UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES PARA LA ELABORACIÓN DEL PLAN DE CONTINGENCIA IT DE LA COMPAÑÍA LA CASA DEL CABLE S.A.

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: William Andrés Moscol Criollo

TUTOR: Ing. César Eras

GUAYAQUIL – ECUADOR
2016

REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO: "Identificación de amenazas y vulnerabilidades para la elaboración del plan de contingencia IT de la compañía LA CASA DEL CABLE S.A."		
	REVISORES:	
INSTITUCIÓN: Universidad de Guayaquil	**FACULTAD: Ciencias Matemáticas y Físicas**	
FECHA DE PUBLICACIÓN: Abril 2016	**N° DE PÁGS.: 108**	
ÁREA TEMÁTICA: Seguridad informática.		
PALABRAS CLAVES: Elaboración del plan de contingencia IT, Veeam 8.0, Retrospect, respaldos, réplica de datos.		
RESUMEN: Casa del Cable S.A. en la actualidad cuenta con aplicaciones para la seguridad de la información pero no se encuentra documentado el proceso a seguir durante una contingencia del Departamento de sistemas, con la elaboración del mismo se puede solventar cualquier error de las aplicaciones críticas de la compañía.		
N° DE REGISTRO(en base de datos):	**N° DE CLASIFICACIÓN: Nº**	
DIRECCIÓN URL (tesis en la web):		
ADJUNTO PDF	[X] **SI**	[ ] **NO**
CONTACTO CON AUTOR: William Andrés Moscol Criollo	**Teléfono:** 0989580765	**E-mail:** William.moscol@outlook.com
CONTACTO DE LA INSTITUCIÓN	**Nombre: Ab. Juan Chavez**	
	Teléfono: 2307729	

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación, **"Identificación de amenazas y vulnerabilidades para la elaboración del plan de contingencia IT de la compañía LA CASA DEL CABLE S.A:"** elaborado por el Sr. William Andrés Moscol Criollo, alumno no titulado de la Carrera de Ingeniería en Sistemas Computacionales, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

Ing. César Eras, Msc.

DEDICATORIA

Dedico este trabajo a Dios por brindarme la salud y fuerzas para llegar a culminar mis estudios de tercer nivel.

A mi familia por brindarme sus consejos, en especial a mi madre que desde el cielo es mi guía, y su mayor anhelo es verme como Ingeniero en Sistemas.

AGRADECIMIENTO

Agradezco infinitamente a Dios por dotarme de sabiduría, fortaleza y perseverancia para cumplir cada una de mis metas planteadas.

A mi familia y a mi novia por brindarme sus consejos y apoyo ante todas las dificultades.

A mi tutor, Ing. Cesar Eras M. Sc. por la dedicación y apoyo brindado para lograr mi formación profesional

Mi agradecimiento sincero a todos los que conforman la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil por dar apertura a la unidad de proyectos de titulación y llegar con la propuesta en beneficios de todos.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, Msc.
DECANO DE LA FACULTAD CIENCIAS MATEMATICAS Y FISICAS

Ing. Inelda Martillo Alcívar, Mgs
DIRECTORA
CISC

Ing. César Eras, Msc
DIRECTOR DEL PROYECTO DE TITULACIÓN

Lcdo. Jorge Alvarado Chang
PROFESOR DEL ÁREA - TRIBUNAL

Ing. Viviana Pinos
PROFESOR DEL ÁREA – TRIBUNAL

Ab. Juan Chávez Atocha
SECRETARIO

DECLARACIÓN EXPRESA

“ La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL”

WILLIAM ANDRES MOSCOL CRIOLLO

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

"IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES PARA LA ELABORACIÓN DEL PLAN DE CONTINGENCIA IT DE LA COMPAÑÍA LA CASA DEL CABLE S.A."

Proyecto de titulación que se presenta como requisito para optar por el título de INGENIERO EN SISTEMAS COMPUTACIONALES

Autor: William Andrés Moscol Criollo

C.I. 0926629668

Tutor: Ing. Cesar Eras M. Sc.

Guayaquil, Abril del 2016

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por el estudiante WILLIAM ANDRES MOSCOL CRIOLLO, como requisito previo para optar por el título de Ingeniero en sistemas computacionales cuyo problema es:

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES PARA LA ELABORACIÓN DEL PLAN DE CONTINGENCIA IT DE LA COMPAÑÍA LA CASA DEL CABLE S.A.

Considero aprobado el trabajo en su totalidad.

Presentado por:

Moscol Criollo William Andrés C.I. 0926629668

Tutor: Ing. César Eras

Guayaquil, Abril del 2016

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

Nombre Alumno: William Andrés Moscol Criollo	
Dirección: Guayaquil, Cdla Huancavilca Mz. 13 Solar 1	
Teléfono: 0989580765	**E-mail:** William.moscol@outlook.com

Facultad: Física y matemáticas
Carrera: Ingeniería en Sistemas computacionales
Proyecto de titulación al que opta: Ingeniero en Sistemas Computacionales
Profesor tutor: Ing. Cesar Eras M.

Título del Proyecto de titulación: Identificación de amenazas y vulnerabilidades para la elaboración del plan de contingencia IT de la compañía LA CASA DEL CABLE S.A.

Tema del Proyecto de Titulación: Identificación de amenazas y vulnerabilidades para la elaboración del plan de contingencia IT de la compañía LA CASA DEL CABLE S.A.

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica:

Inmediata	**x**	Después de 1 año	

Firma Alumno:

3. Forma de envío:

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM [x] CDROM [ ]

ÍNDICE GENERAL

ABREVIATURAS

CDC	Casa del Cable
UG	Universidad de Guayaquil
BD	Base de Datos
Msc.	Master
IT	Tecnología de la información
DRP	Plan de recuperación de desastres
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas
ITIL	Biblioteca de Infraestructura de Tecnologías de Información
WSUS	Windows System Updates Services
LAN	Local Area Network
DNS	Domain Name System
AD	Active Directory
IP	Internet Protocol
TI	Tecnologías de la Información
IPS	Intrusion Prevention System

INDICE DE CUADROS

INDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

“IDENTIFICACION DE AMENAZAS Y VULNERABILIDADES PARA LA ELABORACION DEL PLAN DE CONTINGENCIA IT DE LA COMPAÑÍA LA CASA DEL CABLE S.A.”

Autor: William Andres Moscol Criollo

Tutor: Ing. Cesar Eras

RESUMEN

En la actualidad tener un respaldo de la información o una contingencia de la plataforma de sistemas de una empresa no se debe pasar por alto, la seguridad de la información es un aspecto relevante en estos tiempos por lo que es necesario implementar soluciones de contingencia y así mitigar tiempos de errores de las aplicaciones y procesos. Este proyecto de titulación tiene como objetivo principal documentar el proceso de contingencia IT de la compañía LA CASA DEL CABLE S.A., basado en la metodología de investigación de proyecto factible ya que el mismo quedará operativo y documentado posterior a las pruebas a realizarse mensual o trimestralmente. Existen varias herramientas en el mercado que nos permiten tener una réplica de nuestros datos y copias de seguridad, para este proyecto se utilizará el software Retrospect 9.0 para respaldos de usuarios y el software Veeam 8.0 para copias de seguridad de los datos del servidor y réplica de datos en un sitio alterno, de esta manera se controla las vulnerabilidades en el tema de copias de seguridad que era un tema preocupante para la empresa debido a su historial de pérdida de información.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

"Identification threats and vulnerabilities for drawing up the contingency plan IT for company CASA DEL CABLE S.A.

Autor: William Andres Moscol Criollo

Tutor: Ing. Cesar Eras M.

ABSTRACT

In the News have a backup of the information or a contingency platform systems of a company cannot be overlooked, the Information Security is an important aspect in these times for what is needed to implement contingency solutions and so Errors mitigate time applications and processes. This project's main objective is qualification document the process of IT contingency Company CASA DEL CABLE S.A., based on Research Methodology feasible project since it documented Left Operating and subsequent testing be conducted monthly or quarterly. There are several tools on the market that allow us to mirror our data and backups, for project Retrospect 9.0 Backup software will be used for Users and software for Veeam Backup 8.0 Data Server and replication Data on alternative site UN Control of this way if vulnerabilities on the issue of backups that was the subject of UN for worrying the company because one its history information loss.

INTRODUCCIÓN

El plan de contingencia IT o plan de continuidad del soporte proporciona a la empresa una guía que incluye procedimientos y capacidades para recuperar una aplicación principal o un sistema de soporte general. Se enfoca en el desarrollo y mantenimiento de los planes de continuidad del negocio. (Areitio, 2008)

El presente proyecto trata acerca del diseño de un plan de contingencia IT para la empresa Casa del Cable S.A., con matriz ubicada en la ciudad de Guayaquil. Se espera presentar uno de los temas principales del área de sistemas, debido a que en base a éste, se lleva a cabo el desarrollo de muchas actividades que servirán en la empresa como medio para el ahorro de recursos físicos y monetarios.

La empresa Casa del Cable S.A. se dedica a la importación y comercialización de herramientas y materiales para conectividad, eléctricos, sistemas de seguridad, entre otros. Su facturación es diaria, y mantiene 2 sucursales una en Guayaquil y otra en Quito. La falta de un plan de contingencia IT en esta empresa, ha ocasionado serios problemas en el desenvolvimiento normal del negocio, por lo cual es imperiosa su aplicación en la misma.
El proyecto se lo desarrollará en la matriz de la ciudad de Guayaquil, solo cubre la ciudad mencionada.

En los capítulos siguientes se definirá los puntos clave para el desarrollo del plan de contingencias IT y la forma en la cual será aplicado, además de las características particulares de su aplicación.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

Ubicación del Problema en un Contexto

Las empresas diseñan planes de contingencia informáticos de acuerdo a sus necesidades básicas, según su experiencia respecto a eventos pasados, y posibles situaciones futuras. La necesidad de resguardar la información, exige a las empresas prever situaciones de catástrofe y delinear estrategias de reacción. Sin embargo, es preciso realizar evaluaciones continuas, según las respuestas obtenidas en la aplicación de dichos planes; lo cual, debería documentarse para conocer las amenazas y vulnerabilidades resultantes.

Los planes de contingencia que levantan las empresas, no son en su mayoría los más efectivos, ya que si bien no es tan probable que la empresa caiga en una catástrofe de gran extensión, suele considerarse menos remoto el hecho de sufrir mínimas incidencias, en las que si no se cuenta con medios previsores, se convertirán en serios problemas.

Un sistema operativo aprende de las agresiones y mejora en base a las necesidades. No actualizarlo supone dejar tu dispositivo desnudo ante las contingencias. (ABC, 2015)

La empresa Casa del Cable S.A. se dedica a la importación y comercialización de herramientas y materiales para conectividad, eléctricos, sistemas de seguridad, entre otros. Su facturación es diaria, y mantiene 2 sucursales una en Guayaquil y otra en Quito. Esta empresa, cuenta con los equipos para

actuar frente a inconvenientes informáticos, pero no tiene documentado un plan de contingencia IT, y tampoco mantienen registros de los problemas suscitados y su resolución.

Cuando hablamos de plan de contingencia, no es solamente el proceso de respaldo de la base de datos; más bien, es definir los riesgos que tiene el departamento IT, y cómo tenemos pensado enfrentarlos, no esperamos que suceda la crisis para recién empezar, y tener presente los actores, recursos, métodos y tiempos calculados para superar la crisis en el menor tiempo posible.

Por lo antes expuesto, es necesario que en Casa del Cable S.A. se documente la información del planta de contingencias IT y a su vez se evalúen las diferentes amenazas y riesgos, en las que podría caer la empresa en base al plan actual. Además su posterior propuesta de la planificación para la mejora continua del plan.

Situación Conflicto Nudos Críticos

Actualmente la empresa Casa del Cable S.A. no tiene documentado ni ha tomado las acciones necesarias para la definición del plan de contingencia IT, por lo que al presente no se cuenta con registros al día de las emergencias suscitadas, y se desconocen los riesgos que presenta el plan, que sirven como base para las mejoras futuras.

La valoración de riesgos es una parte fundamental del proceso de planificación de contingencias de las TIC. No se puede proteger un sistema sino se conoce contra qué o contra quién tienen que protegerse. Una vez conocidos los riesgos, ya se pueden planificar las políticas y las tecnologías necesarias para reducirlos, con lo que se consigue aumentar la seguridad. (Areitio, 2008)

Si bien realizar una evaluación de riesgos del plan de contingencia IT implica el uso de muchos recursos, es una tarea indispensable dentro de las medidas de seguridad de la empresa. La evaluación inadecuada de los riesgos o la falta de éste, no permite identificar los conflictos a los que se expone el desarrollo normal de la empresa.

Causas y Consecuencias del Problema

CUADRO No. 1

CAUSAS Y CONSECUENCIAS DEL PROBLEMA

CAUSA	CONSECUENCIA
Pérdida de conectividad entre cliente - Servidor	Pérdida de tiempo en atención al cliente.
Falla de Servidor	Malestar en los usuarios y clientes
Pérdida del servicio de internet	Retraso en pagos a proveedores.
Daño Físico en el Datacenter	Pérdida de información
Daños de hardware por fluido eléctrico	Pérdida de datos
Daños de hardware por fluido eléctrico	Fuente de poder del hardware sin encender
Equipos de telecomunicación sin encender	Pérdida de enlace de datos a nivel nacional

Elaborado por: William Moscol Criollo

Delimitación del Problema

El desarrollo del presente proyecto partirá en documentar el plan de contingencia IT y saber actuar ante la ausencia total del servicio IT en la empresa Casa del Cable S.A. en el caso del corte de fluido eléctrico.

Este proyecto se aplicará específicamente al departamento de sistemas de la empresa, ubicado en la matriz en Guayaquil.

Se incluirán diseños del ambiente de contingencia, además de un plan de actividades que se ejecutarán a medida de la aplicación del mismo. Se tomarán

en cuenta los cambios a nivel de usuarios, cuando se vaya del ambiente normal hacia el de contingencia y viceversa.

Formulación del Problema

Es importante identificar claramente cuáles son los riesgos y amenazas de fluido eléctrico a los que es propenso en la actualidad el servicio IT de la empresa Casa del Cable S.A., así también es preciso levantar de forma documental la evolución del mismo, la aplicación ejecutada, y su evaluación respecto de éstas. De tal manera, que la empresa cumpla con medidas de seguridad para futuras contingencias reales que podrían suscitarse en base a la evaluación realizada.

En base a este problema, se ha planteado la siguiente interrogante:

¿En qué medida un plan de contingencia puede reducir el impacto producido por las fallas eléctricas en el hardware de la compañía CASA DEL CABLE S.A.?

Evaluación del Problema

La empresa Casa del Cable S.A. es una de las principales importadoras y comercializadoras del país en las líneas de herramientas de conectividad, tiene una matriz y dos sucursales, una dentro y otra fuera de la ciudad. La venta asciende a la emisión de 200 facturas por día.

El departamento de sistemas de la empresa, está conformado por un técnico de la empresa Ondú Soluciones Tecnológicas, la cual presta servicios de help desk IT, al no ser una dependencia adscrita a la matriz, tenemos como una de sus debilidades, la vulnerabilidad por los cambios de personal, y como ventaja la facilidad para la resolución de problemas debido a la experiencia de la empresa.

El soporte IT de la empresa cuenta con un plan de contingencia, el mismo que no ha sido documentado aún, ni evaluado respecto de las respuestas efectivas y no efectivas al momento de presentarse las contingencias.

Los aspectos generales de evaluación para el enunciado problema en esta empresa son:

Delimitado:
La empresa Casa del Cable S.A. mantiene vulnerabilidad respecto de crisis en los servicios IT, por la falta de métodos planificados para las resoluciones de posibles contingencias.

