un repositorio de agentes de software y componentes de integración de los cuales los de mayor uso y necesarios para GEC son:

- Disk Agent: Responsable de todas las acciones de lectura y escritura al disco de almacenamiento origen que realiza backups y restauraciones con el DP.
- Media Agent: Responsable de todas las acciones de lectura y escritura realizadas a los medios de respaldo por gestiones de restauración & medios del DP.
- User Interface: Proporciona interfaz gráfica de usuario e interfaz de línea de comandos.

Tipos de Backup

Hay 4 formas de configurar un backup en el sistema DP.

- **Full Backup:** Backup completo de todos los archivos y carpetas seleccionadas para respaldar de un filesystem
- **Backup Incremental:** Un backup incremental será un backup en línea solo esos archivos que tuvieron cambios desde el último full backup o incremental
- **Diferencial:** Un backup diferencial será un backup en línea solo de esos archivos que tuvieron cambios desde el último full backup
- **Full sintético**: Es una solución de backup avanzado que elimina la necesidad de ejecutar regularmente full backups. En cambio, los backups incrementales se ejecutan y posteriormente se fusionan con el full backup convirtiéndose en un nuevo full backup sintético.

En este caso se ha instalado la herramienta DP Cell Manager en un servidor Windows, y para instalar basta con ejecutar el instalador con la cuenta de administrador desde un CD o localmente. Las configuraciones de la instalación se dejan por defecto, al final de la instalación tendremos una interfaz gráfica similar al de la Figura 116 con lo cual estaremos listos para configurar clientes y backups.

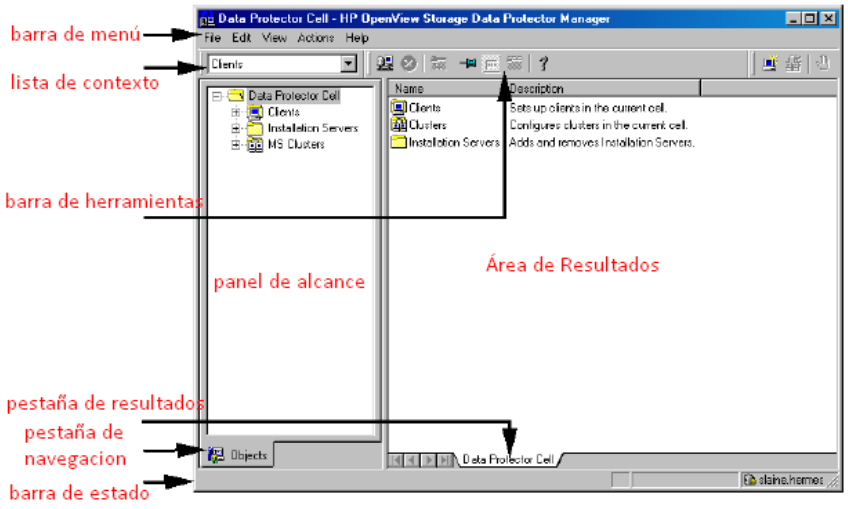


Figura 116 Interfaz gráfica de usuario

Fuente: (Autor)

4.6.2. Políticas de respaldo

4.6.2.1. Respaldos de Información GEC

Los objetivos de este punto es definir las políticas de respaldo de la información de Grupo El Comercio, la manera y frecuencia de realización, además establecer responsables y la manera de respaldar la información de Grupo El Comercio.

Responsables.

- **Subgerencia de Seguridad e Infraestructura:** Para la aprobación de solicitudes de respaldos de Grupo El Comercio y revisión de las tareas de control de respaldos.
- **Administrador de Base de Datos (DBA):** Generación de Full Backups de las bases de datos correspondientes a los aplicativos de Grupo El Comercio para ser posteriormente respaldados por el personal de Infraestructura & Operaciones.

- **Infraestructura & Operaciones:** Para la grabación en cinta, custodia y restauración de los archivos respaldados que permitan la recuperación de datos.
- **Seguridad:** Será responsable de realizar auditorías periódicas al proceso de respaldo y a la calidad de los mismos, sin olvidar las normas de seguridad de la información, teniendo presente la cadena de custodia de los mismos.
- **Coordinadores de Desarrollo:** Para las aplicaciones que sean puestas en producción los Coordinadores Desarrollo serán responsable de detallar el contenido que debe respaldarse y la frecuencia mediante un correo o documento de respaldo, esto debe incluir entre otros lo siguiente: Base de datos, Archivos de Configuración, Aplicaciones, etc.

Procedimiento

Para realizar el respaldo de información de Grupo El Comercio, se utiliza la herramienta HP Data Protector Manager. La cual utiliza cintas magnéticas como medio de almacenamiento masivo de información. Actualmente se dispone de 2 librerías para la realización de BackUps, las cuales las denominamos de la siguiente manera:

- **MSLPRODMSL4048:** Capacidad para 48 cintas: 1600GB asumiendo compresión 2:1.
- **MSLERPMSL4048:** Capacidad para 48 cintas: 3000GB asumiendo compresión 2:1

La información de grupo el comercio, se respalda bajo el siguiente esquema:

La mayoría de respaldos, son realizados en modo FULL y con frecuencia DIARIA. Existen servidores como los File_servers los cuales se realizarán un full Backup en fin de semana e incrementales de lunes a viernes debido al gran tamaño de información que se maneja en estos servidores.

Cabe recalcar que la información contable de la empresa se la realiza en Backups full de las bases de datos diariamente, la cual contienen información a partir del año 2001, que es cuando se adquirió el ERP de PeopleSoft.

Con este procedimiento La Gerencia de Desarrollo y Tecnología garantiza la disponibilidad de información contable de al menos 7 años tal como lo estipula el REGLAMENTO PARA LA APLICACIÓN DE LA LEY ORGANICA DE REGIMEN TRIBUTARIO INTERNO, Art. 34. Por políticas de la empresa no se puede compartir el listado de la documentación que se respalda, pero en el ANEXO 6 se puede observar el cronograma de los backups.

Políticas

- Los respaldos a los servidores de la empresa se los debe realizar diariamente según lo estipulado anteriormente en los procedimientos para solventar cualquier contingencia presentada.
- Se debe enviar cada 15 días los respaldos de toda la empresa a la bóveda de seguridad del banco contratado por el grupo.
- Los respaldos que regresan quincenalmente de la bóveda del banco, deben permanecer quince días más seguros en la empresa. El personal de Infraestructura & Operaciones, se encargará de custodiar estos respaldos.
- Se debe realizar una comprobación de validez de los Backups realizados mínimo una vez a la semana de un Backup realizado aleatoriamente.
- Se deben realizar respaldo anual y semestral con protección permanente de toda la información de la empresa. Estas cintas serán custodiadas por el departamento de QA y Seguridad y guardadas en la caja fuerte que se encuentra ubicada en el interior del Datacenter, actualmente tiene acceso el Gerente de Tecnología.
- El departamento de QA y Seguridad se encargará de revisar y llenar la hoja de recepción de cintas entregadas por el área de Operaciones.

- El área de Operaciones se encargará de llenar y hacer firmar el documento de entrega de cintas al personal del departamento QA y Seguridad.
- El área de Operaciones deberá llevar una bitácora de control de los backups efectuados, estas son bitácora de errores, entrega de respaldos, chequeo de respaldos y pruebas de restore; dichas plantillas se pueden observar en el ANEXO 7.

4.6.2.2. Restauración de Información perdida

Los objetivos de este punto son definir las políticas de restauración de la información del Grupo el Comercio en caso de existir alguna contingencia, además de establecer los responsables y la manera de restaurar la información del Grupo el Comercio.

Responsables

- **Subgerencia de Producción y Soporte Técnico:** Se encargará de la revisión de las tareas de restauración realizados por el personal de Infraestructura & Operaciones.
- **Administrador de Bases de Datos (DBA):** En el caso de que la información perdida o dañada tratase de una Base de Datos, se debe contar con la presencia del DBA para la restauración de la misma de un Backup proporcionado por Infraestructura & Operaciones.
- **Infraestructura & Operaciones:** Serán los responsables directos para la restauración de los archivos respaldados en cinta según los procedimientos de respaldos de información del Grupo El Comercio.
- **Seguridad:** Será responsable de haber realizado junto con el personal de Infraestructura & Operaciones un proceso de calidad de los Backups para así poder asegurar la validez de los mismos.

  Si se da el caso de que la información perdida está en una cinta de la bóveda del banco, el área de seguridad es la encargada de entregar la

misma al personal de Infraestructura & Operaciones para proceder a realizar el restore de los datos.

- **Mesa de ayuda:** En caso de que algún usuario necesite algún archivo perdido, el personal de soporte será encargado de hacer llenar la solicitud de Restauración en la cual se especifica el archivo a restaurar, la fecha de pérdida y la autorización respectiva del jefe superior del área al que pertenece

Procedimiento

Para realizar la restauración de información, se debe llenar la solicitud de restauración, misma que, será entregada al usuario solicitante por el personal de Mesa de Ayuda, en esta se debe determinar exactamente la ubicación donde se encontraba la información y la fecha en la cual se extravió o daño la misma.

Una vez ubicado el archivo, se procederá a la restauración del mismo desde la herramienta HP Data Protector Manager en la ubicación original o una ubicación distinta a la cual se encontraba el archivo original.

Se debe tener en cuenta que el tiempo para la restauración depende del tamaño del archivo. Y este puede ser restaurado según la protección establecida (número de Días) en los procedimientos de respaldos de información del GEC.

Como contingencia extra, se puede restaurar la información de hace un mes (15 días de la bóveda del banco y 15 días a cargo de Infraestructura). Y de los respaldos anuales los cuales poseen protección permanente.

Políticas

- Se debe realizar una comprobación de validez de los BackUps realizados mínimos una vez a la semana de un Backup realizado aleatoriamente.

- EL personal de operaciones es la encargada de restaurar la información y entregarla a la persona solicitante, especialista de una aplicación o a un DBA en el caso de ser un BackUp de una base de datos para que se proceda con la restauración de la información.

De acuerdo a las políticas internas de Grupo El Comercio, la información respaldada será de uso exclusivo dentro de la compañía y para los fines justificados por quien lo solicita.

4.6.3. Configuración del Data Protector Manager

4.6.3.1. Instalación User Interface y creación de usuario de conexión.

Para la instalación de un cliente que administrará los backups, se debe ingresar a Data Protector y seleccionamos el menú “Clients”, con clic derecho escogemos la opción de agregar clientes “Add Clients” e ingresamos la IP o nombre del equipo donde queremos instalar la herramienta. Adicional e importante es escoger la opción “User Interface” con lo cual se instalará por red la interfaz del cliente en el equipo solicitado, previamente ingresando las credenciales de un usuario que tenga privilegios de administrador, (ver figura 117).

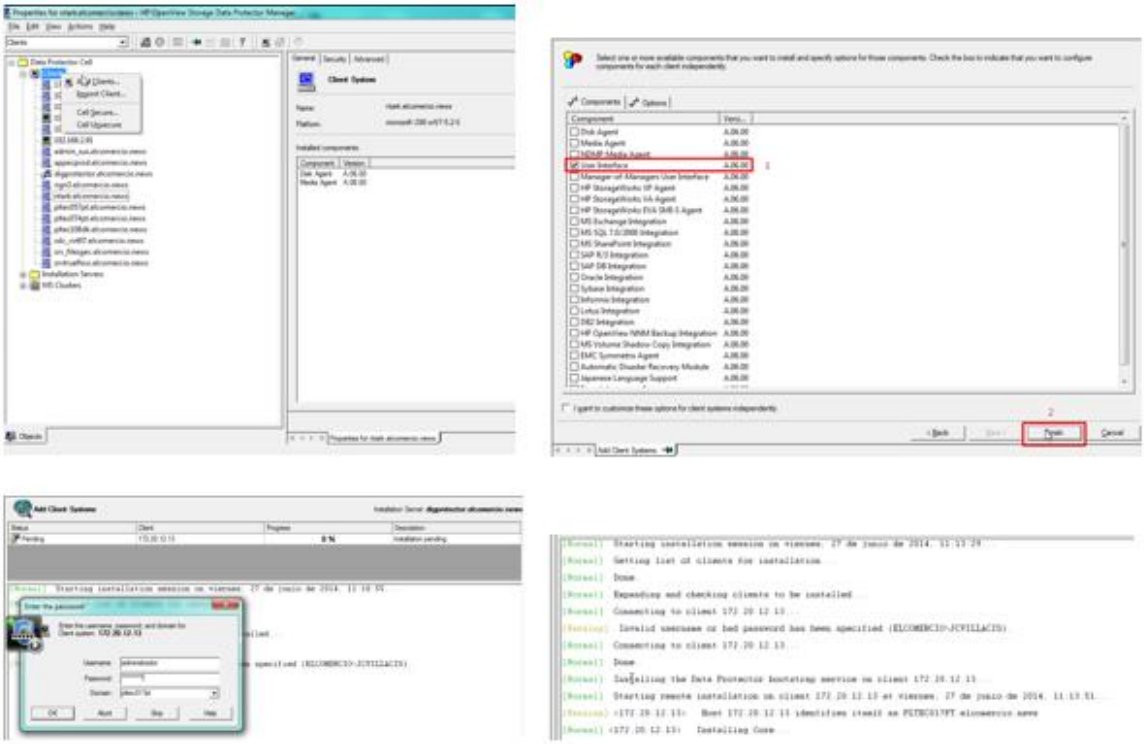


Figura 117 Instalación Cliente de Administración DP

Fuente: (Autor)

Una vez instalado la herramienta en el computador del cliente se crea su usuario de conexión, escogiendo la opción “clients” y dando clic derecho creamos un nuevo usuario de administración, ingresando la cuenta de usuario del dominio o una cuenta local del computador, con esto se podrá conectar el cliente desde el computador hacia la consola de administración del Data Protector, (ver figura 118).

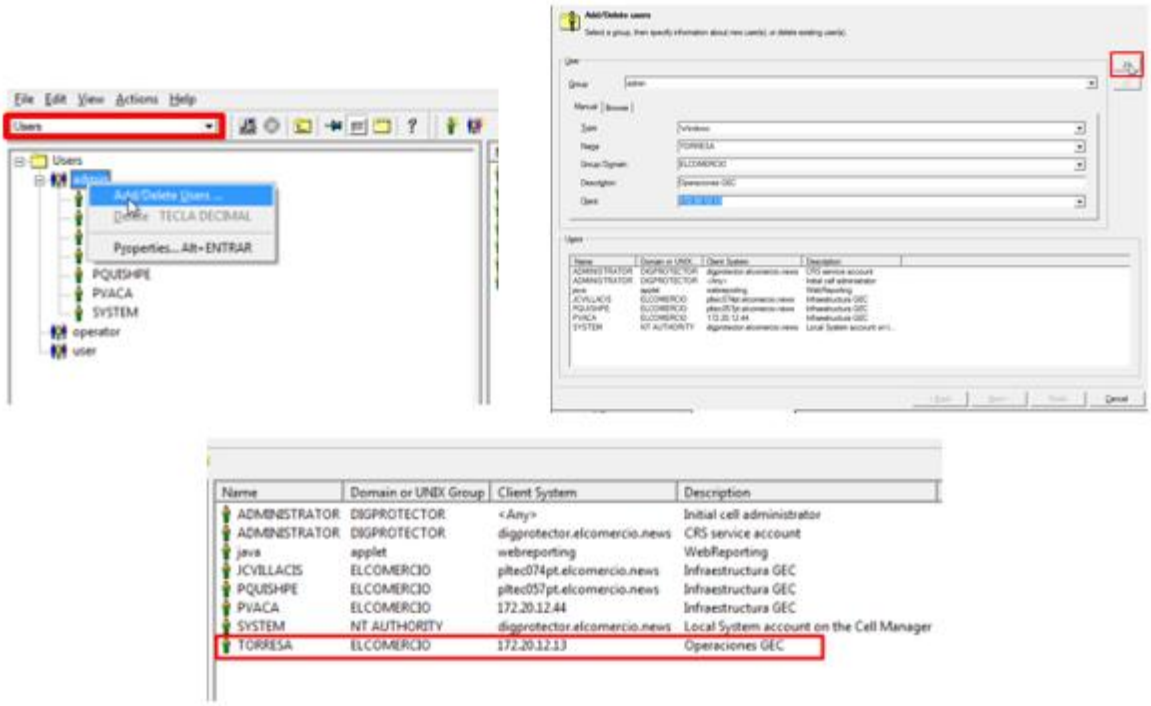


Figura 118 Creación de usuario de conexión al DP

Fuente: (Autor)

4.6.3.2. Configuración de Backups.

Para configurar un backup debemos seguir 3 pasos.

1. Ingresar el servidor como cliente

Para ingresar el servidor a respaldar, se sigue los pasos mencionados anteriormente para ingresar un cliente, solo que en este caso envés de escoger la opción “User Interface” escogemos “Disk Agent” o “Media Agent” el cuál nos permitirá sacar el backup por LAN o SAN respectivamente, (ver figura119).

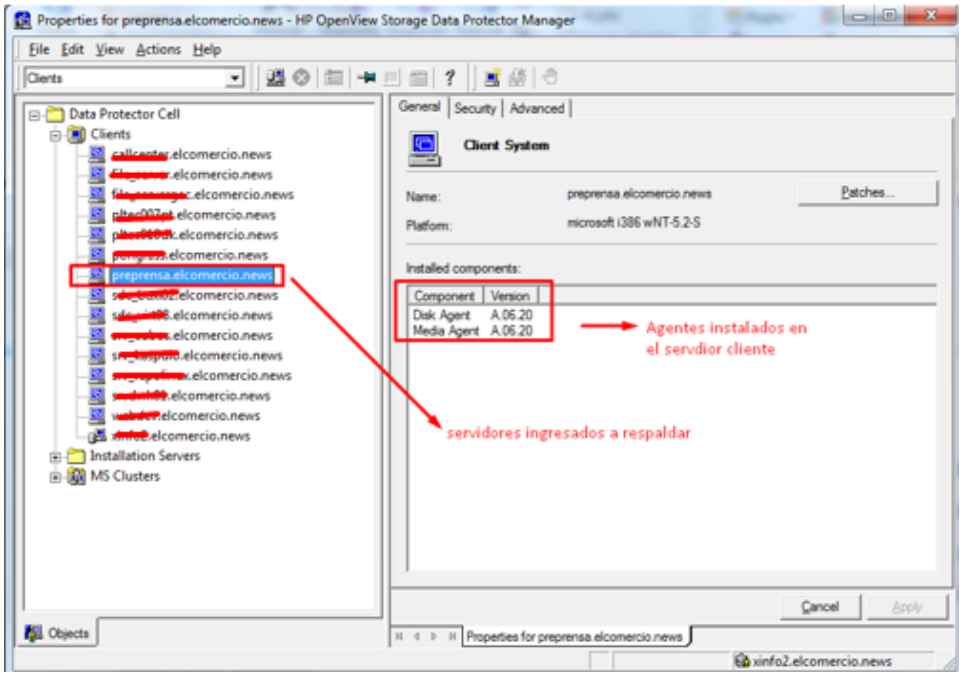


Figura 119 Ingreso de servidores al DP

Fuente: (Autor)

2. Crear un pool de cintas para guardar la información

Una vez ingresado el servidor, creamos un pool de cintas donde asignamos las que serán usadas por la tarea de backup. Para crear el pool se debe escoger la opción “Devices & media”, seguido hacer clic en “Media” y clic derecho en “Pools” y escoger la opción “Add media pool”; se debe ingresar un nombre, de preferencia se ha colocado el nombre del servidor que utilizará el pool y escogemos el tipo de dispositivo a utilizar, en este caso las cintas son de tipo LTO-Ultrium, (ver figura 120).