Evidente:
Los servicios IT representan un factor indispensable para el normal desempeño del negocio; a falta de estos, los usuarios podrían quedarse mucho tiempo sin poder desarrollar las actividades comerciales de la empresa, lo cual podría traducirse en pérdidas económicas.

Concreto:
El desarrollo del proyecto concibe como objetivo principal establecer el plan de contingencias IT de la empresa Casa del Cable S.A., identificando las amenazas y vulnerabilidades de fluido eléctrico a las que está expuesto actualmente, procurando su mejoramiento para beneficio de la empresa y de los usuarios.

Relevante:
La importancia de la aplicación del presente proyecto en la empresa Casa del Cable S.A., radica en la prevención de pérdidas que pudieren originarse a raíz de cualquier eventualidad imprevista de perdida de fluido eléctrico; éstas pérdidas serían tanto de tiempo, recursos y por ende económicas.

Contextual:
El presente estudio conlleva al desarrollo y aplicación de los conocimientos adquiridos en la carrera, y uno de los puntos clave a los que estamos expuestos los profesionales del área de sistemas, debido a que el buen diseño y aplicación de los planes de contingencia IT simbolizan uno de los pilares fundamentales del departamento de sistemas en una empresa.

Factible:

La empresa Casa del Cable S.A. cuenta con los recursos necesarios para llevar a cabo el desarrollo del plan de contingencia IT, este estudio planea diseñar el plan, evaluando riesgos y amenazas de fluido eléctrico a lo que se expone la empresa. En los capítulos siguientes se definirá el uso de cada uno, y la factibilidad del presente proyecto.

Variable:

Variable dependiente:

- Plan de contingencia: documentación y pasos a seguir durante una amenaza de corte de servicio eléctrico
- Impacto: se mide el impacto por las fallas eléctricas en la empresa Casa del Cable S.A.

Variable Independiente:

- Amenazas: en el proyecto nos vamos a enfocar en el tipo de amenazas de fluido eléctrico que es lo que ha pasado en anteriores ocasiones y no saber actuar ante la eventualidad. En los capítulos siguientes se definirá el uso de cada uno, y la factibilidad del presente proyecto.

OBJETIVOS

Objetivo General

Establecer el plan de contingencias IT de la empresa Casa del Cable S.A., identificando las amenazas y vulnerabilidades a nivel de hardware de tipo fluido eléctrico a las que está expuesto actualmente, procurando su mejoramiento para beneficio de la empresa y de los usuarios.

Objetivos Específicos

- Identificar riesgos y debilidades a lo que está expuesto la empresa en el caso de un corte de fluido eléctrico y establecer los pasos a seguir en el manual para la continuidad del negocio.

- Definir el diseño de un ambiente de réplica de datos de las aplicaciones críticas SIAC y base de datos de la empresa.

- Presentar las mejoras resultantes de la aplicación basado en los estándares IT NORMA ISO 22301.

- Documentar el plan de recuperación de desastres de las aplicaciones SIAC y controlador de dominio.

ALCANCES DEL PROBLEMA

En base a reuniones con los administradores de la empresa Casa del Cable S.A. se definirán el producto a entregarse posterior al presente proyecto. En los próximos capítulos se analizarán con detalle los entregables que forman parte de este alcance. Se definen dentro del alcance los siguientes resultados:

- Diseños previos del plan de contingencia IT
  Se considera como criterio de aceptación el informe inicial para su aplicación, evidencias del proceso, documentación técnica del hardware y software implementado, y sus configuraciones.

- Elaboración del plan de contingencia IT
  Se considera como criterio de aceptación la documentación completa del plan, que incluirá:
  Alcance
  Supuestos
  Excepciones
  Roles
  Responsabilidades
  Procedimientos de aplicación
  Plan de pruebas
  Mejoras al plan
  Monitoreo

- Capacitación al personal del departamento de sistemas
  Se considera como criterio de aceptación la entrega de un certificado de capacitación, que garantizará el nivel de conocimiento del personal.

- Pruebas iniciales del plan de contingencia IT
  Se considera como criterio de aceptación la entrega de informes que evidencies los análisis y evaluaciones realizadas, con las firmas de los usuarios pertinentes.

- Entrega final del proyecto
  Se considera como criterio de aceptación el informe por la entrega total de la documentación del plan de contingencia IT de la empresa Casa del Cable S.A., tanto de detalle de los recursos usados, las evidencias de elaboración del plan, las capacitaciones, y pruebas realizadas para su ejecución.

JUSTIFICACIÓN E IMPORTANCIA

El departamento de sistemas, de la empresa Casa del Cable S.A. cuenta con herramientas de respaldo de información, las cuales soportan solamente riesgos inherentes a daños o pérdidas de la información; sin embargo, existen innumerables riesgos y amenazas para los cuales no están preparados en la empresa.

Es imperioso tomar medidas para el correcto funcionamiento del mismo, procurando resultados eficaces y eficientes, evitando perjudicar el normal desarrollo de las actividades comerciales y operativas dentro de las diferentes áreas de trabajo, tanto en la planta central como en las sucursales.

La valoración de riesgos es una parte fundamental del proceso de planificación de contingencias de las TIC. No se puede proteger un sistema sino se conoce contra qué o contra quién tienen que protegerse. Una vez conocidos los riesgos, ya se pueden planificar las políticas y las tecnologías necesarias para reducirlos, con lo que se consigue aumentar la seguridad. (Areitio, 2008)

En el año 2011, la empresa Casa del Cable S.A. sufrió un incidente con el servidor principal de la matriz, lo cual representó en los usuarios el reingreso de información que tardó seis meses en completarse. Es por este motivo que urge a la empresa a evaluar su situación actual frente a nuevos peligros que podrían suscitarse en los próximos años.

La aplicación del presente proyecto llevará a la empresa a un desarrollo de sus actividades de forma segura, procurando el ahorro de recursos físicos y monetarios, mediante la disminución de tiempos de restauración de servicios y el respaldo oportuno de la información.

METODOLOGÍA DEL PROYECTO

La metodología a utilizarse en el desarrollo de este proyecto es la Ex Post Facto, la cual se basa en analizar acontecimientos ya ocurridos en el área de sistemas.

Se basará en un diseño analizando la situación actual de Casa del Cable S.A., comparándolo con las alternativas de tecnología y estándares actuales y vigentes para buscar el diseño adecuado que se ajuste a la solución del problema.

En el desarrollo del proyecto también se definió usar la técnica de entrevista con un cuestionario 8 preguntas abiertas dirigidas a los jefes del área de dirección administrativa, gerencia general y al departamento de sistemas de la compañía CASA DEL CABLE S.A.

Se definió entrevistar a los jefes de área mencionado ya que conocen la problemática de la compañía y el personal de las áreas de contabilidad, administración, importaciones, bodega y comercial reportan directamente a la dirección administrativa y este a su vez transmite a gerencia general y al departamento de sistemas, por tal motivo la problemática ya existía y los jefes de área la conocían.

Investigación Ex Post Facto

Experimento post-facto quiere decir, simplemente, experimento que se realiza después de los hechos. Por su método no se trata de un verdadero experimento, pues en él el investigador no controla ni regula las condiciones de la prueba, pero sí puede considerárselo como tal si nos atenemos al procedimiento lógico de que se vale, que es idéntico al de los experimentos propiamente dichos.

Es apropiado cuando se desea establecer la causa efecto de los fenómenos ya ocurridos y es necesario determinar los factores que intervinieron para que se pudieran ocasionar.

La investigación "ex post facto" tiene como objetivo la validación de las hipótesis una vez que el fenómeno ya ha tenido lugar. Por consiguiente, se trata de una búsqueda "retrospectiva" de las posibles causas que han producido tal fenómeno que hemos estudiado.

Es un tipo de investigación aplicable cuando no podemos producir directamente un fenómeno (o, simplemente, no es conveniente hacerlo).

Por lo tanto, una vez que se produce el hecho -sin la intervención del investigador- se analizan las posibles causas y consecuencias.

Los estudios " post facto" engloban la mayoría de los métodos que se incluyen dentro de la investigación descriptiva (estudios de casos, correlacionales, de desarrollo, método clínico, encuestas, investigación evaluativa, investigación histórica, etc.). Es decir, prácticamente todos aquellos estudios que no son experimentales. **(Urriola, 2010)**

Diseño de la Investigación

Para obtener la información que permita realizar de manera excelente un plan de contingencia IT de las aplicaciones críticas se realizará una **investigación proyectiva** con la finalidad de analizar situaciones o problemas en un ambiente determinado, para finalmente elaborar el modelo que nos guie a la solución del problema.

Investigación Proyectiva

La investigación proyectiva es una modalidad de la ciencia determinada por el propósito de elaborar propuestas susceptibles de ser llevadas a feliz término. Constituye una de las modalidades de la investigación, de singular importancia, dada la necesidad que siempre existe de proponer soluciones a problemas, así como también por el reclamo de creadores, promotores e innovadores de contar con formas científicas y académicas que les permitan comprometerse con iniciativas que amparen su creatividad y propósito de originalidad.

Siempre ha habido propuestas. Sin embargo la manera de hacer coincidir la intención de formalizarlas, con la investigación, con mayor precisión metodológica, es relativamente cercana. La investigación proyectiva se aprecia como un aporte de la planificación y un mérito de todo creativo, de todo innovador, de todo visionario que con su empeño, empuje y decisión desarrolla maneras destinadas a dar cuenta de sus sueños y propósitos.

Académicamente hablando, la investigación proyectiva constituye un modo de hacer ciencia muy apreciado en estudios de pre y de postgrado. Además, corresponde a un esfuerzo de mayor complejidad cuando a la hora de sincerar las propuestas se hace en toda institución, contexto y organización un esfuerzo intelectual destinado a honrar este propósito. **(Morales, 2013)**

Entre otros tipos de investigación que vamos a utilizar de manera secundaria serían:

Investigación Exploratoria

Busca determinar el mejor diseño de la investigación, el método de recogida de datos y la selección de temas. Debe sacar conclusiones definitivas. Este tipo de investigación se aplicará a este proyecto, puesto que es necesario que se establezca una estructura para el trabajo y que, de esta manera, exista orden y sobre todo que se logre el objetivo planteado. **(Ontiveros, 2014)**

Investigación Descriptiva

Según (Rivas, 1995), se “trata de obtener información acerca del fenómeno o proceso, para describir sus implicaciones”. (p.54). Este tipo de investigación se ocupa de la descripción de hechos a partir de un criterio o modelo teórico definido previamente. En la investigación se realiza un estudio descriptivo que permite poner de manifiesto los conocimientos teóricos y metodológicos del autor, para darle solución al problema a través de información obtenida de la Institución. Este tipo de investigación es indispensable de aplicar, debido a la gran cantidad de definiciones que son necesarias explicar para que la interpretación de los conceptos sea de total entendimiento para quien lee este trabajo.

Investigación de Campo

La investigación de campo según (Arias, 2006) “consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variables alguna”. Los datos necesarios para llevar el desarrollo del trabajo, se han obtenidos directamente del sitio donde se realiza la investigación.

Investigación Cualitativa y Cuantitativa

La investigación cuantitativa es de índole descriptiva y la usan los investigadores para comprender los efectos de los diversos insumos promocionales en el consumidor, dándoles así a los mercadología la oportunidad de predecir el comportamiento del consumidor. Estos consisten en observación, experimentación y técnicas de encuestas, se usan muestras probabilísticas. Mientras que la investigación cuantitativa consiste en entrevistas de profundidad, por lo cual se tienen a ser un procedimiento subjetivo, se tratará de percibir el comportamiento del consumidor, estas entrevistas no se realizan a muestras grandes; sin embargo, tiene una función importante para las futuras tomas de decisiones. **(Schiffman & Kanuk, 2005)**

TÉCNICAS UTILIZADAS EN LA INVESTIGACIÓN

Entre las técnicas a utilizarse en este proyecto tenemos:

Entrevista

Es la técnica ideal para la recopilación de datos, con el objetivo de obtener varios puntos de vista técnicos del área de sistemas, así como de los responsables de las relaciones entre el área de tecnología informática y las diferentes áreas de procesos del negocio. Las entrevistas serán de tipo (directa), se plantean en conocer las tecnologías instaladas actualmente en Casa del Cable S.A., con las que se brindan los servicios de IT en general.

Cuestionario

Se planea usar los cuestionarios para recopilación de información cualitativa, con preguntas abiertas o con una gama de opciones que parten desde el problema objeto de esta investigación. Servirán de guía para las entrevistas, ya que los mismos dejarán percibir conceptos y aplicaciones de los mencionados. Serán aplicables a las mismas personas sobre las cuales se aplicará la técnica de entrevista.

Observación

Será utilizada con el objetivo de obtener información de lo instalado actualmente y lo recogido con las entrevistas y lo que realmente se aplica.

Inspección de registros

Esta técnica de inspección de registros es considerada como notable en esta investigación, ya que Casa del Cable S.A. poseen políticas internas, reglamentación y procedimientos en las diferentes áreas. Existe también la necesidad de recopilar y analizar los sistemas existentes, su funcionamiento, configuración e información de registros.

Una vez obtenida la información a través de las técnicas mencionadas anteriormente, debemos validar la información y datos recopilados para lo cual utilizaremos:

- Análisis documental
- Análisis descriptivo

Análisis documental

Constituye el punto de entrada a la investigación e incluso en muchas ocasiones, es el origen del tema o problema de investigación. Los documentos fuente pueden ser de naturaleza diversa: personales, institucionales o grupales, formales o informales. A través de ellos es posible obtener información valiosa para lograr el encuadre al que hicimos referencia antes. Dicho encuadre incluye, básicamente, describir los acontecimientos rutinarios así como los problemas y reacciones más usuales de las personas o cultura objeto de análisis, así mismo, conocer los nombres e identificar los roles de las personas clave en esta situación sociocultural. Revelar los 66 Investigación cualitativa intereses y las perspectivas de comprensión de la realidad, que caracterizan a los que han escrito los documentos. El análisis documental se desarrolla en cinco acciones, a saber: Rastrear e inventariar los documentos existentes y disponibles; y clasificar los documentos identificados; Seleccionar los documentos más pertinentes para los propósitos de la investigación; Leer en profundidad el contenido de los documentos seleccionados, para extraer elementos de análisis y consignarlos en "memos" o notas marginales que registren los patrones, tendencias, convergencias y contradicciones que se vayan descubriendo; Leer en forma cruzada y comparativa los documentos en cuestión, ya no sobre la totalidad del contenido de cada uno, sino sobre los hallazgos previamente realizados, a fin de construir una síntesis comprensiva total, sobre la realidad humana analizada. (Peña, 2006)

Análisis descriptivo

Es necesario hacer notar que los estudios descriptivos miden de manera más bien independiente los conceptos o variables con los que tienen que ver. Aunque, desde luego, pueden integrar las mediciones de cada una de dichas

variables para decir cómo es y se manifiesta el fenómeno de interés, su objetivo no es indicar cómo se relacionan las variables medidas. Por ejemplo, un investigador organizacional puede pretender describir varias empresas industriales en términos de su complejidad, tecnología, tamaño, centralización y capacidad de innovación. Entonces las mide en dichas variables y así puede describirías en los términos deseados. A través de sus resultados, describirá qué tan automatizadas están las empresas medidas (tecnología), cuánta es la diferenciación horizontal (subdivisión de las tareas), vertical (número de niveles jerárquicos) y espacial (número de centros de trabajo y el número de metas presentes en las empresas, etc.); cuánta libertad en la toma de decisiones tienen los distintos niveles y cuántos tienen acceso a la toma de decisiones (centralización de las decisiones); y en qué medida pueden innovar o realizar cambios en los métodos de trabajo, maquinaria, etc., (capacidad de innovación). Sin embargo, el investigador no pretende analizar por medio de su estudio si las empresas con tecnología más automatizada son aquellas que tienden a ser las más complejas (relacionar tecnología con complejidad), ni decimos si la capacidad de innovación es mayor en las empresas menos centralizadas (correlacionar capacidad de innovación con centralización (Sampieri, 1997).

Procesamiento y análisis de la información

La información obtenida a través de la técnica de entrevista, será ingresada y desglosada en modelos, las mismas que deberán poder darnos a conocer los estándares aplicados en Casa del Cable S.A referente a las tecnologías que usan actualmente e identificar las necesidades para garantizar la disponibilidad de los servicios críticos

La información obtenida bajo la técnica de inspección de registros, deberá ser documentada y explicada en términos de documentación técnica y marco delimitador de lo que se posee actualmente, en el caso de la inspección de registros y configuración de los sistemas, frente a lo que se quiere llegar y que está definido en las políticas y procedimientos de los estándares organizacionales referentes al tema de investigación.

A nivel general nos basaremos bajo los siguientes temas durante la investigación:

• Infraestructura de hardware y aplicaciones de software en los que se basan actualmente los servicios IT para beneficio de los usuarios.

• Servicios y herramientas de alta disponibilidad de servicios IT instalados actualmente.

• Estándares organizacionales que hacen referencia a la alta disponibilidad, planes de contingencia y ambientes utilizados.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DEL ESTUDIO

El área IT (Tecnología de la información), es considerada una de las más críticas en una compañía, así mismo la forma de protegerlas, por tal razón son aspectos indudablemente para la continuidad del negocio de la compañía.
Al hablar de Plan de contingencia IT no es un proceso de respaldo de base de datos e información, cuando hablamos de plan de contingencia, es definir los riesgos que tiene el departamento IT y como tenemos pensado enfrentarlos, no esperar que pase la crisis para recién recurrir al “que hacer”, y tener presente los actores, recursos, métodos y tiempos calculados para superar la crisis en el menor tiempo posible.

El plan de contingencias de IT, es una herramienta elaborada de forma planificada, que contiene las acciones, decisiones y eventos que ayudará a recuperar, a pesar de la ocurrencia de una falla, aunque sea en parte los procesos críticos de una organización, manteniendo la capacidad funcional del sistema afectado, entendiendo por recuperación, tanto la capacidad de seguir trabajando en un plazo mínimo después de que se presenta un problema, como la posibilidad de volver a la situación inmediatamente anterior al mismo, habiendo remplazo o recuperando el máximo posible de recursos informáticos, permitiendo que la organización continúe operando. (Maestre, Osorio, Trillos, & Palencia, 2012).

También podemos definir básicamente el plan de contingencias realiza un estudio de las tecnologías y servicios para definir cuáles son los de más alto riesgo de la empresa, luego realizar un análisis y evaluación de riesgos y define

los escenarios considerados en el plan, y frente a cada escenario se propone las acciones necesarias de prevención, mitigación y recuperación.
A nivel mundial es de mucha importancia el concepto de Plan de Contingencia IT, existen millones de herramientas para respaldos, balanceos de carga, restore, etc pero si no existe la debida documentación, capacitación y socialización del plan no podemos actuar ante una catástrofe informática.
Entre los casos más recientes de fallos informáticos tenemos el sucedido en Mayo del presente año en España en el aeropuerto de Málaga donde las pantallas con la información de los vuelos se apagaron y el sistema de facturación falló en donde se presume una anomalía informática, quedando sin servicio durante un periodo de 5 horas.
Gerentes del área indicaron que se harán los correctivos necesarios en donde se incluye un plan de contingencia IT realizando las pruebas respectivas. (Frias, 2015)

En los países de Latinoamérica la aplicación de un plan de contingencia por cada entidad del sector público están regulados mediante normativas de aplicación obligatoria, debido a que estos priorizan el respaldo de la información por tratarse de documentación sensible del estado.

A nivel nacional existen varias empresas que ofrecen distintas soluciones sobre los planes de contingencia aplicados a las empresas, entre los tipos de soluciones tenemos:

- Soluciones Cloud
- Servicios de Housing
- Virtualización
- Cluster de alta disponibilidad.

Entre uno de las recomendados está el servicio de “Housing” que lo ofrece Telconet S.A. que se trata del alquiler de espacio físico (por m^2) en sus centros de datos, los mismos que cuentan con todas las normativas internacionales de seguridad. (TIER, ISO, IEEE).

Con esta solución el cliente paga una considerable mensualidad por el alquiler del espacio en el centro de datos TELCONET, una de las ventajas es que ofrece continuidad del negocio y el cliente se *"desliga"* de cualquier réplica de servicios en otra localidad de la empresa.

La empresa Casa del Cable S.A. es una de las principales importadoras y comercializadoras del país en las líneas de herramientas de conectividad, tiene una matriz y dos sucursales, una dentro y otra fuera de la ciudad.

Provee soluciones de infraestructura de alta calidad en telecomunicación, con profesionales permanentemente capacitados y orientados al servicio; ofreciendo productos seguros y ambientalmente responsables.

El soporte IT de la empresa cuenta con un plan de contingencia, el mismo que no ha sido documentado aún, ni evaluado respecto de las respuestas efectivas y no efectivas al momento de presentarse las contingencias.

Al ser una empresa que brinda soluciones de conectividad y seguridad en calidad de energía; cuentan con tecnología de punta en su plataforma de servidores, cuentan con las herramientas, software para respaldos pero no cuentan con el plan de contingencia IT.

Se tiene como antecedente la perdida de información de la base de datos SQL por no contar con respaldos automatizados y supervisados bajo un plan IT, como consecuencia de este incidente se procedió a ingresar los datos de facturación de los últimos 6 meses del año 2011.

FUNDAMENTACIÓN TEÓRICA

Definición de Plan De Contingencia

Al hablar de plan de contingencia nos estamos refiriendo a una reducción de impacto, es decir que no se vea afectada en lo menos posible la continuidad del negocio.

Entre definiciones puntuales se puede decir que es:

- Una estrategia planificada.
- Un conjunto de recursos de respaldo.
- Una organización de emergencia.
- Procedimientos de actuación para conseguir una restauración de manera ágil de los servicios del negocio afectado.
- Es el resultado de todo un proceso de análisis y definiciones, las cuales dan lugar a las metodologías a utilizarse.

No debemos confundir entre un plan de continuidad y un plan de contingencias.
Un plan de contingencia forma parte de un plan de continuidad, es decir la contingencia solo va ser utilizada en el momento de la catástrofe mientras que en la continuidad analizamos todas las vulnerabilidades y contramedidas para atenuar vulnerabilidades.

Realizando una equivalencia, podemos poner como ejemplo:
La alerta de un disco duro del servidor, el led del disco se encuentra en color naranja es decir presenta una advertencia, por el plan de continuidad que se mantiene (revisión de log, envío de alertas) se notifica la novedad; en el plan de contingencia nos indica que debemos contar en stock con un disco duro de las mismas características para proceder con el cambio solicitado.

A continuaciones algunas definiciones de plan de contingencia de varios autores:

Según MARIO G. PIATTINI .- El plan de contingencias es una estrategia planificada constituida por: un conjunto de recursos de respaldo, una

organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por la paralización total o parcial de la capacidad operativa de le empres. Esta estrategia materializa da en un manual, es el resultado de todo un proceso de análisis y definiciones, las cuales dan lugar a las metodología. (Piattini, 2001)

Según el sitio web www.definición.de.- plan de contingencia es un programa alternativo para que una empresa pueda recuperarse de un desastre informático y restablecer sus operaciones con rapidez. Estos planes también se conocen por la sigla DRP, del inglés Disaster Recovery Plan.

Un programa DRP incluye un plan de respaldo (que se realiza antes de la amenaza), un plan de emergencia (que se aplica durante la amenaza) y un plan de recuperación (con las medidas para aplicar una vez que la amenaza ha sido controlada). (Piattini, 2001)

Definición de Informática

La informática es un conjunto de técnicas que hacen posible la automatización de la información la misma que se puede gestionar por medio de ordenadores o dispositivos electrónicos que reciben una entrada de datos y devuelven información procesada concreta y precisa la misma que se utiliza para fines educativos.

Definición de Plan De Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir

La presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

Definición de Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

Definición de Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Todo Plan de Contingencia informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

Definición de Plan de pruebas

El resultado de las pruebas efectuadas será presentado igualmente para su conformidad. Las pruebas relacionadas a este plan, se ejecutaría semestralmente con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

Definición de Alta Disponibilidad

La alta disponibilidad se trata de que los servicios y/ o aplicaciones estén disponibles la mayor cantidad de tiempo posible para evitar pérdidas de información o inconvenientes para prestar determinado servicio. La alta disponibilidad se mide como el tiempo que el sistema (aplicaciones y/o servicios) está disponible y se representa como un porcentaje.

Definición de Gestión de Continuidad del Negocio (BCM en inglés)

“Proceso de gestión holístico que identifica las amenazas potenciales de una organización y los impactos que pueden causar en las operaciones del negocio si esas amenazas se materializan. Además proporciona un marco de trabajo para construir una organización más resistente con capacidad para responder de forma efectiva y proteger los intereses de las partes interesadas clave, su reputación, imagen de marca y actividades de valor añadido.

Definición de virtualización

La virtualización es un proceso mediante el cual se pueden instalar y utilizar varias máquinas virtuales en una sola maquina física. Las máquinas virtuales comparten los recursos de la máquina física y de esta manera se aprovechan todos los recursos existentes. Adicionalmente, cada una de las máquinas virtuales puede correr un sistema operativo diferente con sus respectivas aplicaciones, según la necesidad. Cabe anotar que cada máquina virtual utiliza los recursos que necesita en el momento que los necesita sin generar conflictos con otras máquinas virtuales instaladas en la misma máquina física. (VMware, 2015)

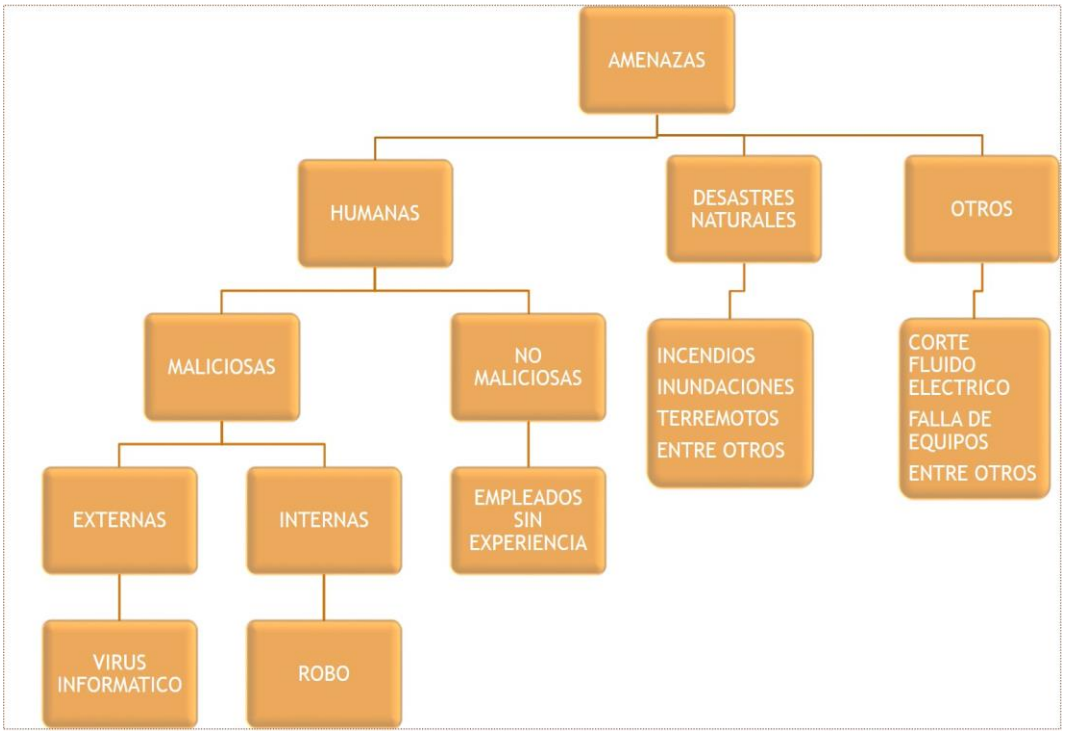
Tipos de amenazas a la seguridad

Ninguna empresa está inmune de sufrir amenazas a su seguridad, estas amenazas a las que son frágiles las organizaciones se observan en el siguiente gráfico.

ILUSTRACIÓN No. 1

TIPOS DE AMENAZA

Elaborado por: William Moscol Criollo



Fuente: (Areitio, 2008)

En el ámbito informático las amenazas más conocidas son los ataques por virus, los daños por desastre natural o fallas eléctricas también son consideradas amenazas que deben ser prioridad de un riesgo dentro del plan de contingencia IT.

Políticas de Seguridad

Las políticas de seguridad son normas que adoptan las instituciones para definir reglas y estándares las mismas que deberán ser aplicadas en cada uno de los procesos que se llevan en las instituciones. La seguridad de la información rige políticas de seguridad en su totalidad ya que se definen procedimientos para regular el uso de la información y de los sistemas esto con la finalidad de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma.

"La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas." *(*Spafford, 2000)

Objetivos de las políticas de seguridad

Los objetivos se los define de la siguiente manera

- Gestionar la seguridad de la información dentro de la organización.
- Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización.
- Salvaguardar la información cuando la responsabilidad del tratamiento de la misma está en manos de terceros.

Como complemento se deberá de diseñar una estructura organizativa dentro de la institución la misma que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo creando una relación con los sistemas de información.

Definición software Retrospect 9.0

Las soluciones empresariales de Retrospect ofrecen copias de seguridad locales y externas, restauraciones precisas de puntos temporales, deduplicación a nivel de archivo, integración con VMware, gestión remota iOS de múltiples servidores de copia de seguridad, restauraciones iniciadas por los usuarios finales y atención al cliente en tiempo real; todo ello sin precisar de personal de TI dedicado para gestionarlo.

Retrospect automatiza el proceso de copia de seguridad de los equipos conectados en red.

- Hace que resulte sencillo crear una estrategia de copia de seguridad completa y fiable.

- Funciona a la perfección en entornos Windows/Mac mixtos sin coste añadido.
- Detecta de forma automática los servidores y equipos de sobremesa & portátiles nuevos o recién conectados, dando prioridad a la copia de seguridad de estos.
- Retrospect ofrece las funciones y el rendimiento de calidad empresarial que necesitan las pequeñas y medianas empresas, sin precisar personal de TI dedicado que gestione las operaciones de copia de seguridad y recuperación.
- Lleva a cabo copias de seguridad versátiles con hasta 16 operaciones ejecutables de forma simultánea.
- Copia de seguridad flexible en discos locales y en red
- Las características de gestión de soportes facilitan la rotación de
- soportes y simplifican la localización de los datos que se deben restaurar. (Retrospect, 2015)

Definiciones Conceptuales

Plan de Contingencia

Son procedimientos que definen cómo una Institución continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas de IT son vulnerables a diversas interrupciones.

Software Veeam

Este software nos va a permitir realizar las copias de las máquinas virtuales o snapshot mediante una consola administrativa.

Los respaldos se van alojar en discos NAS creando reglas en el software e indicando la hora del respaldo.

Software Retrospect 9.0

El mismo que nos va a permitir a administrar mediante una interfaz gráfica los respaldos programados en los PC

En cada PC debe ir instalado un agente de red que es el que permite la conexión de CLIENTE-SERVIDOR, cabe indicar que son respaldos para usuarios finales, es decir los perfiles de Windows

Microsoft SQL 2008 R2

Mediante script de SQL se va a programar las copias de seguridad de la base de datos alojándose en una unidad de red mapeada previamente en el servidor.