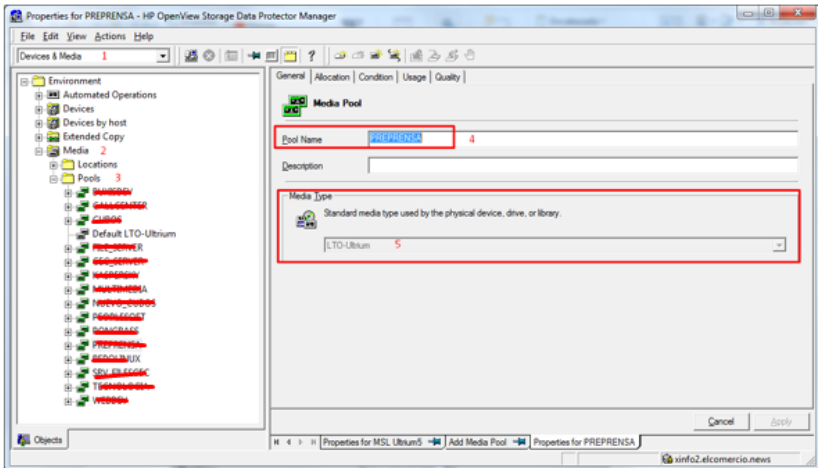


Figura 120 Creación de Pool de cintas

Fuente: (Autor)

Finalmente se asigna cintas al pool, las cuales fueron ingresadas en la librería con anterioridad. Para asignar las cintas se debe escoger la opción “Devices & Media” y dirigirnos a “Slots”, aquí se podrá observar todas las cintas que se encuentra en la librería, escogemos una por una y damos clic derecho para formatearla y asignarla al pool que deseemos, (ver figura 121).

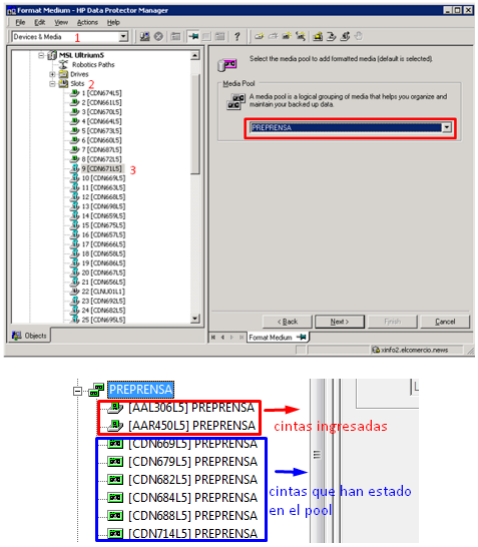


Figura 121 Asignación de cintas al Pool

Fuente: (Autor)

3. Escoger la información a respaldar y configurar la tarea de respaldo.

En esta sección se detallará paso a paso para configurar un Full backup el fin de semana e incrementales de lunes a viernes.

- Escogemos la opción “Backup” y hacemos clic derecho en “Filesystem” para agregar un nuevo backup. En la parte derecha se podrá observar los servidores que se encuentran conectados al DP, aquí se escogerá la información que se desea respaldar como se observa en la figura 122.

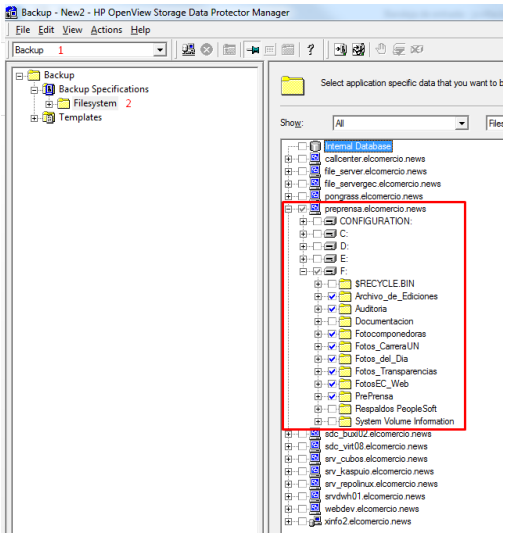


Figura 122 Configuración de archivos a respaldar

Fuente: (Autor)

- Seguido escogemos los dispositivos o drives por dónde sacará los respaldos, llámese drives a los brazos de la librería que toma la cinta para respaldar; en cada “drive” configuramos que media pool y que caminó usará para realizar el respaldo, en este caso como el servidor está conectado a la SAN escogemos el camino de fibra del servidor, (ver figura 123).

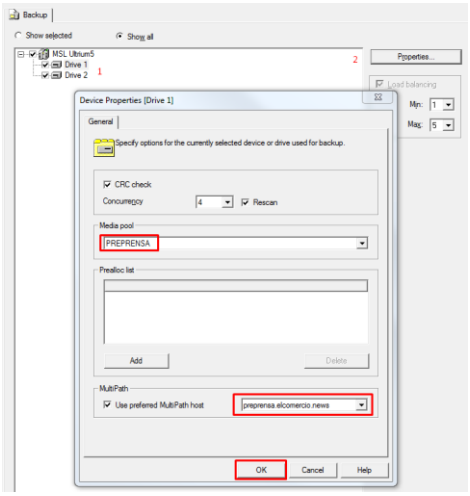


Figura 123 Selección de dispositivos que usará para el backup

Fuente: (Autor)

- Seleccionar el tiempo de protección de los backups en la cinta, adicional para fines de monitoreo se ha seleccionado que en cada tarea se muestre la información del trabajo y los archivos bloqueados durante el backup, (ver figura 124).

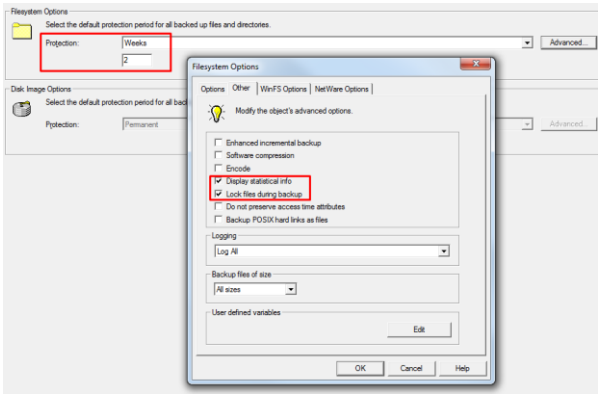


Figura 124 Configuración Opciones adicionales del backup

Fuente: (Autor)

- Finalmente configuramos el horario que se desea que saque los backups, en este caso se ha configurado para que la información del servidor

Preprensa saque Full Backups los días Domingos y de lunes a viernes backups incrementales como se observa en la figura 125.

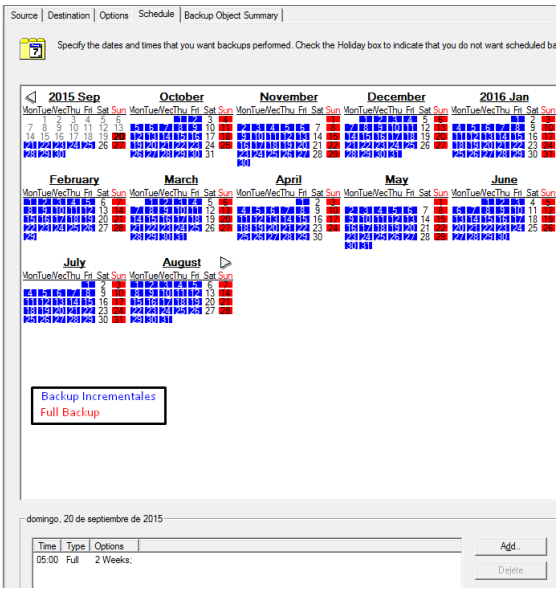


Figura 125 Calendarización del Backup

Fuente: (Autor)

4.6.4. Pruebas de Backup

Para una mejor visualización y control de las tareas de backup se puede configurar notificaciones por correo electrónico, así, se podrá observar si una backup se realizó con éxito o erróneo.

Para configurar notificaciones de cualquier tipo se dirige a la opción de “Reporting”, en este caso se configuró un reporte que envíe por correo con los detalles de la tarea como se muestra en la figura 126.

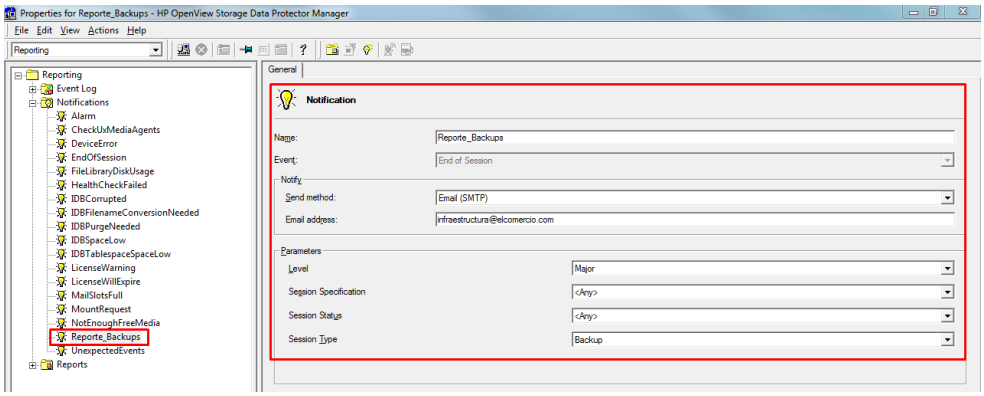


Figura 126 Configuración notificación tareas de Backup

Fuente: (Autor)

Una vez configurado las tareas de backup, estas se realizarán según lo programado, en este caso se mostrará los resultados del backup del servidor “Preprensa”, el cual fue exitoso tanto el full backup como los incrementales. A continuación, en las figuras 127 y 128 se puede observar los resultados mostrados en la consola, y en las figuras 129, 130 las notificaciones que llegaron por correo

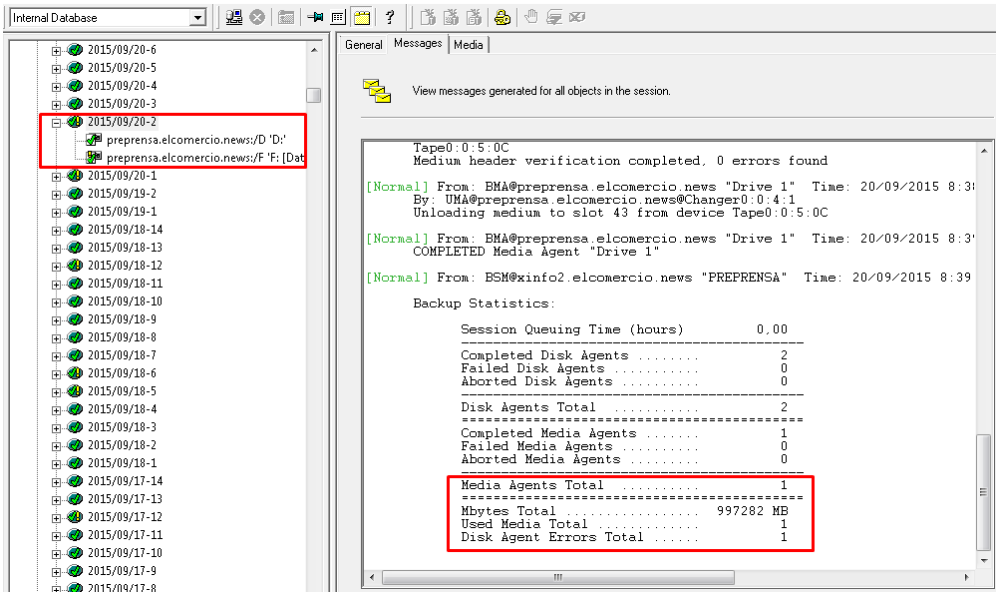


Figura 127 Resultados Full Backup

Fuente: (Autor)

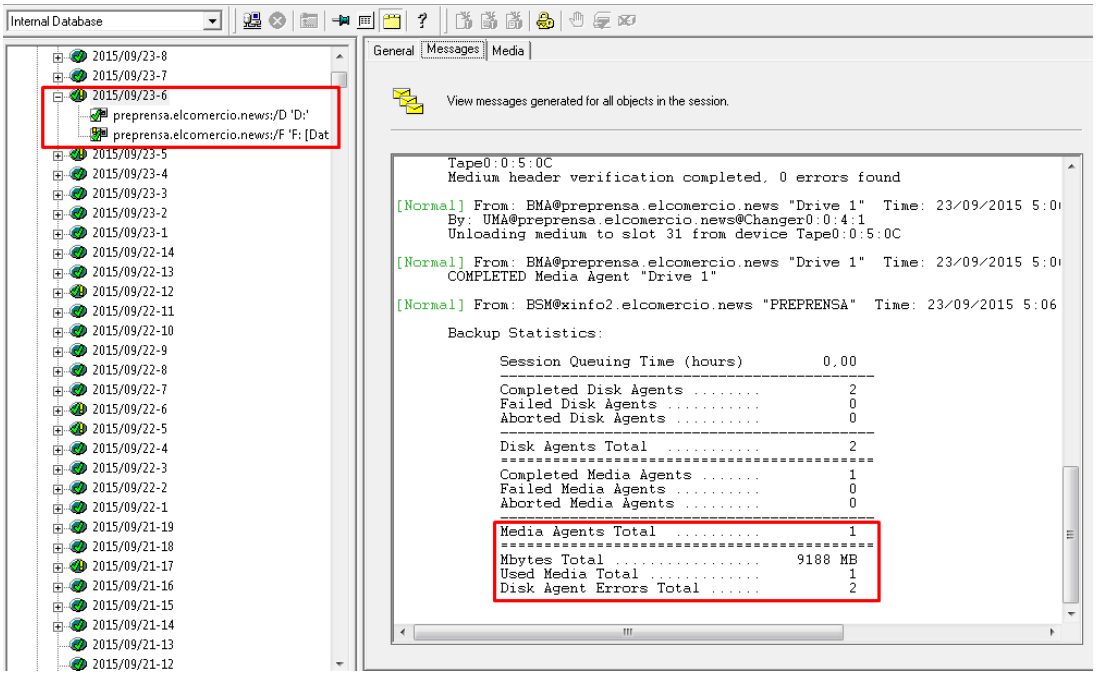


Figura 128 Resultados Backup incrmental

Fuente: (Autor)

De: Data Protector Notification [mailto:DataProtectorGEC@elcomercio.com]
Enviado el: domingo, 20 de septiembre de 2015 8:39
Para: Infraestructura <Infraestructura@elcomercio.com>
Asunto: End Of Session Report (PREPRENSA)

End Of Session Report

Cell Manager: xinfo2.elcomercio.news
Creation Date: 9/20/2015 8:39:10 AM

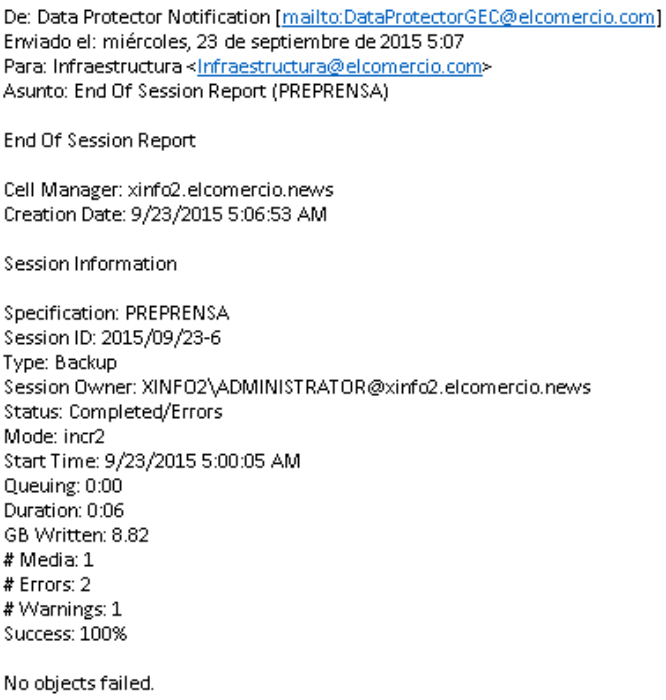
Session Information

Specification: PREPRENSA
Session ID: 2015/09/20-2
Type: Backup
Session Owner: XINFO2\ADMINISTRATOR@xinfo2.elcomercio.news
Status: Completed/Errors
Mode: full
Start Time: 9/20/2015 5:00:05 AM
Queuing: 0:00
Duration: 3:39
GB Written: 967.89
Media: 1
Errors: 1
Warnings: 4
Success: 100%

No objects failed.

Figura 129 Notificación por correo de un Full Backup

Fuente: (Autor)



De: Data Protector Notification [mailto:DataProtectorGEC@elcomercio.com]
Enviado el: miércoles, 23 de septiembre de 2015 5:07
Para: Infraestructura <Infraestructura@elcomercio.com>
Asunto: End Of Session Report (PREPRENSA)

End Of Session Report

Cell Manager: xinfo2.elcomercio.news
Creation Date: 9/23/2015 5:06:53 AM

Session Information

Specification: PREPRENSA
Session ID: 2015/09/23-6
Type: Backup
Session Owner: XINFO2\ADMINISTRATOR@xinfo2.elcomercio.news
Status: Completed/Errors
Mode: incr2
Start Time: 9/23/2015 5:00:05 AM
Queuing: 0:00
Duration: 0:06
GB Written: 8.82
Media: 1
Errors: 2
Warnings: 1
Success: 100%

No objects failed.

Figura 130 Notificación por correo de un Backup Incremental

Fuente: (Autor)

Como se observa en las figuras el full Backup se demora más tiempo que un incremental ya que el full saca un backup completo de toda la información seleccionada en la tarea, aproximadamente 1 TB; mientras que el incremental saca únicamente los archivos que tuvieron cambios o nuevos archivos creados en las carpetas seleccionadas, en este caso respaldó 8 GB aproximadamente.