Vmware Client Vsphere 5.5

Este S.O. es el motor de la administración de las máquinas virtuales, mediante una interfaz gráfica se asigna recursos a las diferentes máquinas virtuales.

Windows Server 2008-2012

Los servidores virtuales se ejecutan bajo esta plataforma permitiendo así una mejor administración por medio de una interfaz gráfica.

NAS

Por sus siglas en inglés (Network Attached Storage) almacenamiento conectado a la red, son dispositivos que permiten una administración vía GUI es de cir por medio de una interfaz gráfica, cuentan como minimo con una interfaz de red permitiendo así un almacenamiento directo en la red.

Rack

O también conocido como soportes metálicos, es donde se alojan todos los dispositivos tanto de telecomunicación como servidores, permitiendo así una administración centralizada de los equipos de computación, vienen en diferentes tamaños acorde a la necesidad del proyecto.

SIAC

Software desarrollado por la compañía FUTURESOFT de Guayaquil – Ecuador, presta servicios a la compañía CASA DEL CABLE ajustando el software a la necesidad del cliente.

El software cuenta con los módulos de administración de empresas, tales como:

- Contabilidad
- Roles
- Inventario
- Importaciones
- Bancos
- Presupuesto
- Activos Fijo

Seguridad Física

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación a la cronología del error.

Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.
El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.
En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc

Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema de computación o intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque Activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje.

Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

Sitios alternos

Los sitios alternos o de almacenamiento off-site se clasifican de la siguiente manera:

- **Hot site**

  Listo para operar en pocas horas, tiene el equipo, red y sistemas necesarios. Sólo falta el staff, datos y documentación.

- **Warm site**

  Puede operar en menos de un día. Está parcialmente configurado, con conexiones de red y equipo periférico seleccionado. Cuenta con requisitos de hardware inferiores a los equipos de cómputo que se encuentran en producción.

- **Cold site**

  Tiene solo la infraestructura básica: suministro eléctrico, aire acondicionado, etc. Está listo para recibir equipo de cómputo y comunicaciones. Puede tardar varios días en operar.

Estrategias para garantizar continuidad

Existen varias maneras de limitar las fallas en el servicio:

- **La prevención de errores:** que consiste en evitar errores anticipándolos.
- **La tolerancia a errores:** cuyo propósito es proporcionar un servicio de acuerdo con las especificaciones a pesar de los errores, presentando redundancias.

  Es la capacidad que tiene un sistema de seguir en funcionamiento cuando se produce un error en parte del mismo. Para crear un sistema tolerante a errores, use medidas preventivas para reducir la posibilidad de que se produzca un error del sistema, así como para minimizar el impacto de un desastre.

  Puede usar las siguientes estrategias para mejorar la tolerancia a errores de la implementación de Client Security: (Microsoft Corporation, 2014)

  - Minimización de puntos únicos de error
  - Uso de configuraciones RAID
  - Uso de fuentes de alimentación de reserva
- **La eliminación de errores:** destinada a reducir la cantidad de errores por medio de acciones correctivas.
- **La predicción de errores:** anticipando errores y su posible impacto en el servicio.

Hardware, Software e Información

Software

Entre los programas que se van a utilizar para respaldos de cliente – servidor tenemos:

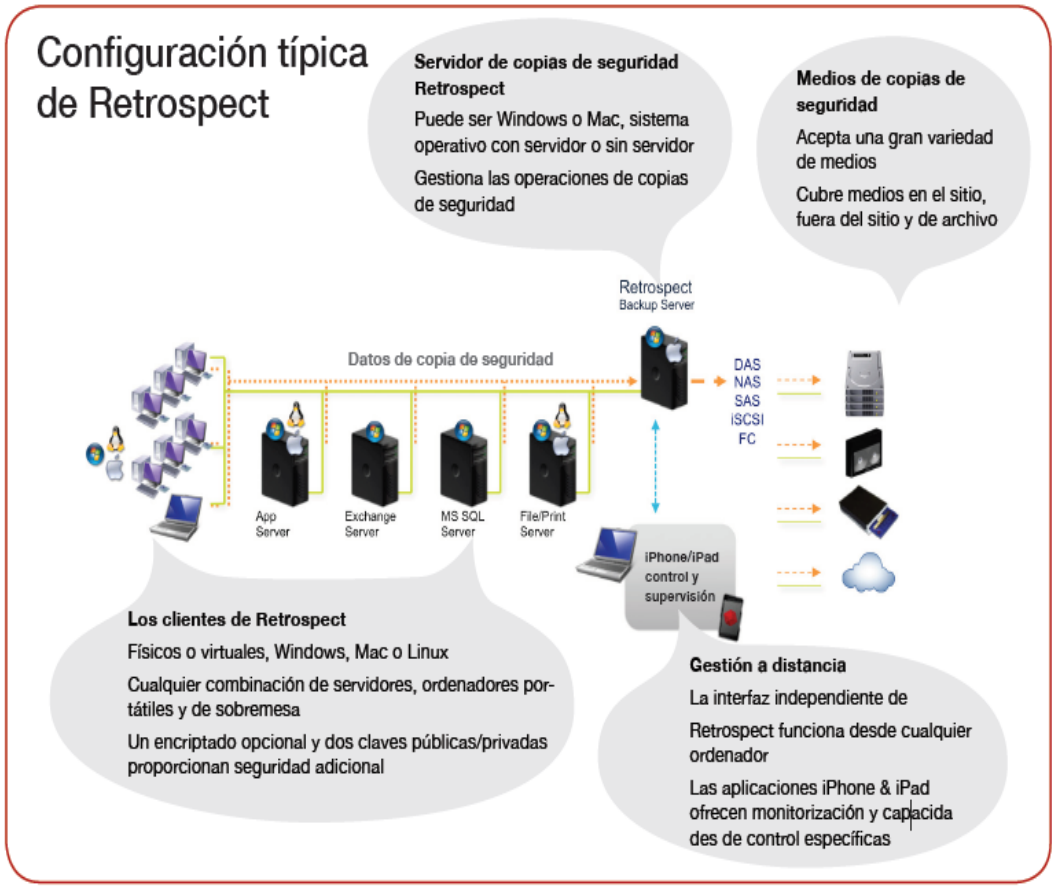
Retrospect.- se va a usar para respaldos de información de los usuarios su versión es Single Server 9.0, el mismo que nos va a permitir respaldar todo el perfil de del Usuario de Windows y Mac.

Entre sus características que resaltan es que contiene un complemento llamado Open File Backup Disk-to-Disk Edition que permite proteger archivos abiertos en volúmenes con formato NTFS en el servidor de Windows. Este complemento permite proteger aplicaciones de línea de negocios, por ejemplo sistemas de contabilidad, CRM y bases de datos sujetas a derechos de propiedad, mientras están en funcionamiento, incluso aquellas con archivos de datos repartidos entre varios volúmenes. El complemento Retrospect Open File Backup Disk-to-Disk Edition solo cubre el servidor host de Retrospect. Específicamente para Retrospect Single Server (Disk-to-Disk) y Desktop (Professional).

A continuación un esquema de cómo trabaja:

ILUSTRACIÓN No. 2

CONFIGURACIÓN BÁSICA DE RETROSPECT



FUENTE: www.retrospect.com

Servidor de copias de seguridad Retrospect.- el funcionamiento del software lo hace bajo la arquitectura CLIENTE-SERVIDOR, es decir el Servidor debe cumplir ciertos requisitos antes de empezar la instalación:

Sistemas operativos compatibles:

Microsoft Windows 8/7/Vista/XP
Microsoft Windows Server 2012/2008/2003*
Microsoft Windows Server 2012 Essentials*
Microsoft Windows SBS 2011/2008/2003
Microsoft Windows Storage Server 2008/2003

Requisitos de Hardware mínimo:

Procesador Pentium (32 y 64 bits)
10-15 GB de espacio temporal en el disco duro para todas las actividades simultáneas (copias de seguridad, restauraciones, etc.)
1 GB para cada actividad simultánea; 3 GB mínimo para Windows de 32 bits, 4 GB mínimo para Windows de 64 bits Almacenamiento adecuado para copias de seguridad

Cliente Retrospect.- la arquitectura a utilizarse es CLIENTE-SERVIDOR, en cada uno de nuestros equipos de la red se debe instalar un agente de red que es él que va a permitir la conexión que es compatible con los siguientes sistemas operativos:

Sistemas operativos compatibles:

Microsoft Windows 8/7/Vista/XP
Microsoft Windows Server 2012/2008/2003*
Microsoft Windows Server 2012 Essentials*
Microsoft Windows SBS 2011/2008/2003*
Microsoft Windows Storage Server 2008/2003*
Mac OS X o Mac OS X Server* 10.6.8 o posterior

Centos 6.4, 6.5 y 7
Red Hat Enterprise Linux 7
Debian 7.6
Ubuntu Server 14.04
Servidor de empresa SUSE 11 11 SP2 y SP3
GLIBC versión 2 o posterior

Una vez instalado el agente de red restrospect automáticamente el servidor detecta el equipo en red, y mediante una contraseña establecida por el administrador de red se logra la autenticación entre cliente-servidor.

Los procesos de copia de seguridad los realiza bajo configuraciones, políticas o script creados en la consola de administración Retrospect Single Server 9.0, los procesos de copia pueden ser:

Copia de seguridad Proactiva: este tipo de copia es ideal para equipos portables de la empresa, son equipos que no están siempre disponibles en la LAN de la empresa, el equipo apenas sea detectado por la consola continúa con el proceso de copia.

Copia de seguridad bajo demanda: este tipo de copia permite desde el mismo cliente ejecutar la copia de los archivos, carpetas personalizadas, incluso ejecutar sus propias restauraciones.

Copia de seguridad incremental inteligente: no es necesario establecer una configuración e indicar al programa que realice una copia de seguridad incremental, Retrospect continúa con el respaldo de los últimos cambios realizados.

Copia de seguridad incremental a nivel de bloque: Retrospect tiene ahora la capacidad de realizar copias de seguridad de solo las partes de un archivo que hayan cambiado. Después de una copia de seguridad completa inicial, Retrospect busca las partes cambiadas de cada archivo de gran tamaño y solo realiza copias de seguridad de esos bloques,

acelerando así dichas copias de seguridad y utilizando menos espacio de almacenamiento.

Des-duplicación automática a nivel de archivo: Retrospect maximiza el uso del almacenamiento copiando los archivos una sola vez (incluso de varios ordenadores) en el soporte de copia de seguridad.

Recuperación de fallo directamente sobre el hardware: Se pueden crear medios de arranque para casi todos los sistemas Windows protegidos por Retrospect para proporcionar una recuperación rápida desde un estado de no arranque del sistema. Ahora es compatible con lo último en hardware y sistemas operativos incluyendo Windows 8.1, Windows Server 2012 R2 y las máquinas y controladores de 64 bits

Entre sus complementos tenemos:

Microsoft SQL Server Agent

Proporciona copias de seguridad en caliente de Microsoft SQL Server 2014, 2012, 2008 y 2005. Restaura automáticamente un servidor SQL o bases de datos individuales a un punto temporal concreto. Tiene licencia para un servidor SQL con la aplicación Retrospect o como Retrospect Client; incluye una licencia de Retrospect Server Client.

Microsoft Exchange Server Agent

Proporciona copias de seguridad en caliente de grupos de almacenamiento, bases de datos y buzones de correo de Microsoft Exchange Server 2013, 2010, 2007 y 2003. Restaura automáticamente un servidor Exchange o componentes individuales a un punto temporal concreto. Tiene licencia para un servidor Exchange con la aplicación Retrospect o como Retrospect Client; incluye una licencia de Retrospect Server Client.

Advanced Tape Support

Reduce la duración de las copias de seguridad al utilizar varias unidades de cinta en paralelo, lo que incluye varias unidades independientes, unidades en bibliotecas o unidades en cargadores automáticos. El

complemento Advanced Tape Support se licencia por servidor host de Retrospect, no por unidad de cinta. Por ejemplo, solo se necesita una licencia de complemento Advanced Tape Support para una biblioteca con cuatro mecanismos de unidad de cinta.

Los complementos en mención se instalan de acuerdo a la necesidad del cliente, se ofrecen por separado, en nuestro caso vamos a utilizar la versión Single Server 9.0 que trabaja con una licencia instalada en el servidor y conexiones ilimitadas de clientes (cliente retrospect).

Análisis de la competencia

Retrospect para Windows y los principales competidores

A continuación se detalla las competencias de herramientas similares para copias de seguridad cliente-servidor.

CUADRO No. 2

ANÁLISIS DE COMPETENCIA DEL SOFTWARE RETROSPECT 9.0

DESCRIPCIÓN	RETROSPECT 9.0	SYMANTEC BACKUP EXEC 2012	ACRONIS BACKUP 11.5	CRASH PLAN PROe 3.5
Recuperación ante daño físico de servidores, desktop y laptop	X	Costosa	X	
Recuperación ante daño físico equipos Apple	X	Costosa		
Fácil sincronización con almacenamiento en nube de terceros	X	X		
Puede ejecutarse en Microsoft SO que no cumplan rol de servidor	X		X	
Evita datos duplicados en volumen	X	X	X	Solo en el mismo equipo local
Restauración precisa desde un punto de	X	Restaura archivos no	X	Restaura archivos no

seguridad incremental		deseados		deseados
Restauración de hardware disímil	X	X	X	Solo restaura datos
Reversión inmediata de un equipo copiando solo los últimos cambios	X			
Flexibilidad en la rotación de los medios extraíbles (cintas)	X			
Verificación de datos restaurados	X		Programada	Programada
Opciones de cifrado de datos	X	X	X	X
Seguimiento y monitoreo desde dispositivos móviles	X			
Soporte de cinta completo (copias primarias, restauración, catálogo de archivos)	X	X	Mínimo	

Elaborado por: William Moscol Criollo
Fuente: www.retrospect.com

Medios de copia de seguridad.- Retrospect Single 9.0 puede usar varios destinos de disco duro, tanto si están agrupados como si se usan de forma independiente; conectados directamente a través de USB, FireWire o eSATA; o en red mediante Ethernet, iSCSI o canal de fibra. Retrospect admite la mayoría de tipos de soportes magnéticos para copia de seguridad, incluidos discos duros, discos conectados a redes, almacenamiento en la nube, soportes flash y los principales formatos de cinta.

Casa del Cable S.A. posee un almacenamiento conectado en red (NAS), físicamente se encuentra en el dispositivo:

CUADRO No. 3

DATOS TÉCNICOS DE LA UNIDAD DE ALMACENAMIENTO

IP	NOMBRE DEL EQUIPO	MARCA	MODELO	CAPACIDAD
192.168.7.234	GYE-NAS-01	IOMEGA	NAS STORECENTER IX4-200D	4 TB

Elaborado por: William Moscol Criollo
Fuente: Inventario de equipos CDC

- Para el proceso de copia de seguridad se usa un disco duro de red (NAS) conectado físicamente al servidor con configuración ISCSI.
- El volumen se encuentra montado con el nombre de *"RetroData"* con la letra *"E"* asignada.
- Maneja un arreglo de discos duros tipo RAID 5.

Software Base de Datos

El motor de base de datos usado actualmente en Casa del Cable S.A. es Microsoft SQL 2008 R2, cuenta con sus licencias y CAL respectivas.
La administración de la base de datos está a cargo del proveedor del software contable y de administración SIAC, la empresa Futuresoft S.A.

Entre algunas de las opciones para disponibilidad, continuidad y replicación de base de datos SQL 2008 R2 tenemos las siguientes:

- Failover clustering – Agrupación de conmutación de error.
- Mirroring.
- Transactional Replication – Replicación transaccional
- Log Shipping – Trasvase de registros.
- Database Snapshots – Instantáneas de Base de datos
- Copia de seguridad, restaurar y Tecnologías Relacionadas

Entre las ventajas de las técnicas de alta disponibilidad de base de datos tenemos:

- Permite el filtrado en la base de datos para obtener un subconjunto de datos en las bases de datos secundarias, dado que opera en el ámbito de las bases de datos.
- Permite más de una copia redundante de la base de datos.
- Permite la disponibilidad y escalabilidad en tiempo real entre varias bases de datos, además de admitir las actualizaciones con particiones.
- Asegura una disponibilidad completa de las bases de datos secundarias para las funciones relacionadas con los informes, entre otras, sin la recuperación de las consultas.

Una de las técnicas que puede utilizarse es la **Mirroring,** fue introducida en la edición 2005, se puede decir que es la evolución del log shipping**.** La principal diferencia es el tiempo de espera para tener la información más actual; el espejo es un recurso más rápido que el log shipping.

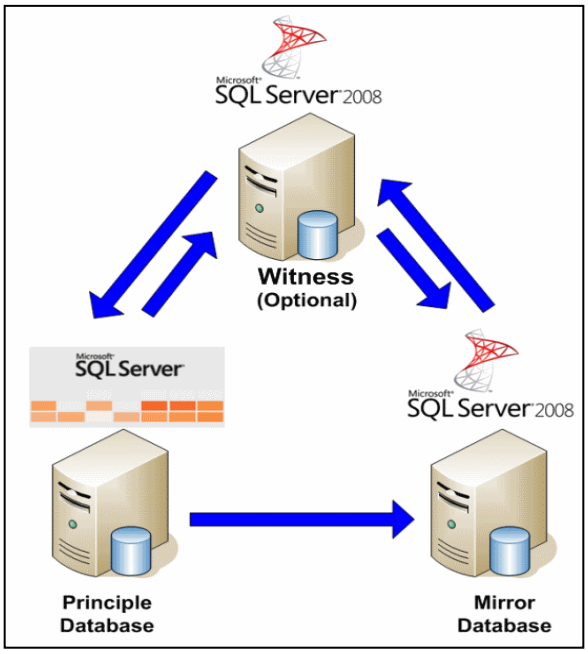
Otra diferencia es que el servidor en stand by automáticamente puede levantarse en caso de que el servidor principal fallara (a esto se le llama espejo de alta disponibilidad**,** y para esto requerimos de un tercer servidor al que nombran testigo), sin tener que restaurar los registros (en realidad, los registros se fusionan de forma continua en este escenario – no es de extrañar que se llama Espejo). Las ventajas adicionales incluyen la creación de reflejo de apoyo a nivel NET Framework. Además de algunas nuevas características como la recuperación automática de páginas incluidas en SQL Server 2008.

Periódicamente a un servidor en stand by si el servidor activo detecta un downtime se puede subir el servidor en stand by restaurando todos los logs transferidos.

Escenario donde se puede usar: si usted desea que el tiempo de recuperación sea menos y también requiere una solución rentable en términos de almacenamiento compartido, interruptores, etc También se dirigen a una base de datos única que se adapta fácilmente en sus discos. (ownerdba, 2012)

ILUSTRACIÓN No. 3

TÉCNICA DE ALTA DISPONIBILIDAD MIRRORING



FUENTE: (ownerdba, 2012)

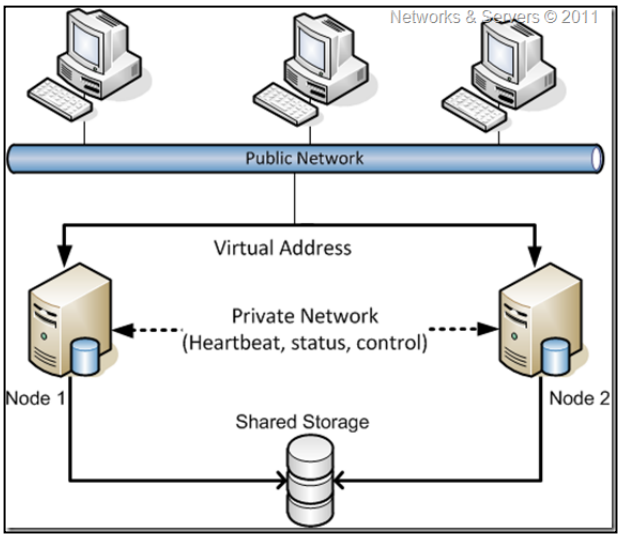
Failover clustering

Otra de las técnicas que se recomienda utilizarse para la replicación de la base de datos es ´´*Failover clustering*´´, es una opción de alta disponibilidad únicamente usado (a diferencia de las otras esta opción puede ser usado perfectamente como un plan para recuperación de desastres) con tecnología en clúster que incluye la cooperación del hardware y del sistema operativo.

Aquí los datos y bases de datos no pertenecen a ninguno de los servidores, y de hecho residen en almacenamiento compartido externo como SAN. Las ventajas de un dispositivo de almacenamiento SAN son de gran eficiencia de almacenamiento de disco. (ownerdba, 2012)

ILUSTRACIÓN No. 4

TÉCNICA DE DISPONIBILIDAD FAILOVER CLUSTERING



FUENTE: (ownerdba, 2012)

Como se observa en la gráfica, la base de datos se encuentra en un repositorio SAN o virtual, de esta manera replica al nodo X1 y X2.

FUNDAMENTACIÓN LEGAL

Dentro de los aspectos legales existen varios registros oficiales donde exigen más que todo a las entidades públicas un plan para mitigar riesgos en todo ámbito, donde se incluye también lo tecnológico.

Entre las entidades que citan estos aspectos está La Contraloría General del Estado.

REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE 2009

NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS

300-02 Plan de mitigación de riesgos

Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizarán el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos. (Estado, 2009)

NORMAS DE CONTROL INTERNO

Es un conjunto de normas establecidas por la Contraloría General del estado, la presente investigación se basa en la norma 410 dirigida para uso de Tecnología de la Información.

Entre las ventajas que nos proporcionan las Normas de Control Interno tenemos:

- Nos permite tener un marco de referencia.
- Tiene un enfoque teórico que se fundamenta en las metodologías antes expuestas.

Su desventaja, muy poco explicita, necesita un mejor detalle, para ello con la ayuda de metodologías internacionales, las cuales nos permiten desarrollar un marco de trabajo adecuado y tener una visión más clara de los procesos a seguir. (Estado, 2009) Otro de los aspectos legales citados es en la CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008 vigente actualmente, donde también hacen referencia de manera general a los riesgos donde también se comtempla planes de contingencia

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

Art 389.- Gestión del Riesgo

Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre. (Constitucion de la Republica del Ecuador, 2008).

LEY ORGÁNICA DE LA CONTRALORÍA GENERAL DEL ESTADO

Art. 21.- *Auditoria de gestión.- La Auditoria de Gestión es la acción fiscalizadora dirigida a examinar y evaluar el control interno y la gestión, utilizando recursos humanos de carácter multidisciplinario, el desempeño de una institución, ente contable, o la ejecución de programas y proyectos, con el fin de determinar si dicho desempeño o ejecución, se está realizando, o se ha realizado, de acuerdo a principios y criterios de economía, efectividad y eficiencia. Este tipo de auditoria examinará y evaluará los resultados originalmente esperados y medidos de acuerdo con los indicadores institucionales y de desempeño pertinentes.*

Constituirán objeto de la auditoría de gestión: el proceso administrativo, las actividades de apoyo, financieras y operativas; la eficiencia, efectividad y economía en el empleo de los recursos humanos, materiales, financieros, ambientales, tecnológicos y de tiempo; y, el cumplimiento de las atribuciones, objetivos y metas institucionales.
A diferencia de la auditoría financiera, el resultado de la fiscalización mediante la auditoria de Gestión no implica la emisión de una opinión Profesional, sino la elaboración de un informe amplio con los comentarios, conclusiones y recomendaciones pertinentes. (Estado L. O., 2009).

PREGUNTAS CIENTÍFICAS A CONTESTARSE

¿Elaborando un plan de contingencia se solucionaran los problemas de vulnerabilidad de fluidos eléctricos?

¿Qué tipos de datos y qué cantidad, va a ser necesario replicar, para el restablecimiento oportuno del servicio IT?

¿Cuál será el modelo a aplicarse para realizar el cambio desde el ambiente normal de desenvolvimiento de la empresa hacia el ambiente de contingencia y viceversa?

¿Cuáles serán los tiempos máximos y mínimos tolerables de interrupción de los servicios IT?

¿Qué riesgos se extinguirán o prevendrán con la aplicación del plan de contingencia IT en la empresa Casa del Cable S.A.?

CAPÍTULO III

PROPUESTA TECNOLÓGICA

El presente capítulo determinará la propuesta a realizarse a la empresa CASA DEL CABLE S.A., mediante el análisis de los factores estudiados previamente, en los anteriores capítulos. La propuesta consistirá en la identificación de amenazas y vulnerabilidades para la elaboración del plan de contingencia IT de la compañía mencionada.

ANÁLISIS DE FACTIBILIDAD

Las necesidades de sistemas de información y sus respectivas operaciones de automatización deben tratarse como proyectos de inversión, motivo por el cual, como para cualquier otro proyecto, deben investigarse y analizarse los elementos que generan las necesidades, Todos los aspectos que de alguna forma intervienen en la actividad deben ser considerados, y como resultado del análisis de las diferentes formas de tratamiento de los datos se deben obtener opciones de solución, sometiendo cada una de las opciones a la evaluación del estudio de factibilidad que debe contemplar: la factibilidad técnica, operativa, y por su puesto factibilidad económica. (Delgado, 1998)

Factibilidad Operacional

La empresa Casa del Cable S.A. inició sus actividades en la ciudad de Guayaquil en el año 1988 con la comercialización de cables de uso electrónico. Actualmente, cuenta con 3 localidades a nivel nacional, la matriz está ubicada en

la ciudad de Guayaquil, en el Km. 4.5 Vía a Daule, una sucursal en la misma ciudad en el centro, y en la ciudad de Quito su segunda sucursal.

La empresa mantiene horarios de operaciones fijos, de lunes a viernes de 8:30 am hasta las 17:30, con 50 usuarios en la matriz, y en las sucursales de Guayaquil y Quito, 5 y 10 respectivamente. Estos usuarios desarrollan diferentes tipos de actividades, con una característica en común: todos necesitan estar conectados al servidor central, para el normal desempeño de sus funciones.

En tal sentido, el desarrollo de un plan de contingencia IT beneficia a la empresa, disminuyendo los riesgos que puedan surgir a partir del desenvolvimiento de sus operaciones. Este proyecto, se orienta a resultados inherentes a la recuperación de información, y a la continuidad de sus actividades en un ambiente de contingencia, disponible las 24 horas del día enfocado solo en matriz de Guayaquil.

Plan De Implementación

Una parte importante del presente proyecto se enmarca en la planeación de los procedimientos necesarios para implementar exitosamente la solución propuesta. Las actividades a contemplarse para llevar a cabo la aplicación del plan de contingencia IT de la empresa Casa del Cable S.A. se describen a continuación:

1. Firma de acta de compromiso
2. Formación del personal
3. Adecuación de instalaciones

   Las condiciones a establecerse en la adecuación, son las siguientes:

   Acceso seguro al departamento de sistemas

   Superficie de suelo

   Ventilación

   Suministro e instalaciones eléctricas

   Suministro de corriente ininterrumpidas

Cableado estructurado.
Equipos de seguridad (extintores)

4. Recopilación de datos
5. Configuraciones en equipos de sistemas
6. Pruebas y verificación en instalaciones
7. Pruebas de funcionalidad del plan de contingencia IT
8. Entrega del plan
9. Periodos de seguimiento

La duración de estas actividades se muestran en un cronograma de implementación, con la descripción de los plazos, prioridades, duración y responsables, en función de la autorización y recomendaciones previas del representante de la compañía.

Plan De Capacitación

La implementación del plan de contingencia IT conlleva consigo un plan de capacitación, con el objetivo de formar al personal de sistemas en el uso del manual de contingencias, y en general de todos los procedimientos a realizarse que se enmarquen dentro del desarrollo del mismo.

Se ha planificado convocar al personal de sistemas en una fecha determinada, y coordinada con el representante de la empresa, sin afectar las funciones desempañadas por tales. De la misma forma, se capacitará exclusiva y brevemente a los administradores de la compañía para que tengan conocimiento general del proceso de contingencia.

Temario de capacitación

Aspectos Generales
Ambiente externo IT de la empresa Casa del Cable S.A.
Aspectos específicos

Descripción de los recursos en la empresa

- Equipos disponibles
- Personal en sistemas

Descripción del plan de contingencia IT

- Actividades a ejecutar
- Guías paso a paso

Características Principales del plan

- Funcionalidad del plan
- Generación de reportes
- Análisis de tiempos

Instructor:

William Moscol, Ondu

Recursos:

Sala de reuniones habilitada, computador portátil, proyector, guías rápidas entregables a usuarios.

Factibilidad Técnica

Descripción del plan de contingencia IT

CASA DEL CABLE S.A. y como en cualquier otra empresa determina como claves del negocio el sistema informático de administración y facturación.

Al ser considerados como clave del negocio surge la necesidad de la continuidad del servicio y minimizar el tiempo de inactividad que se den por circunstancias externas que puedan causar inconvenientes.

El proyecto que se va a desarrollar consiste en implementar un ambiente de contingencia IT en un sitio alterno que en este caso es en la sucursal de CASA DEL CABLE S.A. ubicada en la ciudad de Guayaquil, Baquerizo Moreno 1114 y

Av. 9 de Octubre para las aplicaciones SIAC, Active Directory, y base de datos; en las aplicaciones mencionadas trabajan todas las áreas a nivel nacional.
También se va a elaborar el plan de contingencia IT que se va a ejecutar en el ambiente de contingencia alterno para disminuir cualquier riesgo informático que impida la operatividad de las aplicaciones.

Requisitos del plan de contingencia IT

- En este proyecto se establecen algunos requisitos que deben cumplirse, los mismos que fueron analizados en conjunto con personal del área de sistemas de la compañía CASA DEL CABLE S.A, para cumplir estos requisitos se hizo énfasis en las normas DS4 Garantizar la continuidad del servicio de COBIT V.4

- El tiempo de no prestación del servicio no debe exceder las 2 horas.
- El paso de producción a contingencia y viceversa no deben verse afectados los usuarios, es decir debe ser transparente.
- Se deberá entregar la documentación respectiva del plan de contingencia IT en donde debe indicarse los pasos a seguir, los responsables respectivos y documentar las pruebas realizadas.
- Capacitar al personal del departamento de sistemas sobre el manejo del plan de contingencia IT.
- El hardware ya se encuentra adquirido por la empresa.
- Las licencias de software que se requieran serán facilitadas por CASA DEL CABLE S.A.
- La infraestructura del ambiente de contingencia ya se encuentra instalada en la sucursal de Guayaquil.
- La data replicada en el ambiente de contingencia no debe tener una antigüedad mayor a 2 horas.
- Se procederá con las pruebas de paso de contingencia la misma que debe ser documentada.

- El enlace de datos con el que cuenta CASA DEL CABLE es de 2 MB proporcionado por la compañía Level3 y otro enlace de 2 MB proporcionado por la compañía Conecel.

Situación Actual

Actualmente Casa del Cable cuenta con alrededor de 70 usuarios a nivel nacional, toda la infraestructura de tecnología se encuentra centralizada en la ciudad de Guayaquil, Matriz Mapasingue.