4.6.5. Pruebas de Restore

Si un archivo no puede ser encontrado en el servidor o, por error, fue modificado o eliminado, puede ser restaurado a partir de un backup.Para la prueba de restauración se ha tomado un caso real, en el que el usuario solicitante no encuentra la carpeta llama “Publicidad”, quien indica que fue eliminada por error. Para proceder con la restauración se debe seguir el flujo indicado en el apartado 4.5.2.6, con lo cual se solicita al usuario llenar el formulario de restauración similar al de la figura 131.

GRUPO EL COMERCIO

SOLICITUD DE RESTAURACIÓN DE DATOS

Datos Generales

Usuario Solicitante: Gabriela Valladares.
Gerencia / Departamento: Dep. Financiero. Fecha: 7-04-2015
Ext. Telefónica 3149
e-mail: gfvalladares@elcomercio.com

Restauración de Datos

Servidor donde se encontraban los datos: Administración de ventas.

Path de los datos a recuperar:

Nombre del (los) archivo (os) a restaurar: Carpeta Publicidad en servidor Administración de ventas

Fecha en la que se perdió los datos: 7-04-2015.

Jefe de Área o departamento que aprueba el trabajo: Sofía Morales.

Firma:

Informe Técnico

Responsable: Juan Carlos Villacís
Restauración: ◉ SI ○ NO
Descripción: Se restauró lo solicitado

Notificación al Usuario: Gabriela Valladares Fecha: 07/04/2015

Observaciones

07/04/2015 — Solicitante Fecha: — Subgerencia Tecnología — Restaurado Por: — 07/04/2015 Fecha:
10 ABR 2015

Figura 131: Formulario de restauración llenado por usuario

Fuente: (Autor)

Una vez aprobado el formulario se realiza los siguientes pasos para restaurar los archivos.

1. Se ingresa a la consola de administración DP y escoger la opción Restore, aquí podemos observar todos los trabajos que se ha realizado, y se debe escoger la tarea a la fecha que necesita el archivo. Una vez escogida la tarea buscamos y seleccionamos los archivos que se desea restaurar, (ver figura 132).

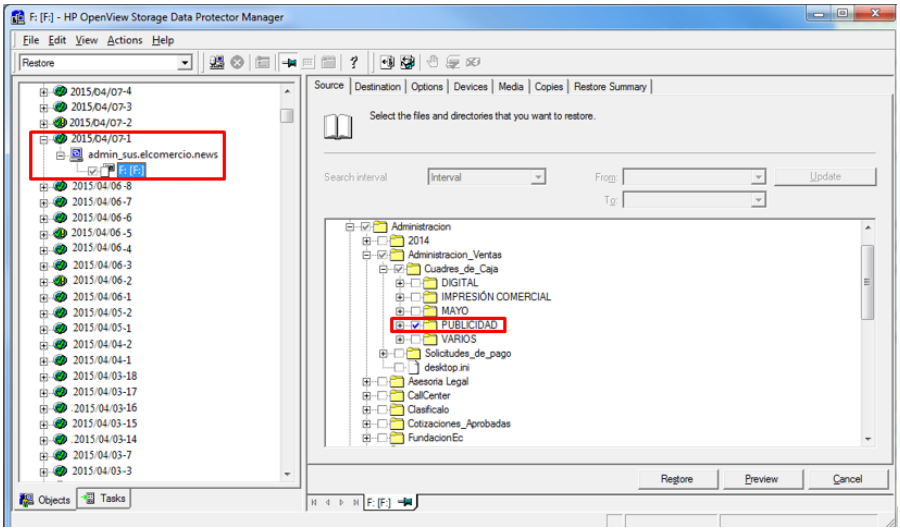


Figura 132 Selección de archivos a restaurar

Fuente: (Autor)

4.7. Roles y Responsabilidades

Para el proceso de recuperación ante un desastre se ha definido los siguientes roles: el equipo del plan de continuidad, los miembros de TI, los usuarios y proveedores.

4.7.1. Equipo del Plan de continuidad

Las principales responsabilidades del equipo de continuidad son:

- Asegurar la recuperación de las actividades en el menor tiempo posible.

- Asegurar que los datos recuperados sean consistentes
- Proteger los recursos asignados para la recuperación.
- Informar a los miembros de la empresa acerca de la situación de recuperación y avances.
- Tomar en cuenta eficacia para la recuperación y optimización de costos de la recuperación.
- Verificar el correcto funcionamiento de los sistemas, aplicaciones, recursos y consistencia de datos una vez que se haya retomado las operaciones.
- Realizar simulacros y pruebas periódicamente del plan para mantenerlo vigente.
- Registrar acuerdos con proveedores para tener un soporte 24x7

4.7.2. Miembros de TI

Generalmente la mayoría de los miembros de TI participan como miembros del plan de continuidad, los que no participan tienen las siguientes responsabilidades.

- Revisar el plan de continuidad para apoyar en las actividades en caso de desastre.
- Colaborar activamente en la elaboración del plan cuando sea necesario.
- Colaborar en las actividades de recuperación, como configuraciones, instalaciones, etc.

4.7.3. Usuarios de la Empresa

Las principales responsabilidades de los usuarios de la empresa son.

- Colaborar en lo que sea posible en la recuperación del plan de continuidad.

- Estar disponibles para realizar pruebas una vez recuperado los servicios.
- Tener en cuenta que el equipo del plan de continuidad se encargará de recuperar los recursos que soporta TI al negocio, mas no de la recuperación del negocio.

4.7.4. Proveedores

Las principales responsabilidades de los proveedores son:

- Cumplir con los acuerdos realizados previamente acerca del soporte, los equipos y tiempo de respuesta.
- Proporcionar equipos de alta calidad que el personal de la empresa ha solicitado
- Disponibilidad de suministrar hardware en caso de fallas de los equipos o componentes.

4.8. Beneficios y posibles inconvenientes.

4.8.1. Beneficios de implementar un plan de continuidad

- Garantizar la continuidad de los servicios sin que el negocio se vea afectado significativamente por un evento o desastre.
- Evitar pérdidas mayores en caso de ocurrir un desastre.
- Protección de la información ante un desastre, ya que es el activo más importante de na empresa.
- Reducir y mitigar los riesgos que pueden afectar al negocio.
- Reducir las pérdidas por interrupción de los procesos ante un desastre
- Aseguramiento de los procedimientos de obtención de backups de manera periódica

- Mantener la documentación actualizada en caso de que las personas responsables no estén disponibles.
- Identificar las debilidades que tiene el departamento de TI en los servicios que proporciona el negocio.
- Establece el plan de acción a corto, mediano y largo plazo, para darle continuidad al negocio.

4.8.2. Posibles problemas al implementar el plan de continuidad.

- Cumplimiento de procedimientos burocráticos como firmas de acuerdos entre los usuarios, el equipo de tecnología y la gerencia, alargando la gestión del plan de continuidad.
- Miembros del departamento de TI no tengan el suficiente conocimiento de los procedimientos de servicio TI.
- Falta de personal para asumir responsabilidades para implementar el plan de continuidad.
- Si han sido bien definidos los objetivos del plan de continuidad entre todo el personal correspondiente.
- Plantearse objetivos en el plan de continuidad inalcanzables, como tiempo tiempos de recuperación muy cortos.
- Que tanto los miembros de TI como los usuarios de la empresa no estén conscientes de la importancia que tiene el plan de continuidad para la empresa.

CAPITULO V

PRUEBAS DE FUNCIONAMIENTO DEL NUEVO EQUIPO Y EVALUACION DEL PLAN DE CONTINGENCIA PROPUESTO.

5.1. Monitoreo del Rendimiento del nuevo equipo.

Como se detalló en este proyecto, durante varios meses el servidor Preprensa presentaba inconvenientes en la respuesta hacia los usuarios, por lo que se tuvo la necesidad de realizar un cambio con el fin de garantizar la información y el servicio en un 99,9%.

El servidor es usado por personal de Redacción, Diseño Editorial y Comercial, Impresión Comercial, Tecnología, Pre-prensa y Post-prensa, los cuales constantemente notificaban a la Mesa de Ayuda mediante tickets de soporte que tenían inconvenientes con el servidor ya sea por espacio, lentitud o pérdida del servicio, (ver figura 133 y 134).

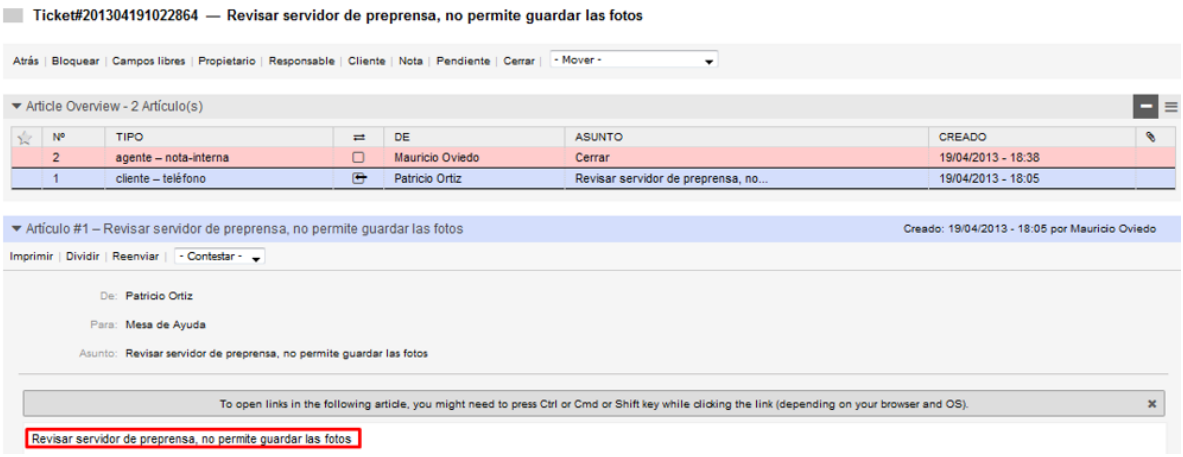


Figura 133 Ticket de soporte por espacio en disco en el servidor preprensa

Fuente: (Autor)

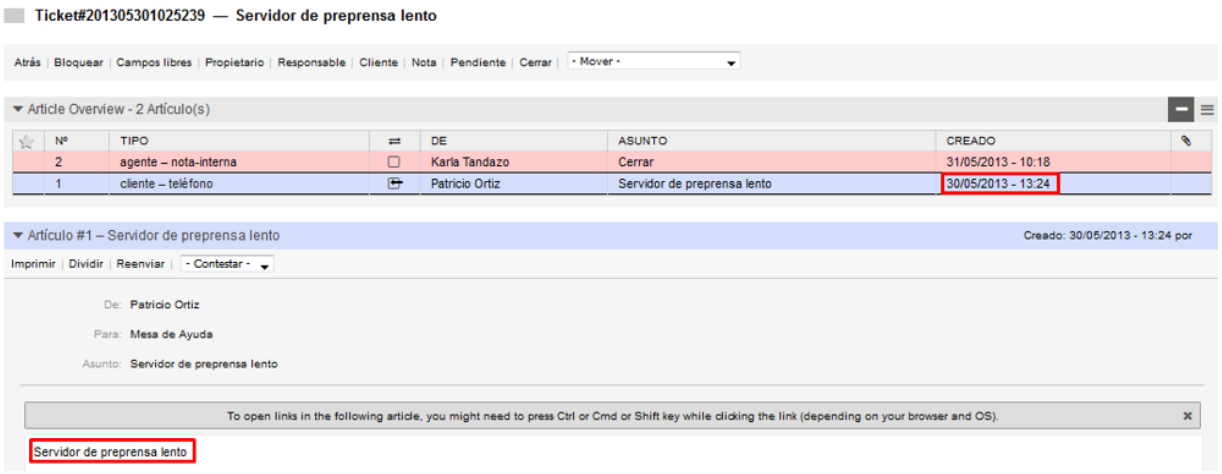


Figura 134 Ticket de soporte por lentitud del servidor Preprensa

Fuente: (Autor)

El servidor Proliant DL380 G4 tenía un espacio máximo de 600 GB el cual estaba usado un 99%, además de la saturación de los recursos como son la memoria y el procesador en las horas pico, hacía que el trabajo que desempeñan los usuarios sea inestable y tedioso, el consumo de memoria llegó a oscilar entre 70 % y 100 %.

Con la instalación del nuevo servidor y el manejo de cuotas se ha mejorado notablemente el desempeño del trabajo y la administración ordenada del file_server; además de reducir la apertura de tickets hacia la mesa de ayuda.

Para monitorear el rendimiento del servidor se hizo uso de la herramienta WhatsUp Gold, es así, que se ha tomado una muestra desde el 1 al 31 de agosto del 2015 del comportamiento del servidor en cuanto a memoria, CPU y espacio en disco, con lo cual se ha obtenido los resultaos esperados.

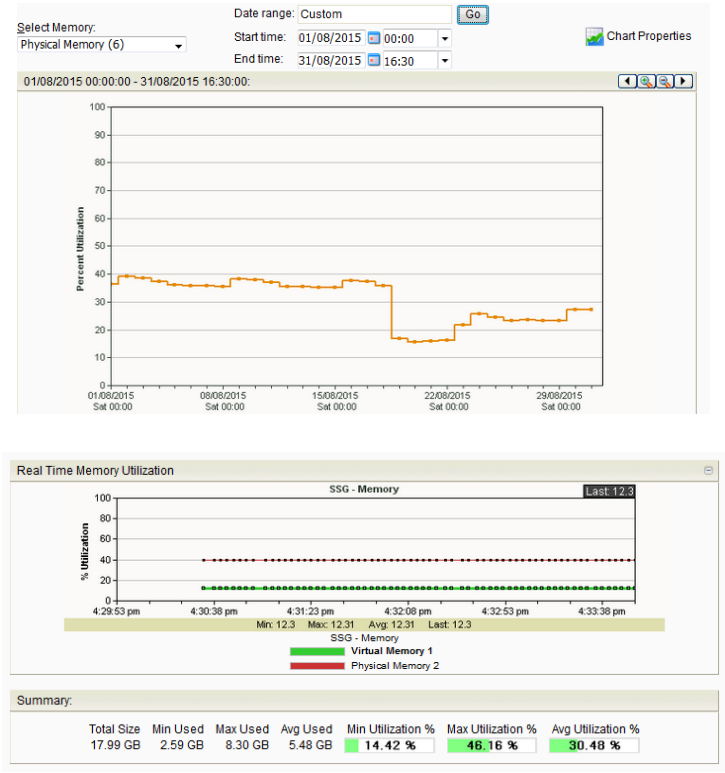


Figura 135 Uso de memoria del nuevo servidor

Fuente: (Autor)

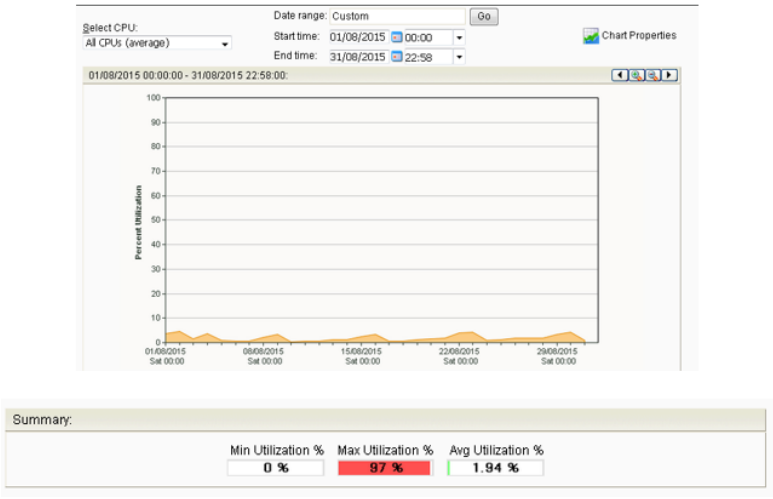


Figura 136 Uso de CPU del nuevo servidor X1800

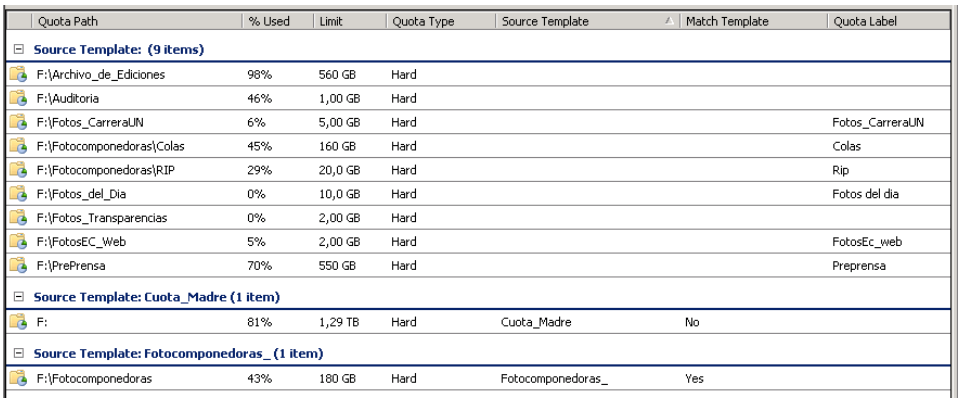
Fuente: (Autor)

En las figuras 135 y 136 se puede observar que el uso de memoria del servidor oscila entre 10% y 45 %, y el consumo de procesador llega a un 2 %; con el cambio de equipo y la actualización del sistema operativo podemos observar que el servidor se encuentra trabajando de forma óptima sin tener mucha carga y abasteciendo las necesidades de los usuarios. En un servidor y cualquier ordenador es importante la memoria y el procesamiento ya que, al saturarse estos componentes, se verá afectado el rendimiento del equipo.

En cuanto a almacenamiento, podemos observar en la figura 137 que ha crecido la información al doble aproximadamente, pero gracias a la administración de cuotas ha sido posible controlar este crecimiento y así solicitar a los usuarios revisar sus carpetas si no contienen información basura cuando estas lleguen a usar el 100% de la cuota asignada, caso contrario se le podrá incrementar su valor, algo que no se podía realizar en el antiguo servidor. Aun así, observamos que ya se encuentra usado un 82% del disco F, por lo que pensando en el crecimiento de la información se ha configurado un nuevo disco (ver figura 139) para poder cumplir con las necesidades que se presenten a futuro.