El software SIAC cuenta con todos los módulos para la administración de la empresa, entre los módulos están: contabilidad, RRHH, importaciones, facturación, bancos, inventario, la administración y servicios del software lo hace la compañía Futuresoft S.A. es la encargada de resolver cualquier requerimiento solicitado a nivel de software.

Los requerimientos de hardware, soporte e infraestructura tecnológica son administrados a través de un servicio outsourcing que se mantiene con la compañía ONDU SOLUCIONES TECNOLOGICAS la misma que cuenta con personal de planta donde el cliente en el horario de Lunes a Viernes de 8:30 a 17:30 en la localidad matriz administrando a nivel nacional la infraestructura.

Casa del cable S.A. tiene una infraestructura tecnológica con herramientas que son tendencia en la actualidad, entre las cuales tenemos:

- Virtualización
- Voip
- Office365
- Endpoint Security
- Backup usuario final
- Cableado Estructurado 7A
- Webinar Services
- Sistema de cámaras IP HD, Bosch

- Control de Acceso Bosch
- Seguridad perimetral.
- Conexiones VPN
- Localizador móvil, app de monitoreo móvil para gestión del área comercial.

Factibilidad Legal

El desarrollo del proyecto se lo realizará bajo lo dispuesto en la normativa legal vigente en el Ecuador, para lo que se cita a continuación a la "***LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS"***

Título V DE LAS INFRACCIONES INFORMÁTICAS
Capítulo I DE LAS INFRACCIONES INFORMÁTICAS

"Art. 57*.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.*

Reformas al Código Penal Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:
Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y

multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ....- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."

***"Art. 61.-** A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados: "*

Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de

datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art. ....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica."

***"Art. 62.-** A continuación del Art. 553, añádanse los siguientes artículos enumerados:*
Art. ....- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ....- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios

1. Inutilización de sistemas de alarma o guarda
2. Descubrimiento descifrado de claves secretas o encriptadas.
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes."

***"Art. 63**.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente: "Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de*

Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos."

Factibilidad Económica

Para el análisis de la factibilidad económica se compararan dos modelos de alternativas, el primero es en el que se decide crear el ambiente de contingencia "in site"; es decir, dentro de las instalaciones de la empresa. La primera alternativa se la contrastará con una opción "extra site"; es decir, lo que nos costaría mantener los respaldos del departamento de sistemas en un sitio alterno.

Alternativa 1

Se muestran los costos de la alternativa uno a continuación:

CUADRO No. 4

PRESUPUESTO PARA EL SITIO ALTERNO DE CONTINGENCIA

RUBROS	Costo	Cantidad	Total
Recursos Humanos	**$ 1500**		**$ 1500**
William Moscol - Ondu Soluciones Tecnológicas		80 horas	
Alfredo Mena - Ondu Soluciones Tecnológicas		80 horas	
Ing. Oscar Suarez - Ondu Soluciones Tecnológicas		80 horas	
Recursos Hardware			**$ 20.617,00**
Servidor IBM XSERIES 3650 M3 (Matriz)	$ 5609	1	$ 5609
Servidor IBM XSERIES 3550 M3 (Sucursal)	$ 5164	1	$ 5164
Servidor IBM SYSTEM X3650 M4 (Matriz)	$ 9844	1	$ 9844
Recursos Software			**$**

			6.200,00
Licencia Microsoft	$ 5000	1	$ 5000
Licencia Retrospect	$ 300	1	$ 300
Licencia Veeam	$ 300	3	$ 900
Recursos Varios			**$ 100,00**
Impresiones, DVD.	$ 100	1	$ 100
Servicios técnicos			**$ 700,00**
Soporte técnico Level3	$ 250	8 horas	$ 250
Soporte técnico Conecel	$ 250	8 horas	$ 250
Soporte técnico Futuresoft S.A.	$ 200	48 horas	$ 200
Otros	**$ 200**	**1**	**$ 200**
TOTAL			**$ 29.317,00**

ELABORADO POR: William Moscol Criollo

Siempre será la más económica y la que mejor beneficios brinda.

Alternativa 2

Por el contrario la alternativa 2, según la investigación con diferentes proveedores del servicio realizado en la ciudad de Guayaquil, muestran los siguientes costos:

Proveedor Telconet

Cuenta con una solución de un centro de datos alterno, es decir alquilan sus equipos, espacio físico, conexiones bajo los estándares internacionales con soporte técnico 24/7, el precio del alquiler va de acuerdo al espacio, consumo eléctrico y consumo de internet solicitado.

Telconet cuenta con dos Centros de Datos de Categoría Internacional denominados TELCONET CLOUD CENTER I en Guayaquil y TELCONET CLOUD CENTER II en Quito, los cuales se encuentran a la vanguardia de la tecnología y seguridad en infraestructura, permitiendo

garantizar los servicios de Housing y Cloud Computing que demandan las empresas, instituciones de Ecuador y de los países de la Región que requieran alta disponibilidad y bajas latencias para su crecimiento en el mercado.

Están certificados bajo la norma del Uptime Institute en las más altas categorías siendo el centro de datos de Guayaquil TIER IV y de Quito TIER III, permitiendo formar parte del grupo IDC-G (Alianza Internacional de Centro de Datos de Mercados Emergentes. (Telconet S.A., 2015)

Entre los servicios que ofrece están:

SERVICIOS DE HOUSING

Racks

Jaula Privadas

SERVICIOS ADICIONALES

Manos Remotas

Instalación de Hardware Pasivo

Mantenimiento de Infraestructura Física

Monitoreo Infraestructura

SERVICIOS DE HOSTING-CLOUD

Respaldo en la Nube

Correo en la nube

Correo en centro de Datos

Nube Pública

SERVICIOS ADICIONALES

Manos Remotas Lógicas

Monitoreo de Infraestructura

Licenciamiento SP (Service Provider)

CUADRO No. 5

PRESUPUESTO 2 DE SOLUCIÓN DE CONTINGENCIA IT

RUBROS	COSTO	CANTIDAD	TOTAL
Respaldo en sitio alterno (contrato 3 años)	**$ 1500**	**36 meses**	**$ 54000**
Servidor 2U con fuente de poder redundante.		3	
Enlace de datos 8 MB		1	

ELABORADO POR: William Moscol Criollo

Por lo expuesto, se puede observar que la mejor alternativa para el desarrollo del plan es la alternativa 1, ya que ofrece más servicios tanto en hardware como en software, además de que su costo es relativamente menos costoso, lo que generará el ahorro económico a la empresa, que se lo interpretaría como un beneficio económico, por los gastos suprimidos.

ETAPAS DE LA METODOLOGÍA DEL PROYECTO

Estándares

Casa del Cable S.A a nivel nacional en el área de tecnología posee equipos con tecnología de punta y para la implementación del plan de Contingencia nos guiaremos bajo las normas internacionales como:

- ISO 22301 - Continuidad del negocio.
- ITIL (Biblioteca de Infraestructura de Tecnologías de Información)- Proceso de Gestión de la Continuidad de Servicios IT.
- Cobit V5 – Continuidad de las operaciones.

COBIT.- Una de las herramientas que nos pueden ayudar a tener un adecuado enfoque para el plan de contingencia es el COBIT, el cual tiene 4 dominios.
En el dominio de “Entregar y dar soporte” que es el que cubre la entrega de los servicios requeridos, incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales, recibe las soluciones y las hace utilizables por los usuarios finales.
Este dominio incluye 13 objetivos detallados de control, los cuáles, permitirán asegurar la continuidad del servicio y por lo tanto, mantener la continuidad de las operaciones, los objetivos del dominio son:

- DS1 Definir y administrar niveles de servicio.
- DS2 Administrar servicios de terceros.
- DS3 Administrar desempeño y capacidad.

- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la seguridad de los sistemas.
- DS6 Identificar y asignar costos.
- DS7 Educar y entrenar a los usuarios.
- DS8 Administrar la mesa de servicio y los incidentes.
- DS9 Administrar la configuración.
- DS10 Administrar los problemas.
- DS11 Administrar los datos.
- DS12 Administrar el ambiente físico.
- DS13 Administrar las operaciones.

De los objetivos mencionados nos vamos a enfocar en el DS4-Garantizar la continuidad del servicio.

ITIL.- de los fundamentos ITIL nos enfocaremos en el proceso de **Gestión de la Continuidad del Servicio** que es la se preocupa de impedir que una imprevista y grave interrupción de los servicios IT, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.
La estrategia de la Gestión de la Continuidad del Servicio (ITSCM) debe combinar equilibradamente procedimientos:

- **Proactivos:** que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos:** cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

La ITSCM requiere una implicación especial de los agentes involucrados pues sus beneficios sólo se perciben a largo plazo, es costosa y carece de rentabilidad directa. Implementar la ITSCM es como contratar un seguro médico: cuesta dinero, parece inútil mientras uno está sano y desearíamos nunca tener que utilizarlo, pero tarde o temprano nos alegramos de haber sido previsores. (OSIATIS S.A.)

NORMA ISO 22301.- El nombre completo de esta norma es ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio.
La ISO 22301 ha reemplazado a la 25999-2. Estas dos normas son bastante similares, pero la ISO 22301 puede ser considerada como una actualización de la BS 25999-2.
Entre los beneficios que se tiene es que la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, la organización estará preparada para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente. (Cruz, 2012)

ENTREGABLES DEL PROYECTO

Manual De Copia De Seguridad Y Restauración De Archivos De Un Cliente

Los datos de IP, contraseñas y nombres de equipos son ficticios por cuestiones de seguridad y política de la empresa. A continuación se detalla el manual del proceso de copias de seguridad de aplicaciones monitoreadas por el departamento de sistemas:

Copia de seguridad de bases de datos del SIAC.

El almacenamiento se lo hace en un disco externo conectado físicamente al servidor GYE-DCEXC-01

CUADRO No. 6

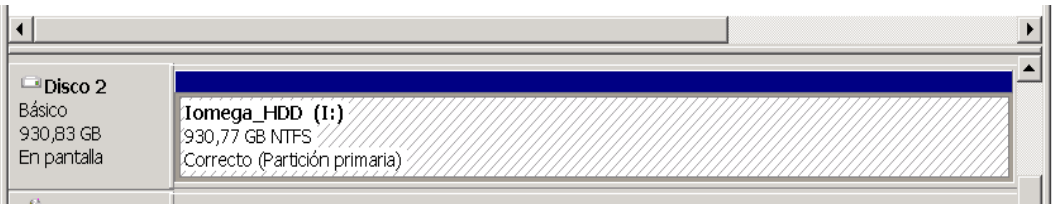
DATOS TECNICOS DE DISCO DURO A UTILIZARSE

N°	MARCA	DESCRIPCION	CAPACIDAD	SERIE
1	IOMEGA	DISCO DURO EXTERNO USB 3.0	1 TB	GSAB52034A

FUENTE: INVENTARIO DE EQUIPOS CDC
ELABORADO POR: William Moscol Criollo

ILUSTRACIÓN No. 5

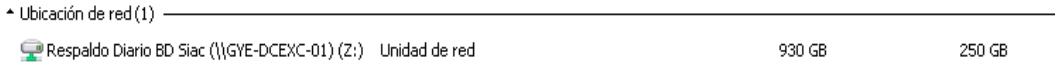
DATOS DE CONEXIÓN DEL REPOSITORIO DE COPIAS DE SEGURIDAD



FUENTE: SERVIDOR RETROSPECT CDC

ELABORADO POR: William Moscol Criollo

En el servidor SIAC – **GYE-APP-01-192.168.7.253,** está configurado como unidad de red con el nombre: **RESPALDO DIARIO SIAC.**



La copia de seguridad de la base de batos del sistema SIAC se maneja de manera automatizada (script), la ejecución del mismo se realiza **todos los días a las 23:00 PM, es un tipo de respaldo completo.**

ILUSTRACIÓN No. 6

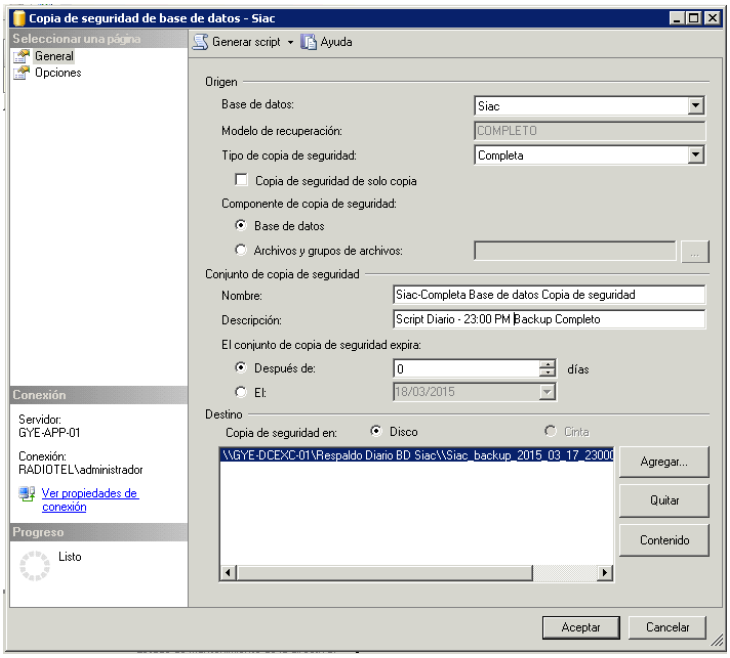
DATOS DE CONEXIÓN A LA BASE DE DATOS

FUENTE: SERVIDOR BASE DE DATOS CDC

ELABORADO POR: William Moscol Criollo

ILUSTRACIÓN No. 7

DESCRIPCIÓN DEL SCRIPT PARA LA COPIA DE SEGURIDAD DE LA BASE DE DATOS



FUENTE: SERVIDOR BASE DE DATOS CDC

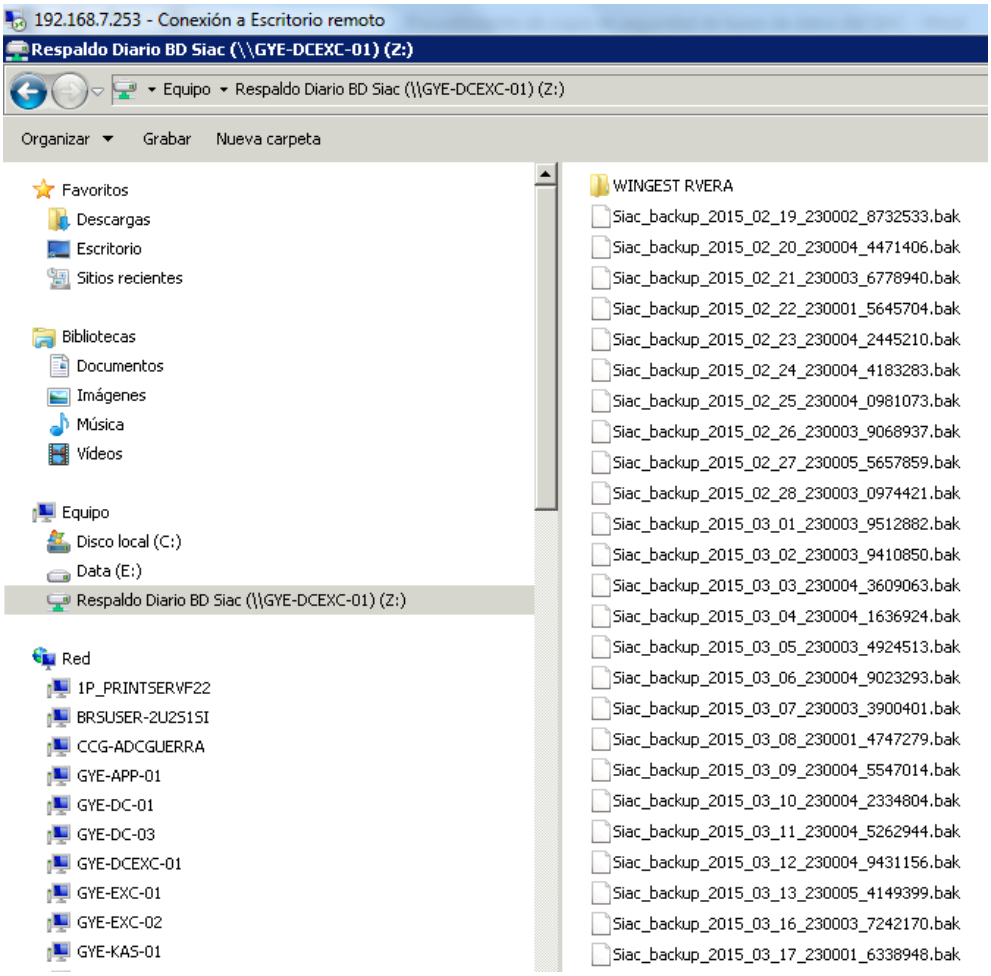
ELABORADO POR: William Moscol Criollo

El monitoreo del respaldo debe ser a diario y verificar que se encuentre generado correctamente el archivo .BAK.