Figura 137 Uso de almacenamiento del nuevo servidor X1800

Fuente: (Autor)



Quota Path	% Used	Limit	Quota Type	Source Template	Match Template	Quota Label
Source Template: (9 items)						
F:\Archivo_de_Ediciones	98%	560 GB	Hard			
F:\Auditoria	46%	1,00 GB	Hard			
F:\Fotos_CarreraUN	6%	5,00 GB	Hard			Fotos_CarreraUN
F:\Fotocomponedoras\Colas	45%	160 GB	Hard			Colas
F:\Fotocomponedoras\RIP	29%	20,0 GB	Hard			Rip
F:\Fotos_del_Dia	0%	10,0 GB	Hard			Fotos del dia
F:\Fotos_Transparencias	0%	2,00 GB	Hard			
F:\FotosEC_Web	5%	2,00 GB	Hard			FotosEc_web
F:\PrePrensa	70%	550 GB	Hard			Preprensa
Source Template: Cuota_Madre (1 item)						
F:	81%	1,29 TB	Hard	Cuota_Madre	No	
Source Template: Fotocomponedoras_ (1 item)						
F:\Fotocomponedoras	43%	180 GB	Hard	Fotocomponedoras_	Yes	

Figura 138 Administración de cuotas

Fuente: (Autor)

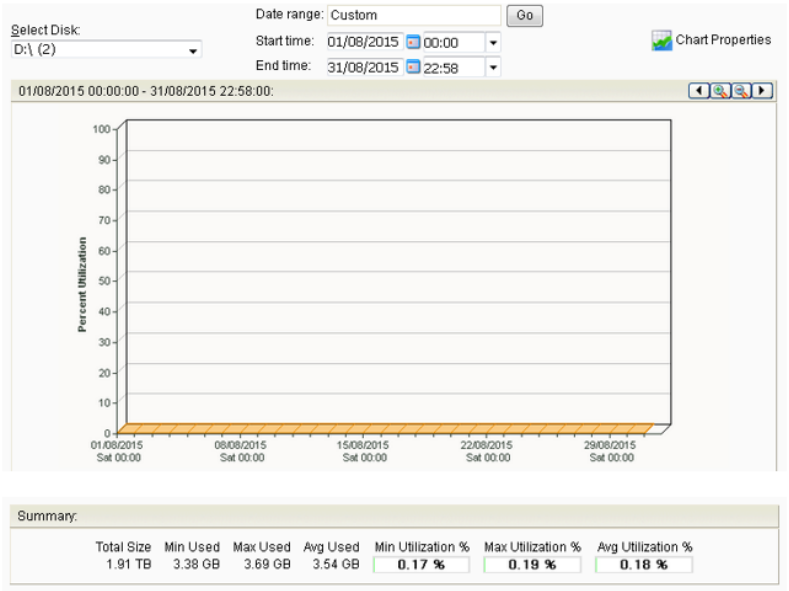


Figura 139 Almacenamiento futuro del servidor Preprensa

Fuente: (Autor)

Finalmente, con la figura 140 se indica que el servidor Preprensa en este año ha tenido una indisponibilidad del 0,2 %, esto debido al mantenimiento de la Infraestructura, mantenimientos eléctricos, configuración de agentes de

monitoreo, etc; todos estos eventos sin afectar al usuario final ya que se realizaba con una ventana de mantenimiento en horarios no laborables.

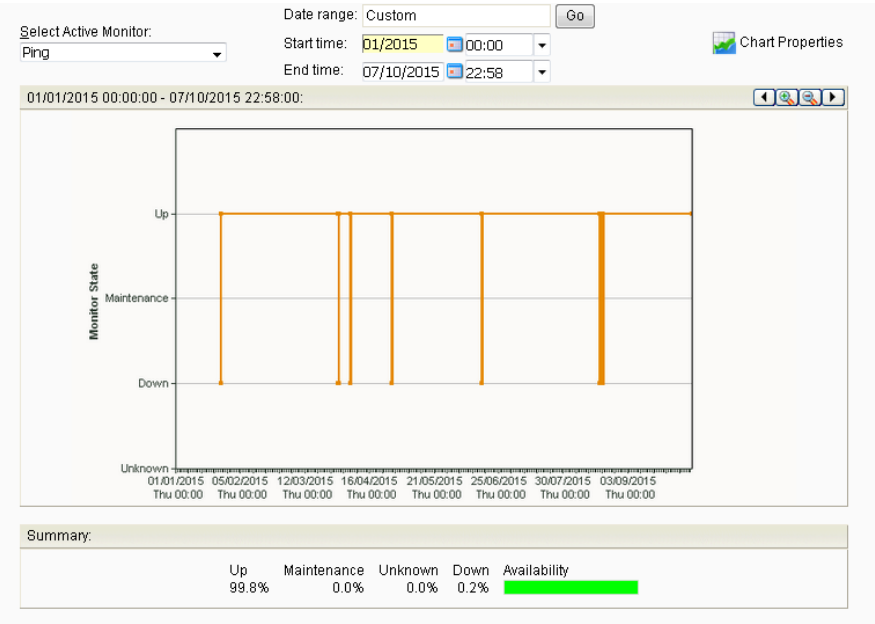


Figura 140 Uptime del servidor Preprensa en el año

Fuente: (Autor)

5.2. Verificación de afectación en el servicio para los usuarios con el cambio mediante las incidencias generadas hacia la mesa de ayuda.

El cambio de servidor fue exitoso ya que fue transparente para el usuario final, no existieron problemas de conexión, ni problemas con los permisos de seguridad. Hacia la mesa de ayuda no se generaron tickets de soporte que fueran causados por la migración. En conclusión, el haber llevado un orden y haber utilizado bien las herramientas de migración han permitido que los resultados sean positivos, cumpliendo las expectativas de la Gerencia y el área en general.

5.3. Parámetros a ser evaluados acerca del plan de contingencia

El Plan de Continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el Plan de Pruebas que asegure la viabilidad de las soluciones adoptadas.

Para realizar la evaluación del plan de continuidad propuesto se registrarán los datos de dos simulacros que ha sido planificado con los miembros del departamento de Tecnología de Grupo El Comercio C.A. con el fin de identificar falencias del plan y retroalimentar al personal del departamento para que sea efectivo el plan ante cualquier tipo de desastre.

En los simulacros se evaluarán parámetros de tiempo y costos haciendo uso del plan y sin utilizarlo, con el objetivo de realizar una comparación y analizar los resultados que cada uno genera. De igual forma se evaluarán parámetros propios del plan, denominados parámetros de efectividad del plan de continuidad.

5.3.1. Parámetros de Tiempo

Los parámetros que se muestran a continuación se evaluarán en función del tiempo.

- *Tiempo de obtención de un servidor con capacidades similares:* Es el tiempo que transcurre desde que se ha solicitado al proveedor un equipo o recurso hasta que sea entregado.
- *Tiempo de instalación y configuración del Sistema Operativo:* Tiempo que transcurre desde el ensamblado del servidor hasta que finaliza la instalación del sistema operativo que usa el servidor afectado.
- *Tiempo de instalación y configuración del aplicativo:* Es el tiempo que se invierte para instalar y configurar el aplicativo afectado y sus parches o librerías necesarias.
- *Tiempo para reiniciar el servidor:* Tiempo que se requiere para reiniciar al servidor para que reconozca la nueva configuración y se sincronice con los demás equipos.

- *Tiempo para restaurar el backup:* Tiempo que transcurre desde que inicia hasta que finaliza la restauración del backup en un servidor determinado.
- *Tiempo para verificar el funcionamiento del servicio:* Tiempo que se invierte para verificar que los datos estén completos y sean confiables para su utilización.
- *Total tiempo de recuperación:* Tiempo total que ha transcurrido desde el inicio hasta el final de la recuperación. Suma de los tiempos anteriores.

5.3.2. Parámetros de costos

Los parámetros que se muestran a continuación se evaluarán en función de costos.

- *Costo de un servidor con capacidades similares:* Costo en dólares de un servidor de las mismas capacidades del servidor que ha sufrido el daño
- *Costo de consultoría de proveedores en caso de usar este servicio:* Es el costo por hora de asesoría que realizan los proveedores en caso de daños que TI no pueda resolver.
- *Total costo de recuperación:* Es la suma de los costos anteriores.

5.3.3. Parámetros de efectividad del plan de continuidad

A continuación, se muestran los parámetros de efectividad del plan de continuidad.

- *Tiempo de paralización de operaciones del negocio por el desastre:* Es el tiempo que el desastre ha afectado al negocio paralizando los servicios.
- *Tiempo de retrasos de trabajo:* Tiempo que han sufrido los usuarios en entregar sus trabajos a causa de la paralización de los servicios.

- *Número de usuarios afectados por el desastre:* Es el número de usuarios que se ve afectado por la paralización de los servicios.
- *Esfuerzo invertido por los miembros de TI:* Es el esfuerzo medido en horas/persona para la recuperación de los servicios.
- *Confiabilidad e integridad de la información recuperada:* Porcentaje de la integridad de la información una vez recuperada, ayudan a medir los usuarios.
- *Número de recursos de personal adicionales para la recuperación:* número de personas que se necesitaron para la recuperación, adicionales a los miembros de TI.
- *Maximun Tolerable Downtimes (MTD):* Indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio.
- *Recovery Time Objective (RTO):* Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción.
- *Recovery Point Objective (RPO):* Es la magnitud de los datos perdidos que pueden ser tolerados por un proceso del negocio en términos de un periodo de tiempo.

5.4. Evaluación.

Para la evaluación del plan de continuidad se ejecuta dos simulacros y se describe en los escenarios utilizando el plan propuesto y sin utilizarlo, con el fin de realizar una comparación efectiva y obtener recomendaciones para mejorar la gestión de la continuidad del negocio en caso de desastres posteriores en el departamento de Tecnología de Grupo El Comercio C.A.

Para realizar esta comparación se ejecuta el plan de continuidad para el caso de la caída de uno de los servidores que brinda el servicio de Sistema de recursos Empresariales (ERP), el cual es un servidor físico.

Para el segundo simulacro se ejecuta el plan de continuidad para el caso de la caída del servidor Aplicativo del sistema editorial, en el cual se encuentra configurado la aplicación que usan los usuarios para trabajar en las distintas ediciones de los productos impresos del Comercio, este servidor es virtual.

5.4.1. Simulacro de la caída del servidor App del ERP

Se asume que el simulacro se realizará sobre la caída del servidor físico del sistema ERP, el cual lo llamaremos PeopleApp; se asume también que la emergencia se activa un domingo a primera hora de la mañana.

Debido a un daño en el sistema de aire acondicionado del Data Center ha quedado afectado el arreglo de discos del servidor PeopleApp por calentamiento del equipo. Los servidores restantes no han sufrido daños y se encuentran operando con normalidad. La indisponibilidad del servidor PeopleApp ha provocado que los usuarios de todas las áreas no puedan realizar su trabajo respectivo, sin embargo, se asume que el desastre ocurrió un domingo en la madrugada y que la persona de turno de Stand By del área de Infraestructura detecto la alerta de la caída del servidor a través de un correo que envió la herramienta de monitoreo HPSIM.

Se asume que se tiene disponible las cintas con los backups obtenidos automáticamente del día sábado, adicional las cintas que se transportó donde el proveedor contratado para almacenamiento de backups de acuerdo a las políticas de respaldo manejadas por el Departamento de TI. Cabe mencionar que todas las opciones de recuperación están basadas en los documentos de procedimientos donde constan datos como.

- Configuraciones de los servidores, aplicativos, bases de datos, conexiones de red, etc.
- Diagrama de flujos y descripción de los procesos que dependen de TI.

- Políticas para manejo de los procedimientos.

A continuación, se describen las acciones que se realizarán para levantar el servicio afectado en el escenario donde se utiliza el plan y en el escenario donde no se utiliza ningún plan.

5.4.1.1. Escenario sin plan de continuidad

Para solventar el inconveniente, se realizan las siguientes acciones en caso de no implementar ningún plan de continuidad.

1. Obtener un servidor con capacidades similares al servidor actual que ha sufrido el daño, es decir, debemos solicitar al proveedor un nuevo equipo.
2. Recibir el nuevo equipo
3. Configurar equipo
    a) Instalar y configurar el sistema Operativo
    b) Instalar y configurar el aplicativo
    c) Instalar el agente de la herramienta DataProtector para subir el backup.
4. Recuperar las cintas correspondientes al último backup obtenido.
5. Por medio del DataProtector Restaurar la información necesaria en el nuevo servidor.
6. Revisar que los archivos se hayan restaurado con satisfacción y que las carpetas tengan los permisos adecuados.
7. Verificar el funcionamiento de la aplicación.

5.4.1.2. Escenario con plan de continuidad

Se debe realizar las siguientes acciones en caso de implementar el plan de continuidad.

1. Se asume que previamente se virtualizó el servidor físico con la herramienta Virtual Converter, una vez virtualizado se sacó un backup con la herramienta VeeamBackup el cual se tiene respaldado.
2. Realizar una restauración instantánea del backup de la máquina virtual
3. Prender el equipo y verificar que se levante sin inconvenientes.
4. Recuperar las cintas correspondientes al último backup.
5. Por medio del DataProtector Restaurar la información necesaria en el nuevo servidor.
6. Revisar que los archivos se hayan restaurado con satisfacción y que las carpetas tengan los permisos adecuados.
8. Verificar el funcionamiento de la aplicación.

5.4.2. Simulacro de la caída del servidor del Sistema editorial

Se asume que el simulacro se realizará sobre la caída del servidor virtual que presta el servicio del Sistema Editorial, el cual lo llamaremos XredApp; se asume también que la emergencia se activa un lunes a primera hora de la mañana.

Debido a un daño en el servidor virtual por una actualización indebida se corrompió el sistema operativo provocando así que el equipo no encienda y no reconozca el ambiente virtual a la máquina. La indisponibilidad del servidor XRedApp ha provocado que los usuarios de la redacción no puedan realizar su trabajo respectivo, es decir no pueden trabajar en la creación de las distintas ediciones de los productos del GEC, en especial en la edición diaria del diario El Comercio y Ultimas Noticias, sin embargo se asume que el desastre ocurrió un lunes en la madrugada y que la persona del primer turno de Mesa de Ayuda al realizar el monitoreo diario de las aplicaciones detectó que era imposible conectarse al sistema editorial por lo que escaló el problema al área de Infraestructura.

Al igual que el anterior caso se asume que se tiene disponible las cintas con los backups obtenidos automáticamente del día Domingo

A continuación, se describen las acciones que se realizarán para levantar el servicio afectado en el escenario donde se utiliza el plan y en el escenario donde no se utiliza ningún plan.

5.4.2.1. Escenario sin plan de continuidad

Para solventar el inconveniente, se realizan las siguientes acciones en caso de no implementar ningún plan de continuidad.

1. Crear un nuevo servidor virtual con las mismas características del servidor que presentó daños (almacenamiento, cpus y memoria RAM).
2. Configurar equipo
   d) Instalar y configurar el sistema Operativo
   e) Instalar y configurar el aplicativo (solicitar apoyo al proveedor de la aplicación)
   f) Instalar el agente de la herramienta DataProtector para subir el backup.
3. Recuperar las cintas correspondientes al último backup obtenido.
4. Por medio del DataProtector Restaurar la información necesaria en el nuevo servidor.
5. Revisar que los archivos se hayan restaurado con satisfacción y que las carpetas tengan los permisos adecuados.
6. Verificar el funcionamiento de la aplicación.

5.4.2.2. Escenario con plan de continuidad

Se debe realizar las siguientes acciones en caso de implementar el plan de continuidad.

1. Revisar que el último backup sacado con la herramienta VeeamBackup de la máquina virtual haya termina satisfactoriamente
2. Realizar una restauración instantánea del backup de la máquina virtual
3. Prender el equipo y verificar que se levante sin inconvenientes.
4. Recuperar las cintas correspondientes al último backup.

5. Por medio del DataProtector Restaurar la información necesaria en el nuevo servidor.
6. Revisar que los archivos se hayan restaurado con satisfacción y que las carpetas tengan los permisos adecuados.
7. Verificar el funcionamiento de la aplicación.

5.4.3. Ejecución del Plan de Continuidad

A continuación, se detallarán los pasos a seguir en cada fase del plan de continuidad.

- **Etapa 1: Respuesta Inicial y notificación.**

1. Registrar personal que notó el desastre

En esta etapa se registran la o las personas que notaron el desastre o inconveniente con fecha y hora. En el primer caso alertó sobre el inconveniente el Ingeniero de Infraestructura que se encontraba de turno de Stan By a las 05:00 del día domingo, y en el segundo caso notó el inconveniente el Ingeniero de Mesa de Ayuda a las 07:30 del día lunes; en ambos casos se notificó al Coordinador de Infraestructura, Subgerente de Tecnología y Gerente de Desarrollo Digital y Tecnología.

2. Definir el lugar de reunión del equipo de continuidad

Debido a que el inconveniente no se debe a un desastre natural, se define que el lugar de reunión es en el primer piso de las matriz de la empresa en el departamento de Desarrollo Digital & Tecnología, donde el Coordinador de Infraestructura y Networking junto a los miembros del área hacen un análisis general del problema, por lo que se ha determinado que el grado de severidad del impacto es crítico, ya que los dos servidores afectan directamente al negocio

de la empresa; el impacto crítico se encuentra dentro del rango de pérdidas financieras de 0 a 24 horas.

3. Alertar a cada miembro del equipo mínimo y proveedores sobre la alerta del desastre

En esta etapa también se define si es necesario convocar a los demás miembros del equipo mínimo, utilizando el árbol de llamadas que se encuentra en la Figura 112, en este proyecto de titulación no se publican los datos personales de los miembros de la empresa ni de sus proveedores ya que representa información reservada de la misma.

Dado que los miembros de TI pueden resolver el problema no es necesario convocar a más miembros para ejecutar el plan de continuidad, por consiguiente, para la recuperación, el equipo del plan de continuidad del negocio está conformado por.

- Subgerente de Tecnología
- Coordinador de Desarrollo Administrativo
- Ingeniero de Infraestructura y Operaciones
- Ingeniero de Mesa de Ayuda

Con respecto a la convocación de proveedores, en este caso, se convoca al proveedor del Aire Acondicionado para la respectiva revisión y reparación, ya que, si no se controla, puede seguir afectando a los recursos de TI por el aumento de temperatura. También se debe contactar proveedor de hardware para reemplazar las partes afectadas del primer simulacro con el fin de poner operativa la aplicación en el servidor original con una ventana de mantenimiento programada.

4. Determinar hora y condiciones del desastre

Hay que tomar en cuenta que, si el desastre ocurre en horario no laborable, hay que trasladarse al establecimiento inmediatamente. En el primer caso, se

percataron del desastre el domingo a las 05:00 por lo que se acudió de inmediato a las instalaciones. En el segundo caso se percataron del inconveniente el lunes a las 07:30 cuando empezó la jornada laboral.

5. Evaluación preliminar de los daños y sus causas.

De forma general y en caso de ocurrir cualquier desastre, los miembros del departamento TI deben realizar las siguientes actividades.

a) Realizar una inspección general del desastre
    - Revisar que todos los servidores del DataCenter se encuentren encendidos y sin presentar alarmas.
    - Revisar el correcto funcionamiento de los sistemas operativos y aplicaciones de los servidores.
    - Revisar los logs de la obtención de los últimos backups que se debió realizarse de forma automática.
    - Verificar que los usuarios tengan acceso a todas las herramientas de uso diario su respectiva información.
b) Buscar indicios que puedan ayudar a determinar la causa del problema.
    - Verificar si existe algún tipo de amenaza natural, tecnológica o humana.
    - Revisar las conexiones eléctricas, fugas de agua, humo, etc.
    - Asegurar que la amenaza no siga afectando a los demás servidores o servicios del Departamento de Desarrollo & Tecnología
c) Asegurar los recursos del Departamento TI.

6. Preparar un reporte preliminar del desastre y sus problemas

Para tener una idea general del inconveniente se debe realizar un informe preliminar de falla, con lo cual se completa la primera etapa de implementación del plan de continuidad del negocio.

7. Notificar a los miembros del plan de recuperación.

Inmediatamente después de elaborar el informe preliminar de falla, el Gerente de Tecnología debe comunicar el inconveniente a todos los miembros del área, para que de manera inmediata cada uno de los miembros del departamento empiecen a realizar sus funciones de acuerdo a sus roles y responsabilidades.

Para este caso los roles y responsabilidades son:

a) Gerente de Desarrollo y Tecnología
    - Notificar a los gerentes y coordinadores de las áreas afectadas acerca del año ocurrido.
    - Coordinar actividades de administración de la continuidad del negocio.
b) Ingenieros de Infraestructura & Networking.
    - Coordinar la recuperación de los servidores.
    - Coordinar la restauración de los backups.
    - Monitorear el proceso de recuperación de los servidores.
    - Comunicarse con proveedores en caso de ser necesario.
c) Coordinador de Desarrollo Administrativo
    - Revisar que sistemas se encuentran afectados por la caída del servidor Peopleapp.
d) Ingenieros de Mesa de Ayuda
    - Brindar soporte a usuarios mientras se normalizan operaciones para minimizar el impacto de los desastres.
    - Apoyar a Infraestructura en sus actividades.

- **Etapa 2: Evaluación del problema y escalamiento.**

En esta etapa se analiza la magnitud del problema basado en el reporte preliminar y se decide si se pasa o no de manera inmediata a la siguiente fase.

Las actividades a seguir en esta etapa son:

1. Recepción del reporte preliminar del inconveniente

El área de Infraestructura es la encargada de la recuperación de los servidores, realiza un check list y pasa la información a Operaciones para continuar con la documentación; cabe recalcar que todas las personas del área deben trabajar en conjunto.

2. Evaluar la interrupción de los procesos, el daño de los equipos y recursos.

Se debe determinar los procesos y áreas que fueron afectadas, los sistemas e infraestructura de red. Para este caso se registra el impacto en el negocio a causa de los dos simulacros, (ver tabla 25 y 26).

Tabla 25
Análisis de impacto en el negocio por la caída del servidor Peopleapp

Procesos	Descripción	Frecuencia	Área Afectada	Criticidad
Cargas contables	Información Gerencial	Diaria	Ventas – Financiera	4
Pedidos diarios de suscripciones	Entrega de ejemplares diarios	Diaria	Distribución	4
Contabilidad Interna	Contabilidad	Diaria	Financiera	2
Cuentas por Cobrar	Cuentas por cobrar de carteras diaria	Diaria	Distribución – Financiera	4
Facturación Clientes	Facturación de servicios clientes	Diaria	Ventas – Agencias	4
Inventario de Activos	Inventario de activos	Diaria	Financiera	1
Cuentas por pagar	Cuentas por pagar	Diaria	Financiera	2

Fuente: (Autor)

Tabla 26
Análisis de impacto en el negocio por la caída del servidor XRedapp

Procesos	Descripción	Frecuencia	Área Afectada	Criticidad
Botado del Comercio	Elaboración de la edición del Comercio	Diaria	Redacción - Preprensa	4
Botado Ultimas Noticias	Elaboración de la edición de Ultimas Noticias	Diaria	Redacción - Preprensa	4
Botado Revista Líderes	Elaboración de la edición de Revista Líderes	Semanal	Redacción - Preprensa	2
Botado Revista Familia	Elaboración de la edición de Revista Familia	Semanal	Redacción - Preprensa	2
Botado Carburando	Elaboración de la edición de Carburando	Semanal	Redacción - Preprensa	2
Botado Educación	Elaboración de la edición de Educación	Mensual	Redacción - Preprensa	1
Botado Pandilla	Elaboración de la edición de Pandilla	Semanal	Redacción - Preprensa	2

Fuente: (Autor)

3. Estimar el impacto del desastre, catalogando el desastre como bajo, medio, alto o crítico.

De acuerdo a un análisis preliminar se cataloga a los dos desastres como críticos.

El segundo simulacro es crítico debido a que sin el servicio del servidor xredapp se ve afectada la elaboración de la edición del Comercio y Ultimas Noticias, las cuales salen al mercado diariamente. Esto provocaría el riesgo de que no salgan a la venta dichas ediciones, ocasionando pérdidas económicas y daño a la imagen de la empresa.

4. Determinar si se debe continuar a la siguiente fase y estimar el tiempo de recuperación.

Al ser desastres que afectan procesos críticos de acuerdo al informe de Análisis de impacto, se debe continuar con la siguiente fase del plan.

El tiempo estimado de recuperación de los servicios se detalla a continuación.

- Para recuperar el servidor Peopleapp se requiere aproximadamente 6 horas, utilizando el plan de continuidad propuesto.
- Para recuperar el servidor Xredapp se requiere aproximadamente 3 horas utilizando el plan de continuidad propuesto.

- **Etapa 3: Recuperación.**

Una vez analizado el problema y en el primer caso al ser un inconveniente con el aire acondicionado se debe verificar que no exista más servidores alarmados, contactar al proveedor para que revise inmediatamente el equipo, obtener ventiladores de manera inmediata y lo más importante apagar los servidores que no afecten a la producción del negocio con el fin de disminuir la temperatura en el Datacenter y evitar más daños de los componentes o equipos en general.

En el segundo caso se verifica la correcta funcionalidad de todos los servidores virtuales, se prueba conexión de los clientes a los servicios, y se revisa logs y el correcto funcionamiento de los Sistemas Operativos

Una vez realizado las tareas mencionadas anteriormente se pone en marcha la recuperación de los servicios afectados, tarea que se encarga el área de Infraestructura & Operaciones. A continuación, se detalla los pasos de recuperación en cada uno de los simulacros.

1. <u>Simulacro 1: Recuperación del servidor PeopleApp</u>

En el primer caso el daño se presenta en un servidor físico y como se comentó en el capítulo IV se ha implementado la herramienta llamada Vmware Vcenter Converter y Veeam Backup, con lo cual se asume que todos los servidores físicos

que brindan servicios críticos fueron virtualizados y a su vez respaldados para afrontar una emergencia.

Es decir, para este caso se tiene un backup del servidor Peopleapp virtualizado, el cual se restaurará en el ambiente virtual y posterior se actualizará los archivos necesarios haciendo uso del backup diario que se saca en cintas.

A continuación, antes de pasar al detalle de la recuperación del servicio, se describe los pasos que se realizó para la virtualización y obtención del backup del servidor con lo cual se pudo poner en marcha el plan de contingencia.

Virtualización del servidor PeopleApp

Para virtualizar el servidor se debe seguir lo siguientes pasos.

- Abrir el programa Vcenter Vmware Converter y escoger la opción “Convert Machine”

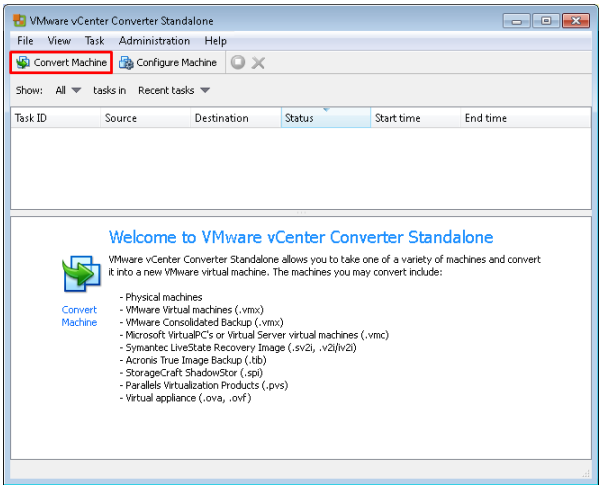


Figura 141 Conversión de un servidor físico

Fuente: (Autor)

- Especificar los datos del servidor a convertir (IP, usuario administrador o con privilegios de administrador, contraseña y sistema operativo)

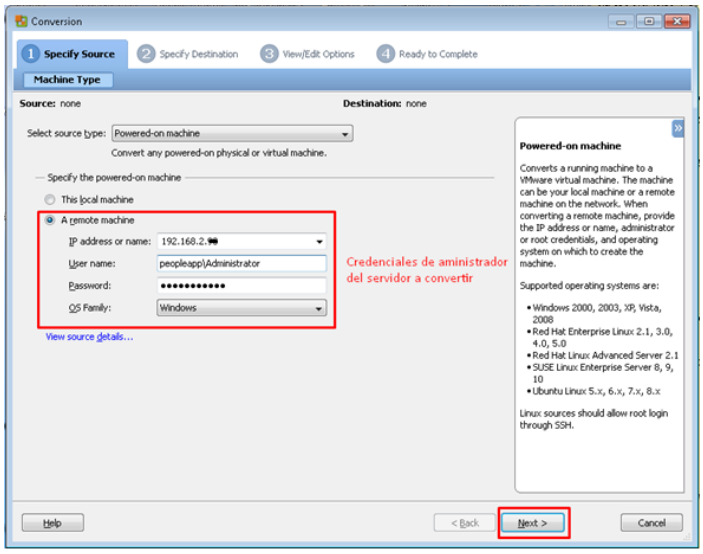


Figura 142 Configuración datos del servidor a convertir

Fuente: (Autor)

- Especificar los datos de acceso al servidor destino, puede ser acceso al servidor donde se encuentra la consola de administración de todo el ambiente virtual o directamente al servidor físico donde se desea ubicar el servidor. En este caso se conectó a la consola del ambiente virtual, seguido se escoge el servidor y el DataStore donde se alojará el servidor y se especifica una etiqueta o nombre del equipo como se observa en la figura 143.

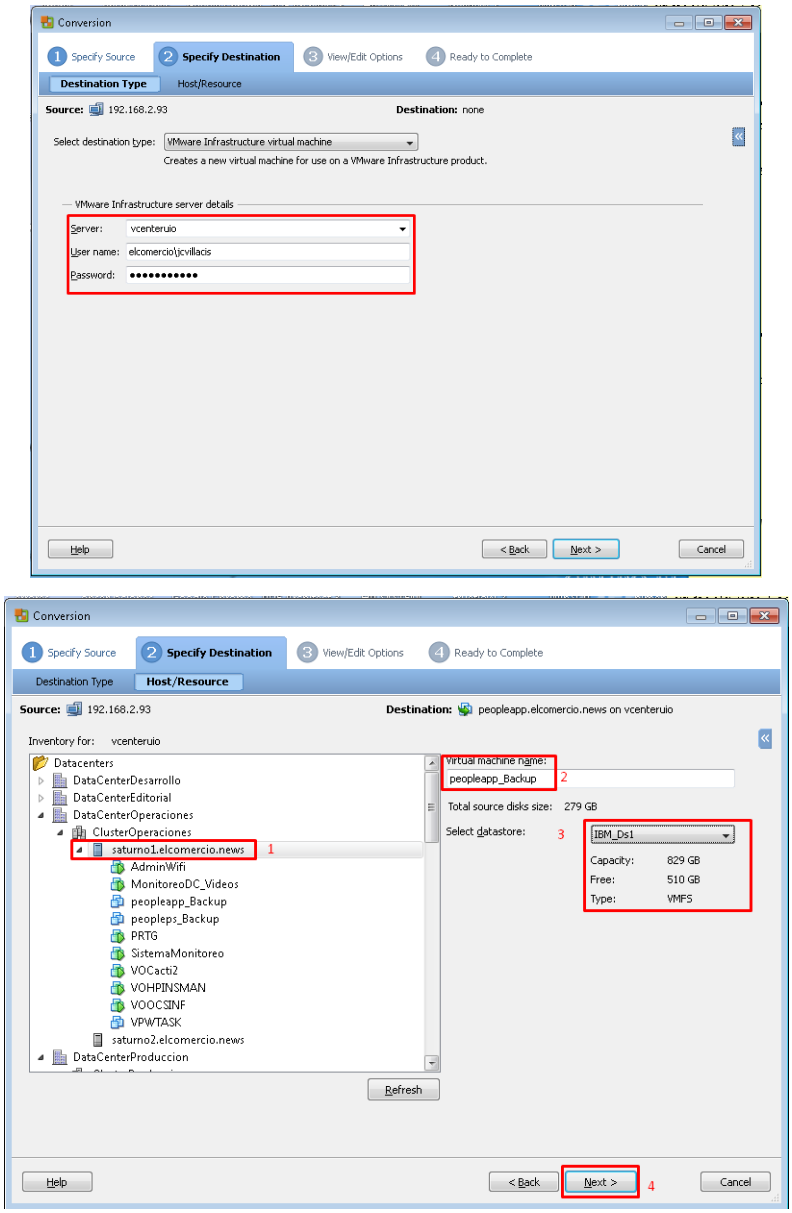


Figura 143 Configuración de datos del servidor destino donde se alojará el servidor convertido

Fuente: (Autor)

- Una vez configurado el origen y el destino, en la siguiente ventana se puede editar los recursos con lo que la máquina virtual se creará, en este caso se dejó todo por defecto, es decir, el servidor virtual tendrá las

mismas características del servidor físico en cuanto a recursos (Espacio de disco, memoria, procesadores, red, etc)

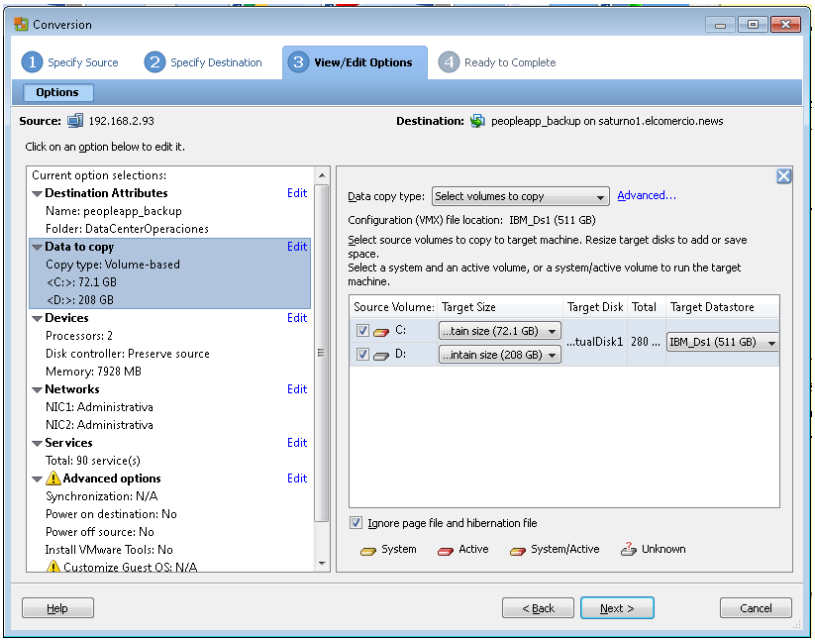


Figura 144 Configuración de recursos de la máquina virtual a convertirse

Fuente: (Autor)

- Finalmente se mostrará una ventana con el resumen de las configuraciones realizada, con lo cual se ha completado el proceso de configuración. Una vez hecho clic en el botón finalizar la tarea correrá y se realizará la conversión del servidor. En este caso la tarea de conversión del servidor Peopleapp tardó aproximadamente 3 horas.

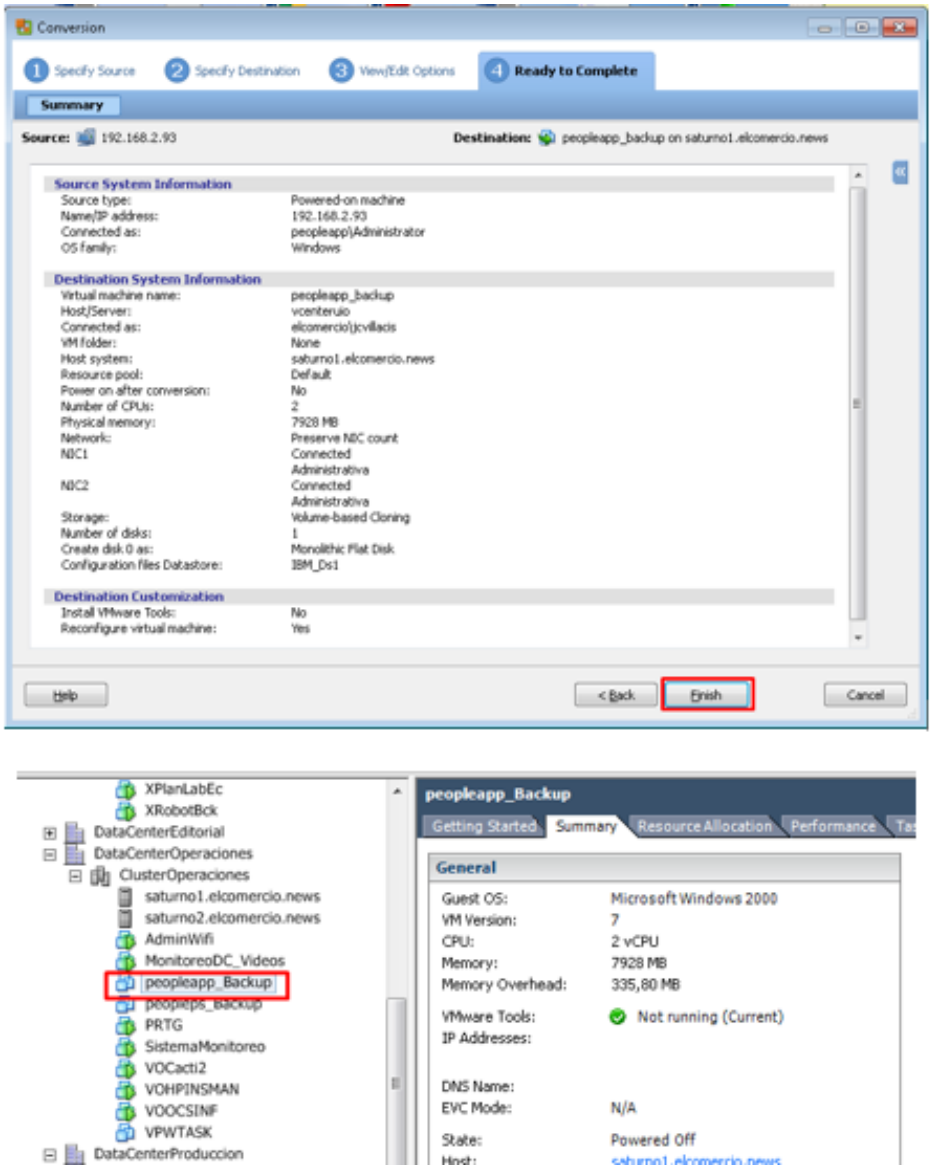


Figura 145 Resumen y finalización de la tarea de conversión del servidor físico

Fuente: (Autor)

Backup del servidor Peopleapp virtualizado

Una vez virtualizado el servidor peopleapp se procede a sacar backup de la máquina haciendo uso del software Veeam Backup & Replication, el cual se explicó en el capítulo IV. Para configurar se debe crear un trabajo de backup,

donde se escoge el servidor virtual a respaldar, el repositorio donde se almacenará y de ser necesario un horario de respaldo, en este caso como solo se lo sacará por una vez no se configura el horario, (ver figura 146).