- Se debe ingresar vía remota al servidor SIAC – 192.168.7.253 – GYE-APP-01
- Verificar desde el explorador de Windows en la unidad de red si está el respaldo a la fecha.

ILUSTRACIÓN No. 8

HISTORIAL DE COPIAS DE SEGURIDAD



FUENTE: SERVIDOR BASE DE DATOS CDC

ELABORADO POR: William Moscol Criollo

- En la unidad externa se alojan máximo 40 copias de seguridad, es decir de los últimos 40 días.
- La unidad externa debe ser depurada constantemente de los respaldos antiguos para permitir la creación del respaldo diario.

Procedimiento de Copia Semanal SIAC

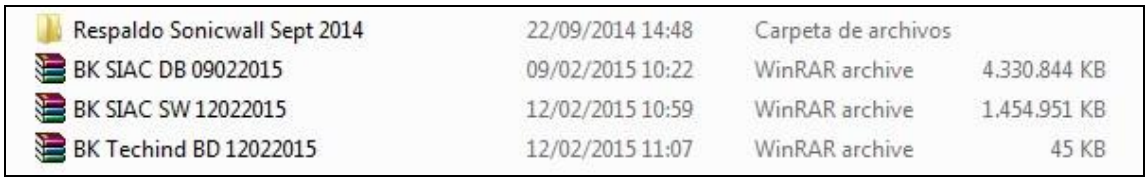
Consiste en guardar en un medio externo (DVD) a inicio de semana (lunes) la base de datos del SIAC comprimida en formato .RAR

El contenido del DVD consta de lo siguiente:

- Respaldo Base de Datos SIAC (Semanal)
- Respaldo de software SIAC (Semanal)
- Respaldo de archivos de marcaciones del biométrico TECHIND (Semanal)
- Respaldo Firewall Sonicwall NSA 250M (Mensual)
- Respaldo Consola Kasperky Endpoint (Mensual)

ILUSTRACIÓN No. 9

CONTENIDO DEL DVD



FUENTE: SERVIDOR BASE DE DATOS CDC
ELABORADO POR: William Moscol Criollo

El nombre de los archivos tiene la siguiente nomenclatura:

[Backup] [Nombre del programa] [Tipo de archivo respaldado (Software o Base de Datos)] [Fecha], que en abreviaturas seria lo siguiente: BK SIAC DB 18032015.

El DVD debe ser entregado a dirección administrativa todos los lunes y en la etiqueta del DVD se debe indicar fecha de respaldo realizado.

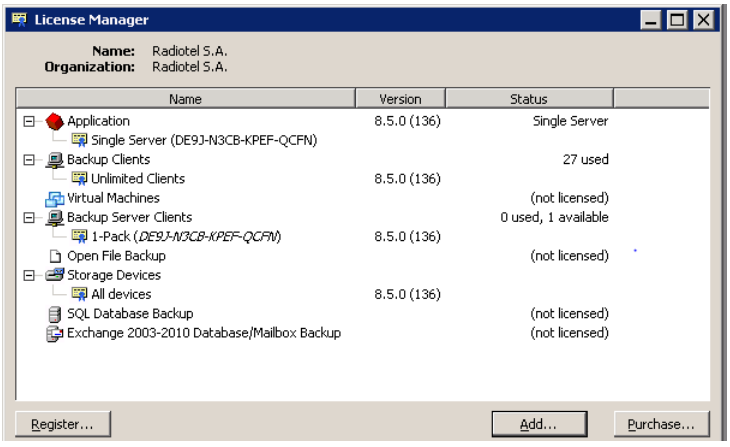
Procedimiento de copia de seguridad de usuarios con aplicación Retrospect 8.5

Retrospect.- aplicación utilizada para el manejo de respaldos automatizados en equipos clientes seleccionados.

- Trabaja con una sola licencia que está instalada en el servidor.
- El número de clientes es ilimitado, se debe tener en cuenta el medio de almacenamiento que tenga el suficiente espacio.

ILUSTRACIÓN No. 10

DETALLE DE LICENCIAS RETROSPECT 8.5



FUENTE: SERVIDOR BASE DE DATOS CDC
ELABORADO POR: William Moscol Criollo

A continuación los datos donde se encuentra la consola de administración:

Nombre del Equipo: GYE-RET-01

IP: 192.168.7.243

Sistema Operativo: Windows Server 2008 R2

Ubicación de Respaldos: unidad *"E"* con el nombre *"RetroData"* con 2 TB asignados.

ILUSTRACIÓN No. 11

UBICACIÓN DE RESPALDOS

FUENTE: SERVIDOR BASE DE DATOS CDC
ELABORADO POR: William Moscol Criollo

- Para el proceso de copia de seguridad se usa un disco duro de red (NAS) conectado físicamente al servidor con configuración ISCSI.
- El volumen se encuentra montado con el nombre de *"RetroData"* con la letra *"E"* asignada.
- Maneja un arreglo de discos duros tipo RAID 5.
- Datos técnicos de Disco NAS:

CUADRO No. 7

DATOS DE CONEXIÓN DEL REPOSITORIO DE COPIAS DE SEGURIDAD

IP	NAME	MARCA	MODELO	CAPAC.
192.168.7.234	GYE-NAS-01	IOMEGA	NAS STORECENTER IX4-200D	4 TB

FUENTE: SERVIDOR BASE DE DATOS CDC
ELABORADO POR: William Moscol Criollo

ILUSTRACIÓN No. 12

ESQUEMA DE RESPALDOS CLIENTES CON RETROSPECT 9.0

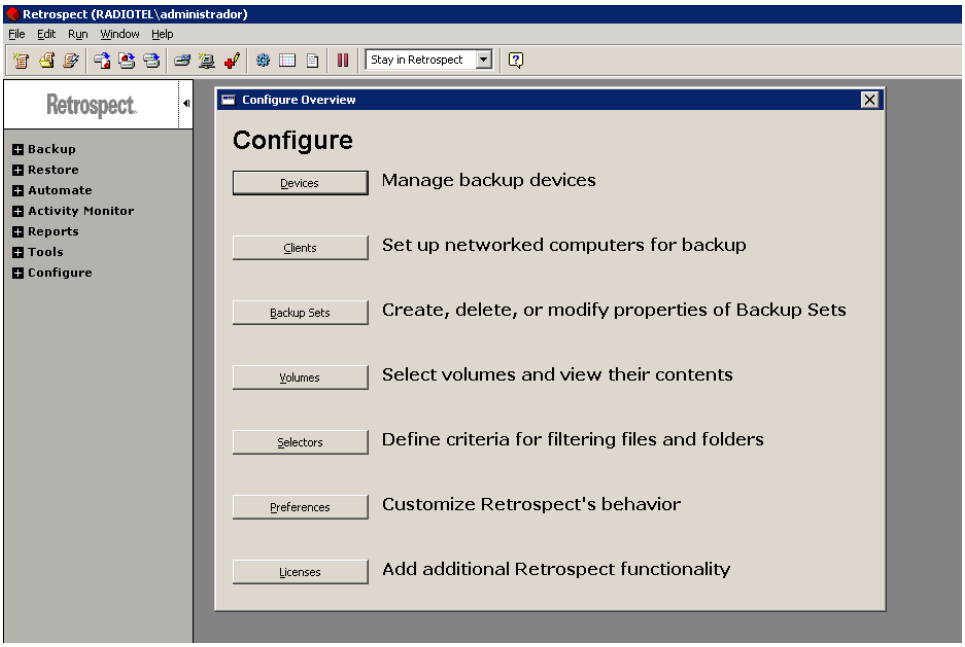
ELABORADO POR: William Moscol Criollo

Para el inicio de la aplicación se encuentra en menú inicio Retrospect 9.0

La interfaz muestra de manera predeterminada las opciones de configuración

ILUSTRACIÓN No. 13

INTERFAZ DE ADMINISTRACIÓN DEL SOFTWARE RETROSPECT 9.0



FUENTE: SERVIDOR RETROSPECT 9.0 CDC

ELABORADO POR: William Moscol Criollo

Los programas de respaldo trabajan creando catálogos, de esta manera se logra comprimir al máximo la información y el proceso de copia se realiza de manera más rápida.

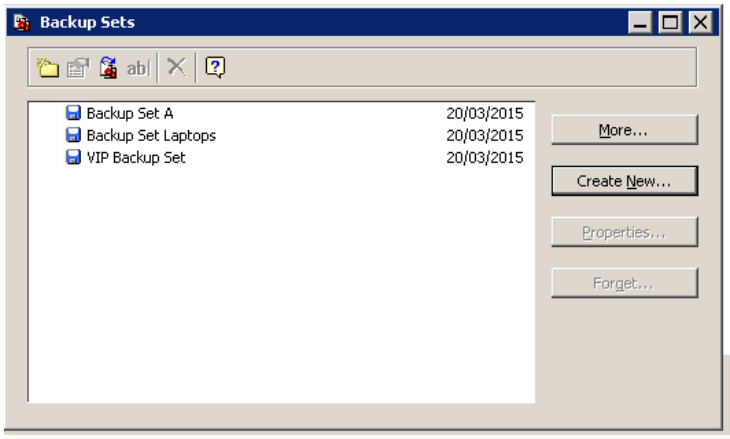
En nuestro caso se encuentran creados 3 “Backup Set”.

- Backup Set A: Respaldo Desktop, Se ejecuta de manera diaria 13:05 PM, es respaldo tipo incremental.
- Backup Set Laptops: Respaldo equipos portátiles, se ejecuta de manera diaria cuando el equipo se encuentre disponible en la red, es respaldo tipo incremental.
- VIP Backup Set: Respaldo Gerencia, se ejecuta de manera diaria cuando el equipo se encuentre disponible en la red, es respaldo tipo incremental.

ILUSTRACIÓN No. 14

CONFIGURACIÓN DE CATÁLOGOS DE DATOS RETROSPECT 9.0

Entre las opciones para el monitoreo diario están: Active monitor-proactive

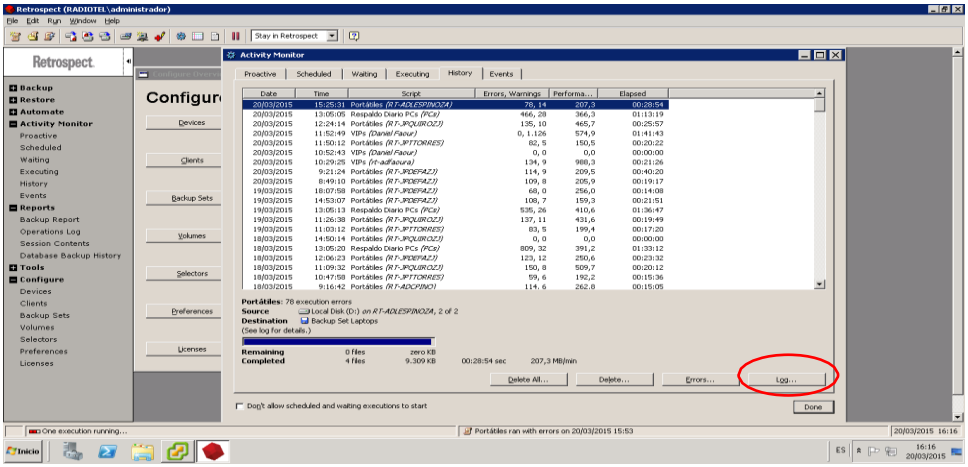


FUENTE: SERVIDOR RETROSPECT 9.0 CDC

ELABORADO POR: William Moscol Criollo

ILUSTRACIÓN No. 15

VENTANA ACTIVE MONITOR



FUENTE: SERVIDOR RETROSPECT 9.0 CDC

ELABORADO POR: William Moscol Criollo

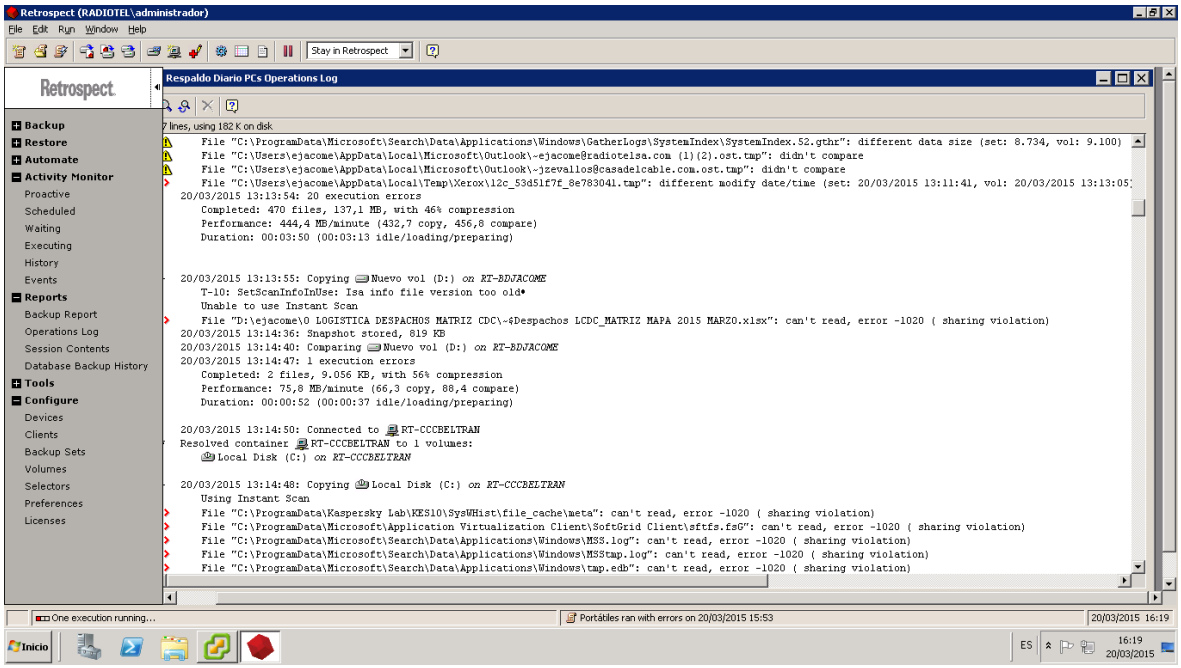
Si requiere ver un historial más detallado está la opción de LOG donde muestra que archivos y a que clientes se les hizo el respaldo.