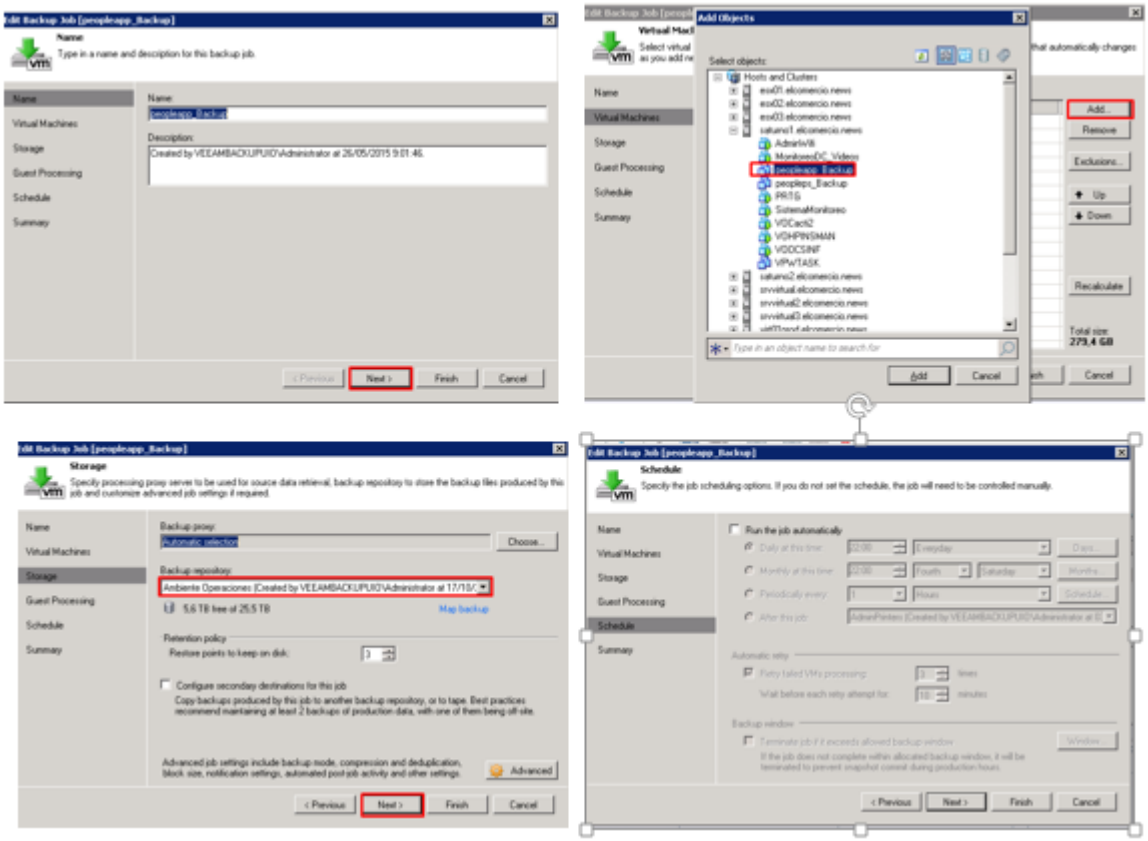


Figura 146 Configuración tarea de backup de un servidor virtual

Fuente: (Autor)

Una vez finalizada la configuración se puede ejecutar la tarea de backup, la cual al final del trabajo, muestra un mensaje si fue satisfactorio o no la tarea, adicional se puede observar datos estadísticos e informativos del trabajo, como el tamaño del backup, la tasa de transferencia, el throughput, etc.

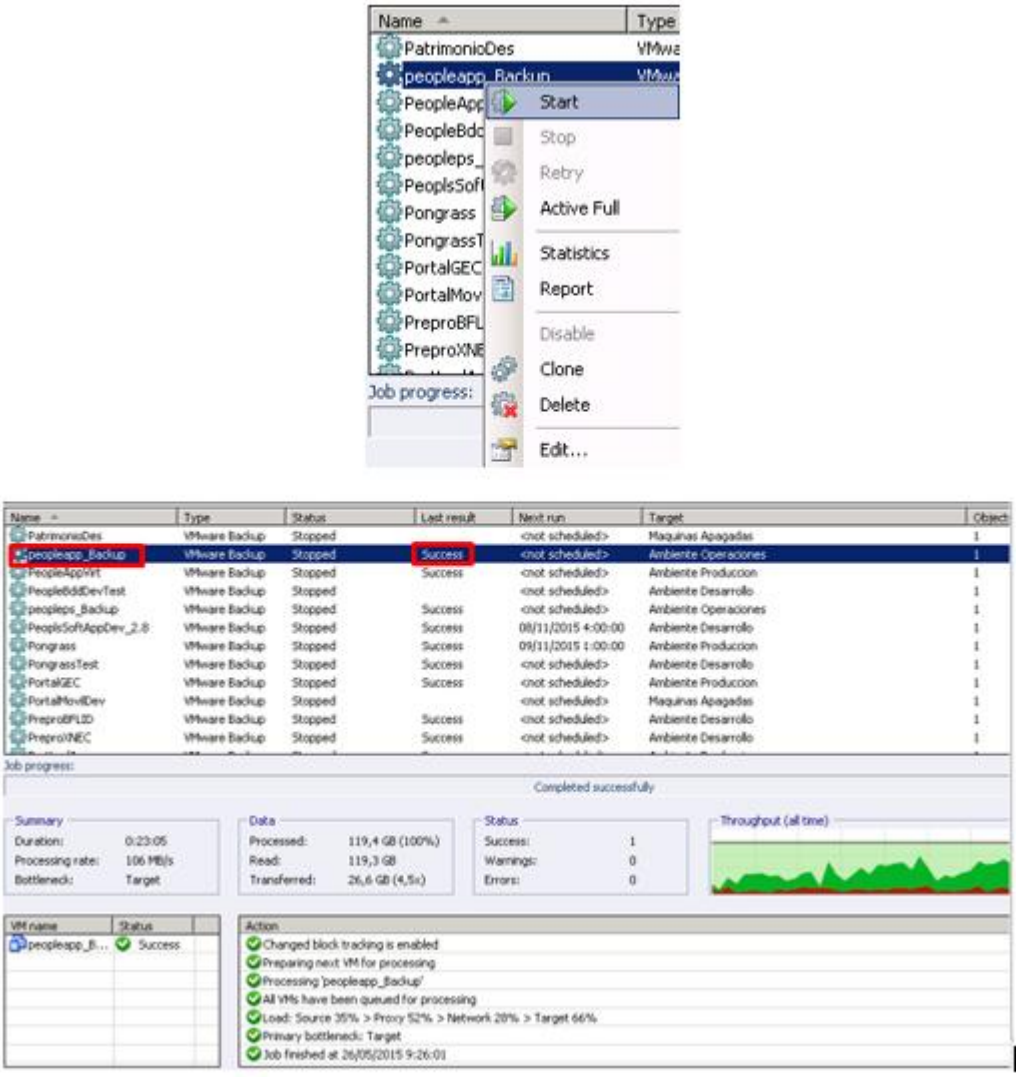


Figura 147 Resultados de la tarea de backup de una máquina virtual

Fuente: (Autor)

Con estas tareas realizadas con anterioridad se puede garantizar que el plan de contingencia pueda ser ejecutado, para lo cual en esta etapa se pone en marcha la recuperación del servicio.

Para este primer caso, al no ser posible poner operativo el servidor físico se hará uso del backup de la máquina virtualizada, para lo cual se usa la herramienta Veeam Backup & Replication siguiendo los siguientes pasos.

1. Crear la tarea de Restore escogiendo entre las opciones que brinda la herramienta, para este caso se escoge una restauración de la máquina entera.

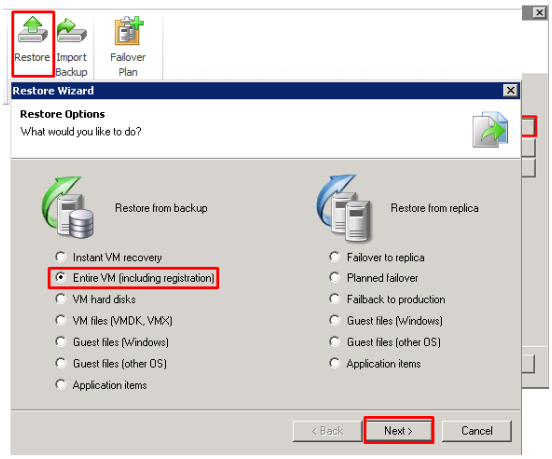


Figura 148 Configuración de restauración opción máquina entera

Fuente: (Autor)

2. Seleccionar la máquina virtual a restaurar desde el repositorio de backup.

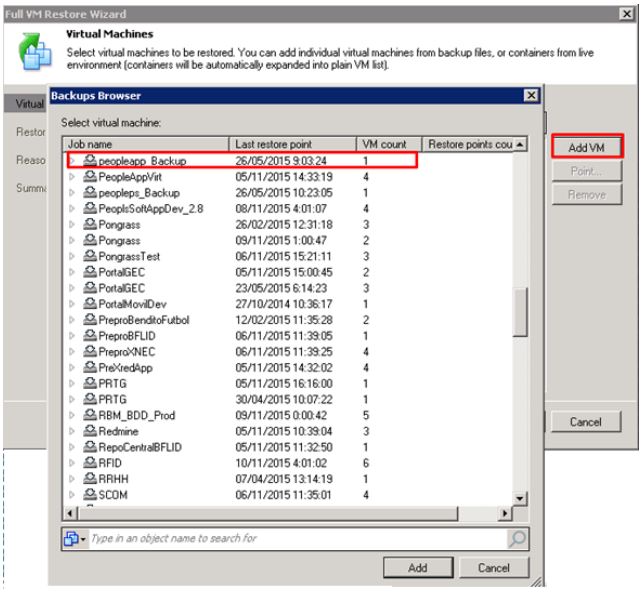


Figura 149 Selección de la máquina a restaurar desde un backup

Fuente: (Autor)

3. Especificar si la restauración se hará en la ubicación original o en una nueva. En este caso se escoge la segunda opción con el fin de ir configurando paso a paso el lugar en donde se realizará la restauración-

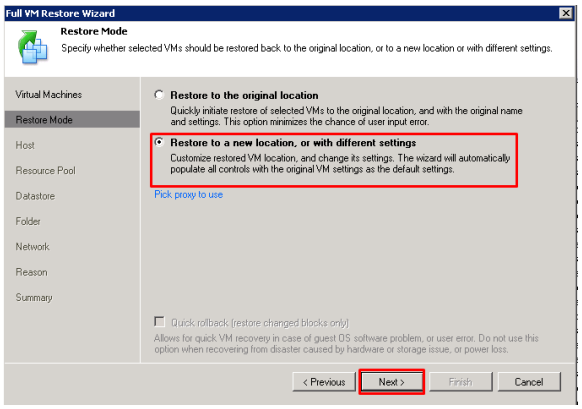


Figura 150 Modo de restauración

Fuente: (Autor)

4. Escoger el host físico donde se alojará la máquina virtual, en este caso se ha escogido el servidor virt02prod que se encuentra en el cluster de producción.

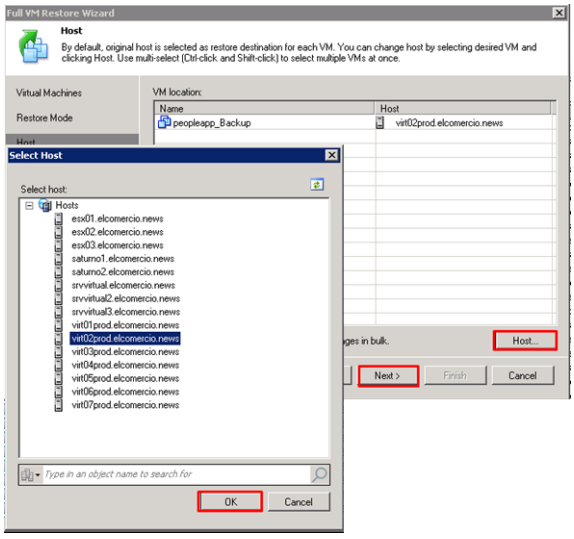


Figura 151 Selección de host físico para la restauración de la MV

Fuente: (Autor)

5. Escoger el Datastore o almacenamiento de donde tomará espacio la máquina virtual para ser restaurada.

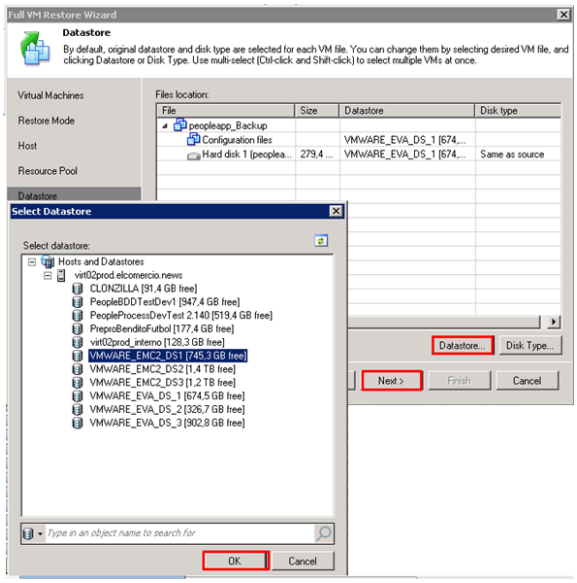


Figura 152 Selección del datastore para la restauración de la MV

Fuente: (Autor)

6. Revisar que la configuración de red sea similar a la de producción en este caso el servidor físico se encontraba en la VLAN de administración.

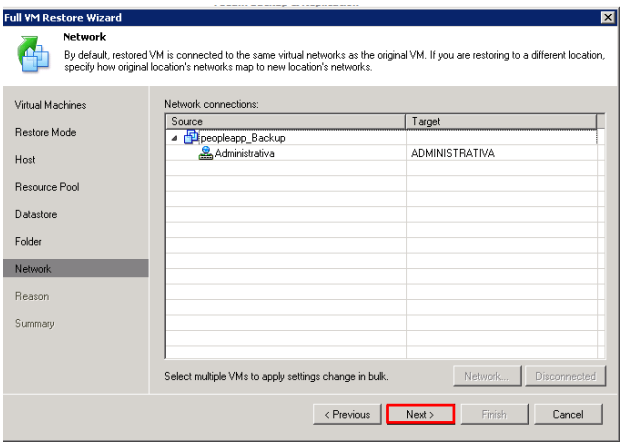


Figura 153 Configuración de red de la MV a restaurar

Fuente: (Autor)

7. Finalmente se coloca una razón de la restauración y se finaliza la configuración para que la tarea arranque inmediatamente.

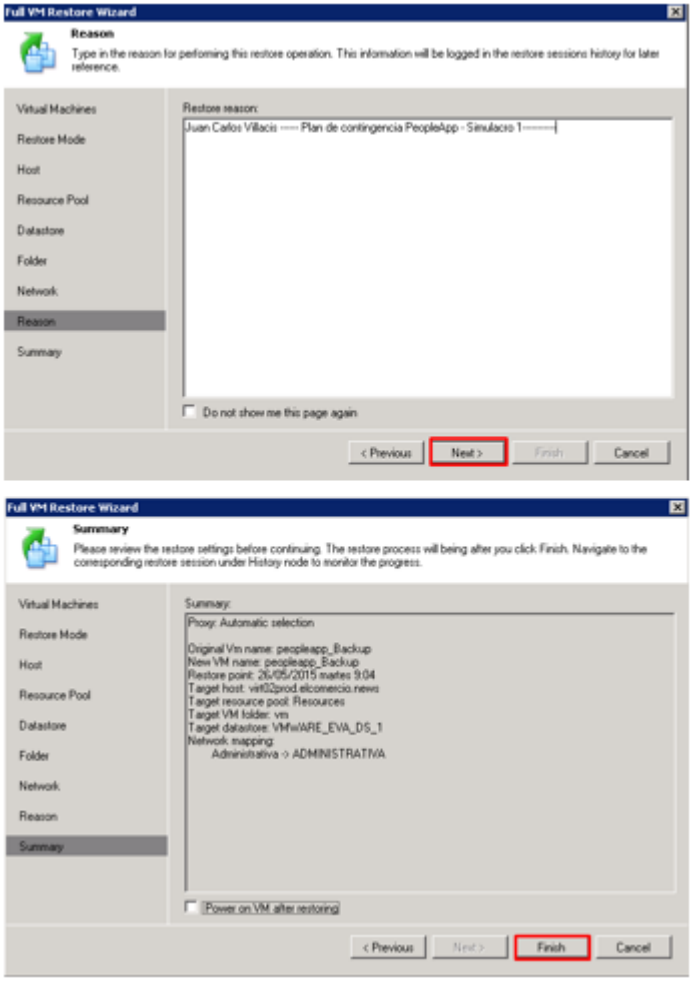


Figura 154 Finalización configuración de la tarea de restauración

Fuente: (Autor)

8. Una vez que comienza a correr la tarea se muestra la pantalla de progreso de la restauración donde se puede observar la información y el porcentaje de restauración.

   Para este caso el servidor tardó en restaurarse aproximadamente 3 horas 7 minutos y su resultado fue satisfactorio como se observa en la figura 155.

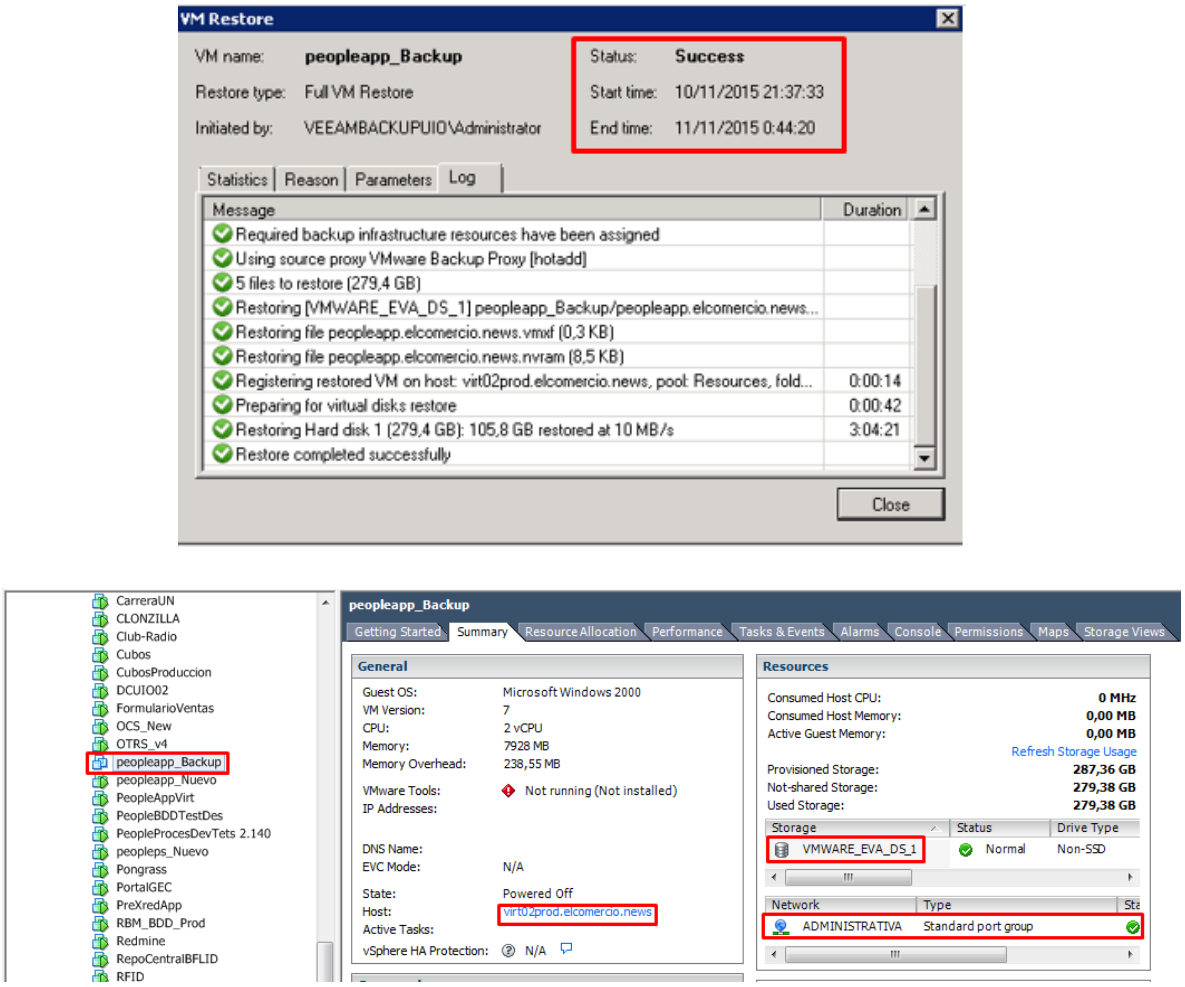


Figura 155 Informe tarea de restauración satisfactoria

Fuente: (Autor)

Con el servidor restaurado, lo único que falta es igualar la información necesaria, para esto restauraremos la información desde el último backup efectuado de los archivos en cintas, es decir, del día anterior. Para esto se hace uso de la herramienta DataProtector y se restaura la información en el servidor original tarea que concluyó en 20 minutos aproximadamente como se observa en la figura 157.

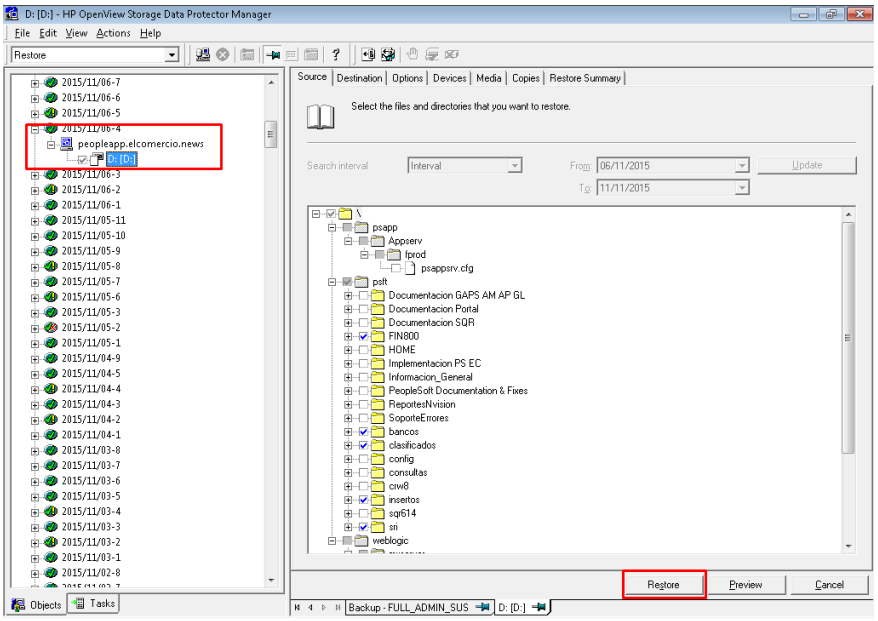


Figura 156 Selección de archivos a restaurar desde DataProtector

Fuente: (Autor)

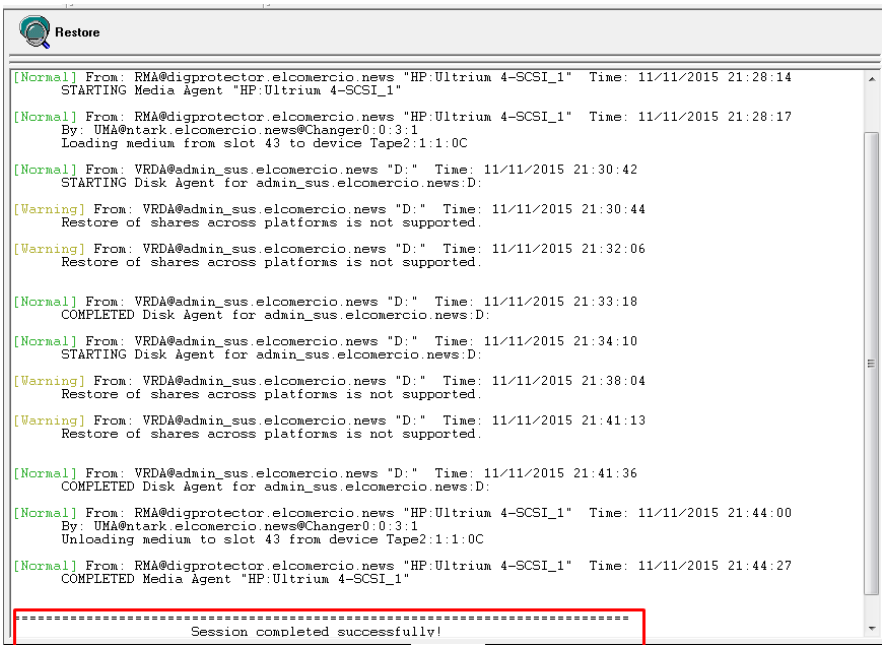


Figura 157 Resultado final de la restauración con el Dataprotector

Fuente: (Autor)

Con esto se ha concluido la tarea de restauración y se ha puesto productivo el servicio de People Soft satisfactoriamente.

2. Simulacro 2: Recuperación del servidor Xredapp

El daño del servidor Xredapp es considerado crítico ya que afecta directamente al negocio, poniendo en riesgo que la edición del Comercio no circule en el país. Por esta razón, al armar el plan de contingencia se ha considerado sacar un backup diario de este servidor por medio del VeeamBackup & Replication.

La restauración de este servidor se lo hace mediante el uso de la misma herramienta antes mencionada, pero a diferencia del simulacro anterior, al necesitar este equipo lo más pronto posible se lo ha hecho escogiendo la opción de Recuperación instantánea, la cual restaura la máquina, pero haciendo uso del repositorio donde se encuentra el backup. Los pasos para restaurar en este modo son los siguientes:

1. Escoger la Opción de restauración de modo instantaneo

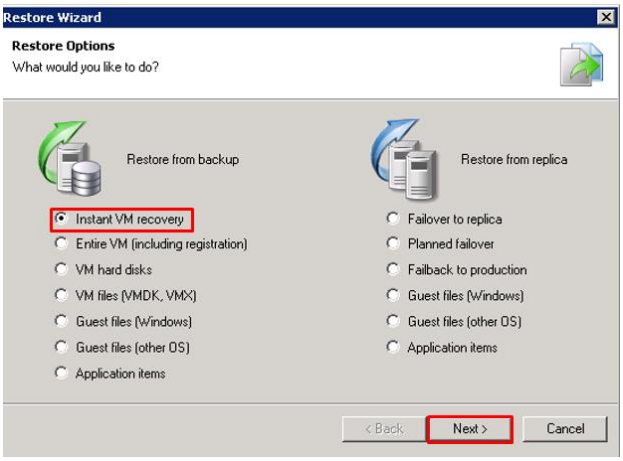


Figura 158 Configuración de restauración de una MV modo instantáneo

Fuente: (Autor)

2. Escoger el backup de la máquina virtual en el punto de restauración que se desea. En este caso el último backup realizado.

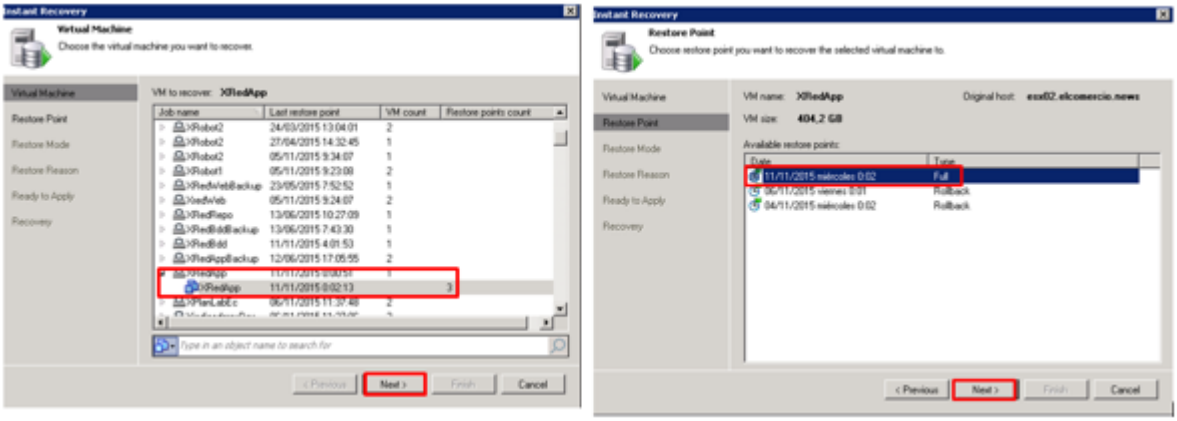


Figura 159 Selección punto de restauración

Fuente: (Autor)

3. Escoger el servidor host donde se creará la máquina restaurada

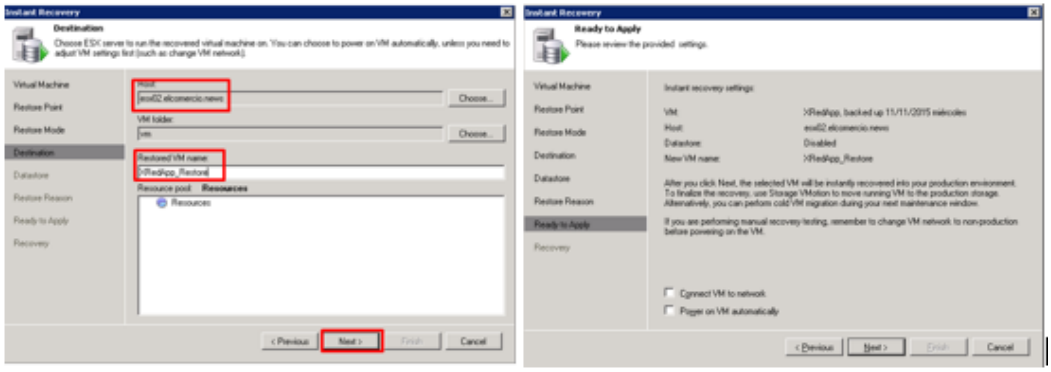


Figura 160 Selección de host físico para la restauración de la MV

Fuente: (Autor)

4. Finalmente procedemos a restaurar la máquina virtual la cual en 2 minutos se encuentra disponible como se observa en la figura 161.

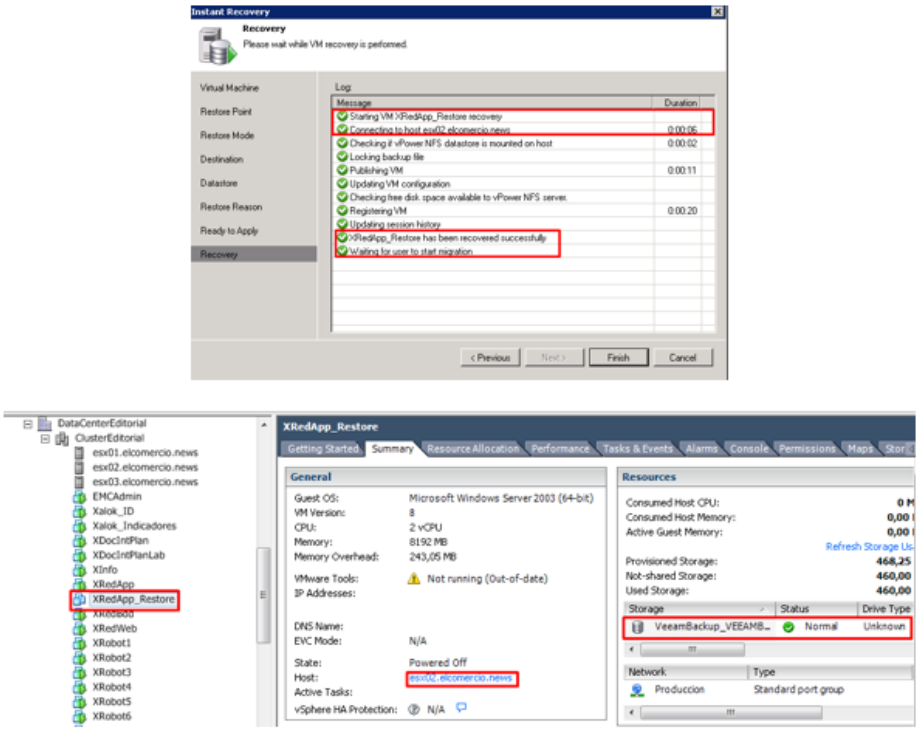


Figura 161 Máquina Xredapp restaurada trabajando desde el repositorio de backup

Fuente: (Autor)

Cabe mencionar que este método tiene una ventaja, pues, después de estar operativos y comprobar que la aplicación se encuentra funcionando se tiene la opción de realizar una migración en caliente, es decir, se puede migrar el servidor hacia el datastore original sin necesidad de tener una indisponibilidad del servicio (ver figura 162).

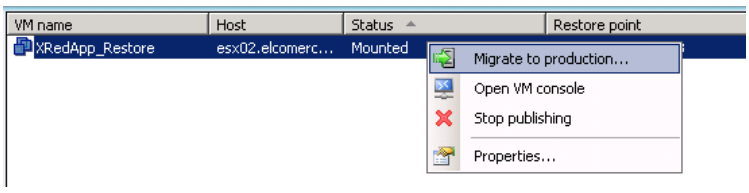


Figura 162 Migración en caliente de la máquina restaurada

Fuente: (Autor)

5.5. Resultados obtenidos de la evaluación.

Como se ha mencionado anteriormente, el simulacro ayuda a retroalimentar el plan de continuidad para así apoyar en su efectividad.

Los resultados de la caída de los servidores han dado como resultado varios valores en parámetros de tiempo, costos y efectividad del plan, de tal forma que ayudan a evaluar si el plan es aplicable a la realidad de la empresa y sus operaciones.

A continuación, se hará un análisis de los parámetros determinados tomando en cuenta que se los compara aplicando el plan y sin aplicarlo, para definir las ventajas y desventajas de su ejecución en el Departamento de Tecnología en Grupo El Comercio C.A.

5.5.1. Tiempo que se ha invertido durante el desastre

En las tablas 27 y 28 se presenta la comparación de los tiempos de recuperación con y sin plan de continuidad en los dos simulacros.

Tabla 27
Parámetros de tiempo de evaluación del simulacro 1

Parámetros	Sin plan de continuidad	Con plan de continuidad
Tiempo de obtención de un servidor con capacidades similares al servidor original	20 días	3 horas
Tiempo de instalación y configuración del sistema operativo	6 horas	0 horas
Tiempo para ingresar el servidor al dominio	10 minutos	0 minutos
Tiempo de instalación y configuración del aplicativo PeopleSoft	1 día	0 días

CONTINÚA

Tiempo para cargar el backup desde cintas	20 minutos	20 minutos
Tiempo para validar los accesos y procesos de la aplicación	1 hora	1 hora
Tiempo para verificar el buen funcionamiento del servicio	1 hora	1 hora
TOTAL TIEMPO	21 días, 8 horas, 30 minutos	5 horas y 20 minutos
Tiempo aproximado	**22 días --> 528 horas**	**6 horas**

Fuente: (Autor)

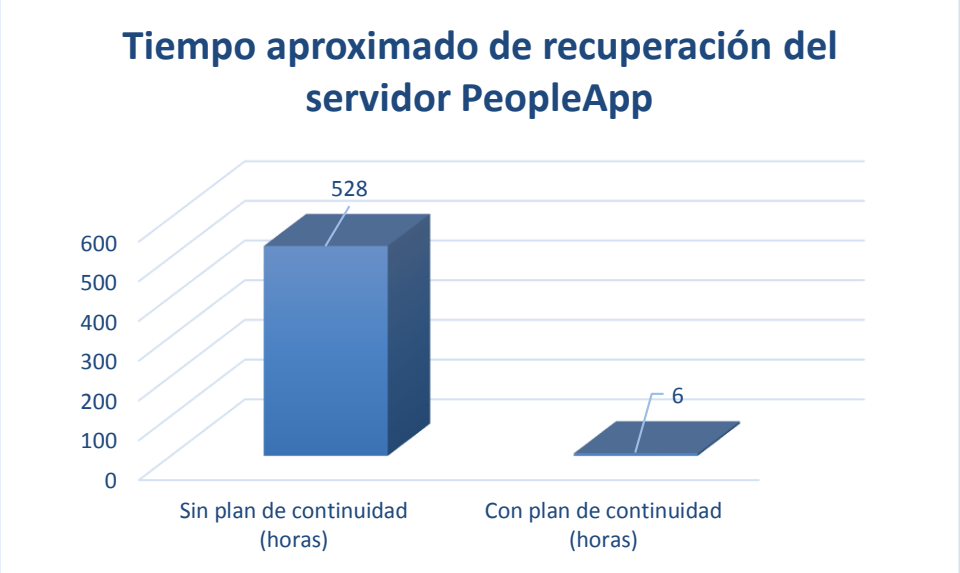


Figura 163 Tiempo aproximado de recuperación del servidor PeopleApp

Fuente: (Autor)

En este caso si se aplica el plan de continuidad, el servidor de reemplazo será el que fue virtualizado con anterioridad y que se encuentra respaldado en el repositorio de backups de las máquinas virtuales, de tal forma que tomaría aproximadamente 3 horas restaurarlo y 3 horas ponerlo operativo.

Si no se aplica el plan de continuidad, los miembros de TI tendrían que dedicarse a conseguir un servidor con similares características, lo cual tomaría mucho tiempo ya que los proveedores de hardware generalmente no tienen disponibles en stock servidores con características determinadas y menos aún servidores descontinuados, por lo tanto, se estima un promedio de 20 días para que el servidor sea entregado y a partir de esto configurar el aplicativo (ver figura 164).

Tabla 28
Parámetros de tiempo de evaluación del simulacro 2

Parámetros	Sin plan de continuidad	Con plan de continuidad
Tiempo de obtención de un servidor con capacidades similares al servidor original	1 hora	10 minutos
Tiempo de instalación y configuración del sistema operativo	6 horas	0 horas
Tiempo para ingresar el servidor al dominio	10 minutos	0 minutos
Tiempo de instalación y configuración del aplicativo Xalok Red	2 días	0 horas
Tiempo para cargar el backup desde cintas	1 hora	0 horas
Tiempo para validar los accesos y procesos de la aplicación	1 hora	1 hora
Tiempo para verificar el buen funcionamiento del servicio	1 hora	1 hora
TOTAL TIEMPO	2 días, 10 horas, 10 minutos	2 horas y 10 minutos
Tiempo aproximado	**3 días --> 72 horas**	**3 horas**

Fuente: (Autor)

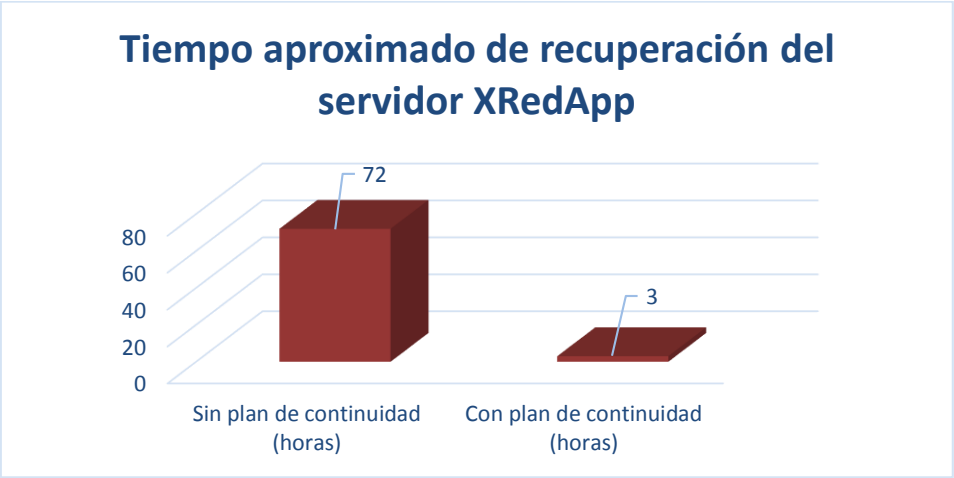


Figura 164 Tiempo aproximado de recuperación del servidor XRedApp

Fuente: (Autor)

Para el simulacro 2, si se aplicará el plan de continuidad se tendría restablecido el servicio en 3 horas aproximadamente, ya que se haría uso del backup del servidor virtual que se saca todos los días.

En tanto que, si no se hace uso de ningún plan de continuidad, será necesario preparar un nuevo servidor virtual y con ayuda del proveedor configurar el aplicativo lo cual tomaría un tiempo aproximado de 3 días, lo cual es crítico para la empresa, (ver figura 164).

5.5.2. Costos generados por el desastre

En las tablas 29 y 30 se presenta la comparación de los costos de recuperación con y sin plan de continuidad.

Tabla 29
Parámetros de costos de evaluación del simulacro 1

Parámetros	Sin plan de continuidad	Con plan de continuidad
Costo de un servidor con capacidades similares	USD 8000	USD 0
Costo consultoría de Proveedores en caso de haber utilizado este servicio	USD 1200	USD 0
Total Costos	**USD 9200**	**USD 0**

Fuente: (Autor)

Tabla 30
Parámetros de costos de evaluación del simulacro 2

Parámetros	Sin plan de continuidad	Con plan de continuidad
Costo de un servidor con capacidades similares	USD 0	USD 0
Costo consultoría de Proveedores en caso de haber utilizado este servicio	USD 2400	USD 0
Total Costos	**USD 2400**	**USD 0**

Fuente: (Autor)

En el primer caso el costo aproximado de la adquisición de un servidor con similares características es de $ 8000, de acuerdo a los valores vigentes en el mercado. En cambio, si se aplica el plan de continuidad propuesto no se invierte costo alguno en ninguno de los dos casos, la inversión sería con antelación y a largo plazo.

Tomando en cuenta que cualquier proveedor al realizar una consultoría cobra un aproximado de $50 la hora dependiendo el tipo de servicio que brinde. En ambos casos sería necesario aplicar a la consultoría para configurar o solicitar ayuda

acerca de la configuración de los aplicativos. Si se aplica el plan de continuidad, teniendo documentados todos los procesos y procedimientos a seguir en caso de daños, la situación puede ser controlada por los miembros de TI, evitándose así los costos por consultoría.

En ambos casos se puede notar la gran diferencia de costos al no utilizar un plan de continuidad, pues uno de los objetivos del plan de continuidad es tratar de minimizar los costos al momento de la recuperación, además de ayudar a la continuidad del negocio.

5.5.3. Parámetros de efectividad del Plan de continuidad

En la tabla 31 se presenta la comparación de los parámetros de efectividad del simulacro 1 y 2.

Tabla 31
Parámetros de efectividad del plan de continuidad del negocio

Parámetros	Simulacro 1 con Plan de Continuidad	Simulacro 2 con Plan de Continuidad
Tiempo de paralización de operaciones del negocio por el desastre	9 horas (paralización parcial)	6 horas (paralización parcial)
Tiempo de retraso de trabajo	5 horas	3 horas
Porcentaje de usuarios afectados por el desastre	80%	50%
Número de procesos críticos afectados por el desastre	8	2
Esfuerzo invertido por los miembros de TI	18 horas / hombre	9 horas / hombre
Integridad de la información recuperada	99 % (1 % si se configuró algún archivo luego de ña virtualización del servidor físico)	100%
Número de recursos de personal adicionales para la recuperación	0	0
Maximun Tolerable Downtimes (MTD)	Los procesos críticos no deben estar indisponibles más de 24 horas	Los procesos críticos del sistema editorial no deben estar indisponibles más de 6 horas
Recovery Time Objective (RTO)	48 horas base	8 horas
Work Recovery Time (WRT)	2 horas	2 horas
Recovery Point Objective (RPO)	Los datos perdidos que pueden ser tolerados en función del tiempo es de 30 minutos	Los datos perdidos que pueden ser tolerados en función del tiempo es de 30 minutos

Fuente: (Autor)

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Con la migración e implementación del storage server X1800, se logró erradicar el cuello de botella que existía al acceder simultáneamente al servidor Preprensa, generando satisfacción en los usuarios finales.
- Al conectar el nuevo servidor de Preprensa a la Red SAN, se logró establecer comunicación entre el servidor y la librería de backup por medio de fibra, logrando así obtener los backups por la SAN sin afectar el rendimiento de tráfico de la LAN.
- El plan de contingencia elaborado, tiene como punto fundamental salvaguardar la información y la infraestructura de Grupo El Comercio, aplicando las mejores prácticas de seguridad para proteger y preparar al personal ante algún desastre.
- El plan de contingencia para un departamento TI debe estar siempre enfocado a la recuperación de las aplicaciones y servicios críticos del negocio.
- Al realizar inversiones y planificaciones de actividades para volver a la operación normal luego de un desastre, los costos de recuperación son bajos; mientras que, a mayor cantidad de tiempo de paralización de operaciones, mayores son las pérdidas del negocio.
- Para lograr que el plan de continuidad sea exitoso, se requiere la participación activa de todos los miembros de TI y de la compañía.

6.2. Recomendaciones

- El software y la información es el activo más importante de la compañía debido a que es un medio de comunicación, cuyo valor se obtiene por la importancia de su uso y eficiencia; por eso es importante y relevante que se opere sobre una infraestructura estable que garantice un óptimo trabajo del software e información.
- Se recomienda migrar las aplicaciones que se encuentren en servidores obsoletos hacia servidores de generación actual, para garantizar la estabilidad de las mismas y evitar futuros inconvenientes e indisponibilidades.
- Se recomienda implementar una solución de backup a disco o librería con cintas LTO6 para mejorar los tiempos de backup y restauración.
- Se recomienda invertir en la compra de 8 licencias VeeamBackup para automatizar el backup diario de las máquinas virtuales y así evitar la revocación de la licencia todos los días.
- Se recomienda mantener el plan de continuidad actualizado mediante revisiones cada 6 meses y simulacros anuales, con el fin de mantener vigente todas sus actividades.

BIBLIOGRAFIA

Anónimo. (07 de Junio de 2010). *Tutorial Allway Sync*. Obtenido de https://maquitoblog.wordpress.com/2010/06/07/tutorial-allway-sync/

Barreto, J. (2011). *Windows Storage Server 2008 R2 Architecture and Deployment*. Obtenido de http://blogs.technet.com/b/josebda/archive/2011/02/17/new-white-paper-windows-storage-server-2008-r2-architecture-and-deployment.aspx

Benitez Pereira, P. F., & Casachahua Medina, J. R. (2011). *Seguridad en computación e informática.* Obtenido de http://www.slideshare.net/villarrealino/anlisis-de-riesgos-8181863

Bligoo. (2015). *Que son los respaldos de información, como y en donde se utilizan*. Obtenido de http://seguridadeninformacionweb.bligoo.com.mx/que-son-los-respaldos-de-informacion-como-y-donde-se-utilizan#.V5o9KriGuko

Brandt, A. (2012). *Free and Easy Backup With SyncToy*. Obtenido de http://www.pcworld.com/article/248927/free_and_easy_backup_with_synctoy.html#comments

BSIGROUP. (2014). *Sistemas de gestion ISO/IEC 27001 de Seguridad de la Información*. Obtenido de http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

Computo y Accesorios. (2015). *QNAP TS-269 PRO, Servidor de Almacenamiento en Red (NAS) de alto rendimiento 2 Bahías para SMBs*. Obtenido de http://computoyaccesorios.com/producto/qnap-ts-269-pro-servidor-de-almacenamiento-en-red-nas-de-alto-rendimiento-2-bahias-para-smbs

Cruz, C. (2012). *Magic Transfer*. Obtenido de http://www.portalprogramas.com/magic-transfer/

Escuela Abierta de Nuevas Tecnologías. (28 de Agosto de 2009). *Robocopy, una mejor manera de copiar archivos en Windows*. Obtenido de http://escuela.conexionesbcn.com/robocopy-una-mejor-manera-de-copiar-archivos-en-windows/

Fourdtech. (2014). *Comparación entre redes de área de almacenamiento y almacenamiento de red.* Obtenido de http://www.fourdtech.com/downloads/san_nas.pdf

Garth A., G., & Van Meter, R. (Noviembre de 2000). *Network Attached Storage Architecture.* Obtenido de http://www.cs.cmu.edu/~garth/CACM/CACM00-p37-gibson.pdf

GOMEZ CAMPOS, R. (10 de Agosto de 2012). *Fundamentos de Los Servidores y El Software de Servidor*. Obtenido de

http://redesdedatosrichardin.blogspot.com/2012/08/fundamentos-de-los-servidores-y-el.html

Grass Valley. (2014). *Network Attached Storage (NAS) System.* Obtenido de http://www.grassvalley.com/docs/DataSheets/newsprod/nas/nas_ds.pdf

Grupo El Comercio C.A. (30 de 01 de 2012). *Información Corporativa Grupo El Comercio*. Obtenido de http://grupoelcomercio.com/index.php/informacion-corporativa/filosofia-empresarial

GuilleSQL. (2007). *Windows Storage Server 2008 (WSS 2008) y Microsoft iSCSI Software Target v3.2, disponibles para descarga en MSDN*. Obtenido de http://www.guillesql.es/Noticias/Windows_Storage_Server_2008_WSS_Microsoft_iSCSI_Software_Target_32_SAN.aspx

Hernandez Zapardiel, I. (s.f.). *Métodos y políticas de respaldo (backup) en planes de contingencia.* Obtenido de http://benjamin.davy.free.fr/Auditoria/ContingenciaybackupenSI.pdf

Iamateche. (2014). *Almacenamiento en red*. Obtenido de http://www.iamatechie.com/post-series-on-network-attached-storage/282

Informática Moderna. (02 de Enero de 2015). *El servidor para Redes / Server*. Obtenido de http://www.informaticamoderna.com/Servidor.htm

InformaticaModerna. (3 de Abril de 2015). *El respaldo de datos - Backup de datos*. Obtenido de http://www.informaticamoderna.com/Backup.htm

InfoWorld. (2008). *¿Está preparado para la migración de servidores?* Obtenido de http://www.iworld.com.mx/iw_Opinions_read.asp?IWID=99

Instituto Nacional de estadísticas e información. (2001). *Guía Práctica para el desarrollo de Planes de Contingencia de Sistemas de Información.* Obtenido de http://www.ongei.gob.pe/seguridad/seguridad2_archivos/Lib5131/Libro.pdf

Jarrin, V. H. (Julio de 2010). *TELEPROCESO,SERVIDOR DE ARCHIVOS,CLIENTE SERVIDOR.* Obtenido de https://sisandes.wordpress.com/2010/07/09/6/

Jiménez, L. (Marzo de 2009). *Guía de Desarrollo de un Plan de Contingencia de Negocio.* Obtenido de http://www.criptored.upm.es/guiateoria/gt_m001r.htm

Kioskea.net. (Junio de 2014). *Redes - Arquitectura Cliente/Servidor en 3 niveles.* Obtenido de http://es.ccm.net/contents/147-redes-arquitectura-cliente-servidor-en-3-niveles

Márquez Avendaño, B. M. (03 de Mayo de 2013). *Cliente servidor.* Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/marquez_a_bm/capitulo5.pdf

Maryuri, C. (2008). *Servidores y sus Tipos*. Obtenido de http://servidoresysustipos.blogspot.com/

Microsoft. (2015). *Windows Server 2003 Standard Edition*. Obtenido de http://www.microsoft.com/spain/windowsserver2003/evaluation/overview/standard.mspx

Microsoft. (2015). *Windows Storage Server 2008 R2*. Obtenido de https://technet.microsoft.com/en-us/library/gg232660(v=ws.10).aspx

Ministerio de Educación, cultura y Deporte de España. (28 de Agosto de 2009). *Synkron*. Obtenido de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/734-synkron

Ministerio de Energía y Minas Perú. (2015). *Plan de Contingencias.* Obtenido de http://www.minem.gob.pe/minem/archivos/file/DGGAE/ARCHIVOS/estudios/EIAS%20-%20hidrocarburos/EIA/EIA%20LOTE%20138/VOL%20IV%20PLAN%20DE%20MANEJO%20AMBIENTAL/Cap%207.0%20Plan%20de%20Contigencias.pdf

Mundo NAS. (2011). *Sistemas Operativos gratuitos para montar un NAS a medida*. Obtenido de http://www.mundonas.com/2013/07/sistemas-operativosgratuitos-para.html

Nanosystemns. (2016). *Uranium Backup Free*. Obtenido de http://www.uranium-backup.com/es/uranium-backup-free/

Nanosystems S.r.l. . (2015). *¿POR QUÉ URANIUM?*

Nanosystems S.r.l. . (2015). *Precios Uranium Backup*. Obtenido de http://www.uranium-backup.com/es/comprar-uranium-backup/

Nanosystems S.r.l. . (2015). *URANIUM BACKUP*. Obtenido de http://www.uranium-backup.com/es/

Net Humans S.A. (2013). *Sistemas de bases de datos*. Obtenido de http://www.nethumans.com/solutions/development/Database.aspx

NETGLOBALIS. (26 de Diciembre de 2012). *Métodos de respaldo de información*. Obtenido de http://www.netglobalis.net/blog/metodos-de-respaldo-de-informacion/

Osiatis S.A. (2015). *Gestión de la Continuidad de los Servicios TI*. Obtenido de http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti/evaluacion_riesgos.php

Redessil. (2015). *Instalacion de servidor de archivos*. Obtenido de http://www.redessil.com/instalacion-de-servidor-de-archivos/

Sánchez Garreta, J. S. (2003). *Ingeniería de proyectos informáticos: Actividades y procedimientos.* Castellón de la PLana: Universitas.

Sánchez Garreta, J. S. (2003). *Ingeniería de proyectos informáticos: Actividades y procedimientos.* Castellón de la PLana: Universitas.

Studija, R. (2007). *Sistema de Archivos - Modelo Jerárquico*. Obtenido de http://sistemasoperativos.angelfire.com/html/5.7.html

TechTarget S.A. (2012). *Elegir un sistema de almacenamiento en red (NAS) de gama media*. Obtenido de http://searchdatacenter.techtarget.com/es/consejo/Elegir-un-sistema-de-almacenamiento-en-red-NAS-de-gama-media

Ureña Gómez, F. (26 de Septiembre de 2012). *Rutas relativas y absolutas*. Obtenido de http://www.discoduroderoer.es/rutas-relativas-y-absolutas/#

Veeam. (2015). *Veeam Backup & Replication v8*. Obtenido de https://www.veeam.com/es-lat/vm-backup-recovery-replication-software.html

Vergara, J. (23 de 04 de 2004). *Operaciones con directorios*. Obtenido de http://lsub.org/ls/export/pfc_pfs/node9.html

Vision Solutions. (2015). *Double Take Move*. Obtenido de https://world.visionsolutions.com/Products/DT-Avail.aspx

Wikipedia. (30 de Noviembre de 2015). *RAID*. Obtenido de https://es.wikipedia.org/wiki/RAID

ANEXOS