Entre las políticas asignadas de tipo de archivo están:

- No se copia archivos mayores a 200 MB.
- No se copia archivos de *.mp3, *.mp4, *avi
- Agregada las exclusiones de archivos del sistema.
- Se copia todo el perfil de Windows del usuario a excepción de los archivos mencionados anteriormente.

ILUSTRACIÓN No. 16

INTERFAZ LOG DEL RESPALDO EN EJECUCIÓN



FUENTE: SERVIDOR RETROSPECT 9.0 CDC

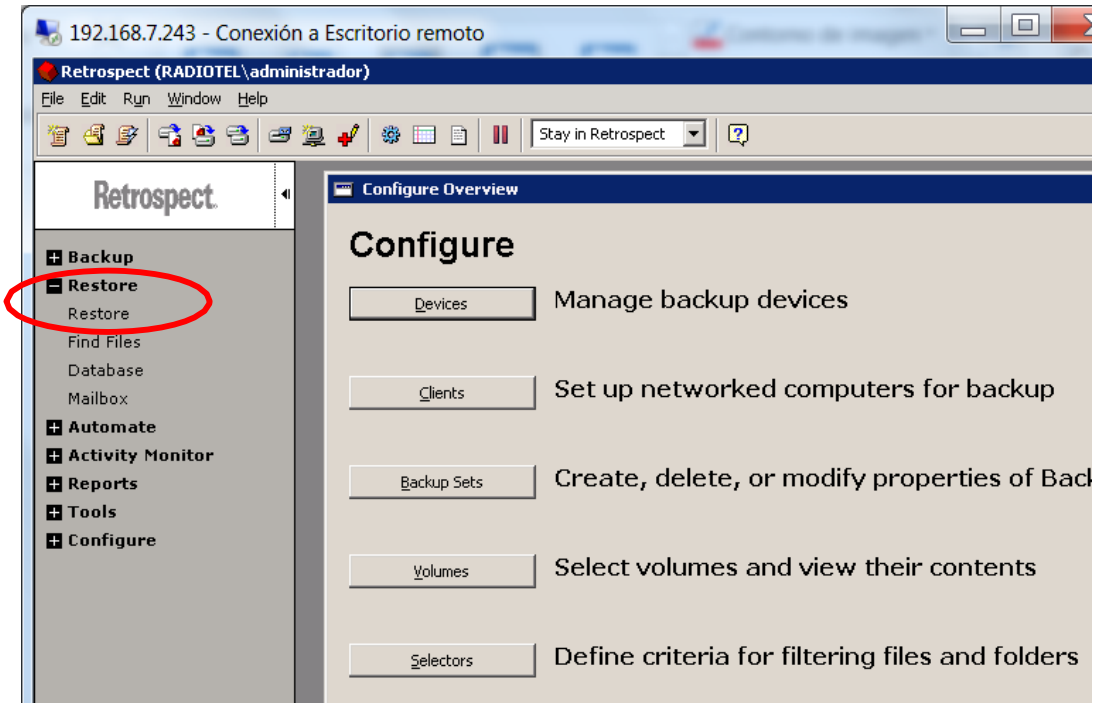
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Restauración de copia de seguridad Retrospect.

Desde la opción: Restorer--restore.

ILUSTRACIÓN No. 17

INTERFAZ OPCIÓN DE RESTAURACIÓN RETROSPECT 9.0



FUENTE: SERVIDOR RETROSPECT 9.0 CDC

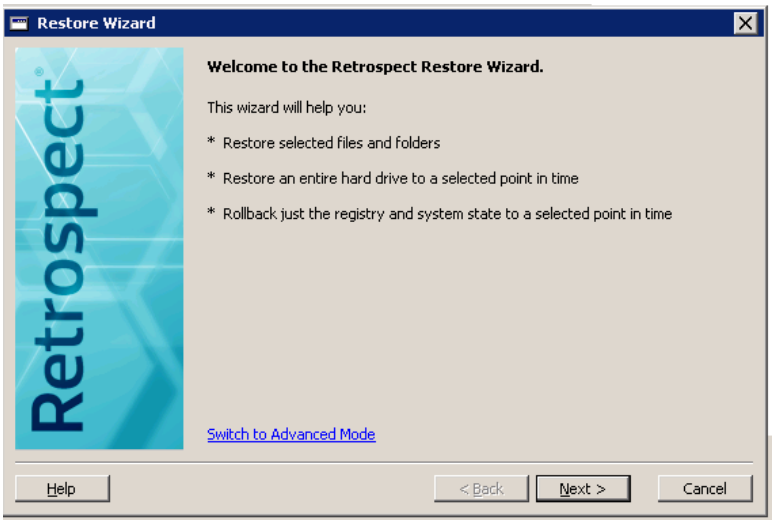
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Se ejecuta el wizard donde se debe elegir:

- Tipo de respaldo (archivo, carpeta, perfil de windows)
- Elegir el backup set donde se encuentra alojado el respaldo.
- Elegir destino donde desea restaurar.

ILUSTRACIÓN No. 18

INTERFAZ WIZARD OPCIÓN DE RESTAURACIÓN RETROSPECT



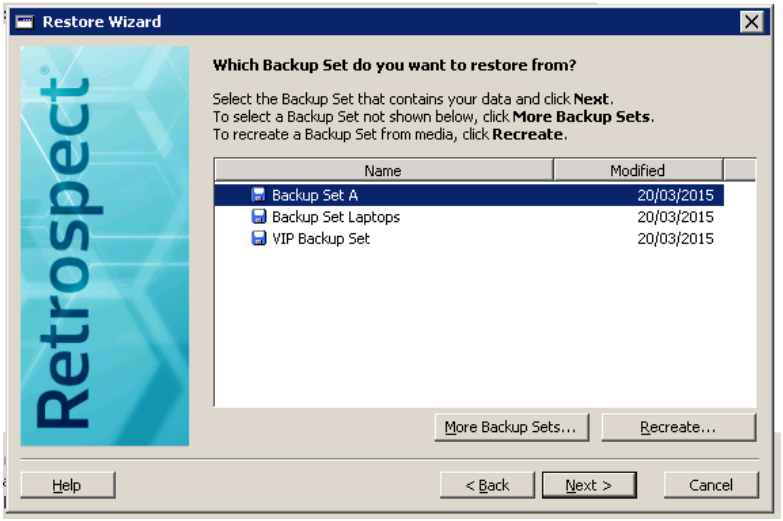
FUENTE: **SERVIDOR RETROSPECT 9.0 CDC**

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Elegir el backup set donde se encuentra alojado el respaldo

ILUSTRACIÓN No. 19

ELEGIR CATÁLOGO DE DATOS A RESTAURAR



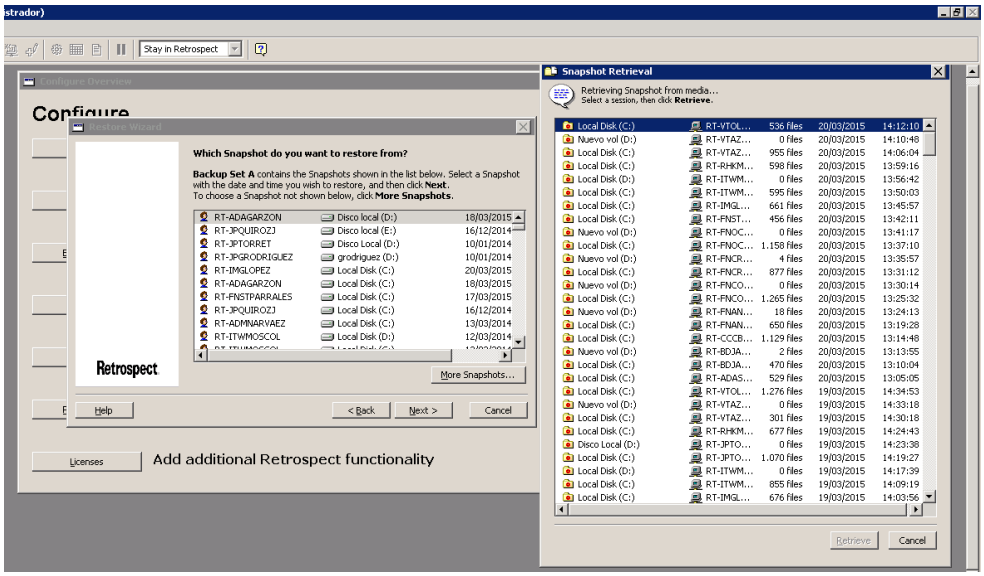
FUENTE: SERVIDOR RETROSPECT 9.0 CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Seleccionar usuario, y unidad de disco a restaurar (puede ser una carpeta, archivo, o perfil).

ILUSTRACIÓN No. 20

ELEGIR PERFIL DE USUARIO A RESTAURAR



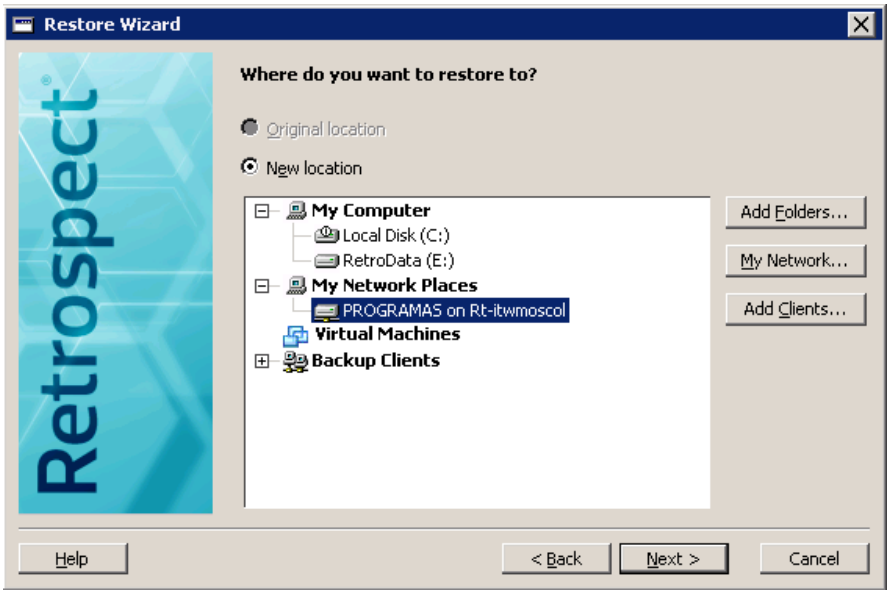
FUENTE: SERVIDOR RETROSPECT 9.0 CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Elegir destino donde desea restaurar copia de seguridad.

ILUSTRACIÓN No. 21

ELEGIR DESTINO A DONDE RESTAURAR



FUENTE: SERVIDOR RETROSPECT 9.0 CDC

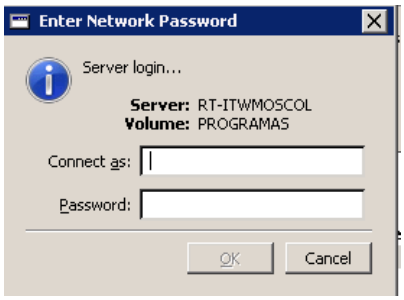
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Ingresar contraseña de autenticación entre cliente-servidor:

Contraseña: xxxxxx

ILUSTRACIÓN No. 22

INGRESAR CONTRASEÑA DE AUTENTICACIÓN CLIENTE-SERVIDOR



FUENTE: SERVIDOR RETROSPECT 9.0 CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Por último se confirma destino y el proceso de restauración comienza, el tiempo de restauración depende del tamaño en MB de la copia de seguridad.

MANUAL DEL PLAN DE CONTINGENCIA IT PARA LA COMPAÑÍA CASA DEL CABLE S.A

Actualmente CASA DEL CABLE S.A. cuenta con varias herramientas de contingencia informática, cada una cumple funciones diferentes:

- **Retrospect 9.0-** utilizado para respaldos de clientes Windows y mac.
- **Microsoft Office 365.-** cliente de correo, su potencial característica es su portabilidad ya que el servicio se encuentra alojado en la nube.
- **Veeam Avaliable Suite v8-** software para la administración de respaldos de máquinas virtuales VMware y réplicas de las mismas en sitios alternos.

OBJETIVOS DEL MANUAL DE PLAN DE CONTINGENCIA

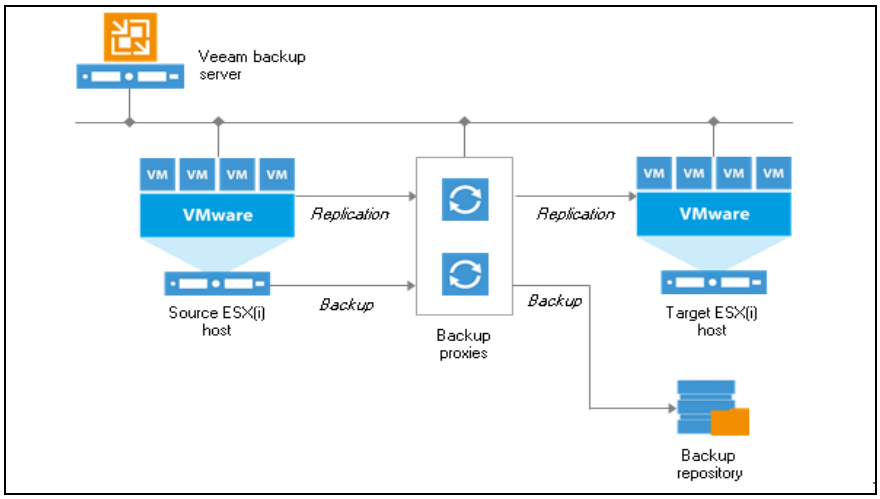
- Mejorar la continuidad de negocio con protección de datos casi continua para cualquier aplicación virtualizada.
- Mantener réplicas basadas en imagen ya sea on-site para conseguir alta disponibilidad u off-site para recuperación ante desastres.
- Replicar sin afectar su entorno de producción (Retrospect, 2015)

PLAN DE RECUPERACIÓN DE DESASTRES UTILIZANDO EL SOFTWARE VEEAM AVALIABLE SUITE V8

Veeam V8 mediante una interfaz gráfica permite la administración de las copias de seguridad de los servidores virtuales ejecutándose, réplicas de máquinas virtuales en un sitio alterno que en este caso sería en la sucursal de Guayaquil.

ILUSTRACIÓN No. 23

ESQUEMA BÁSICO DEL FUNCIONAMIENTO DE RÉPLICA Y COPIAS DE SEGURIDAD DE SERVIDORES



FUENTE: www.veeam.com/es

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

INSTALACIÓN

Veeam Suite 8 mediante su interfaz inteligente y fácil manejo permite identificar de manera inmediata cualquier tipo de eventualidad.

Se encuentra instalado en una máquina virtual con los siguientes datos y características:

- Sistema operativo Windows Server 2012 Standard R2 64 bits
- Memoria RAM 12 GB
- Disco Duro 60 GB
- Partición de 300 GB y 600 GB.- repositorio para almacenamiento de copias de seguridad, físicamente es un disco duro NAS SYNOLOGY 3TB X 4, RAID 10.

ACCESO

El acceso para el monitoreo se lo puede realizar de varias formas:

- RDP (Acceso Remoto)
- VMware client 5.5
- VMware web (VCenter)

De forma rápida y ágil es recomendable acceder de manera remota usando los siguientes datos desde cualquier equipo Windows o Mac con el asistente de conexión remota de Windows:

MATRIZ

Nombre del equipo: GYE-VBR-01

IP: 192.168.7.232

SUCURSAL

Nombre del equipo: GYE-VBR-02

IP: 192.168.5.11

ILUSTRACIÓN No. 24

CONEXIÓN REMOTA AL SERVIDOR VEEAM

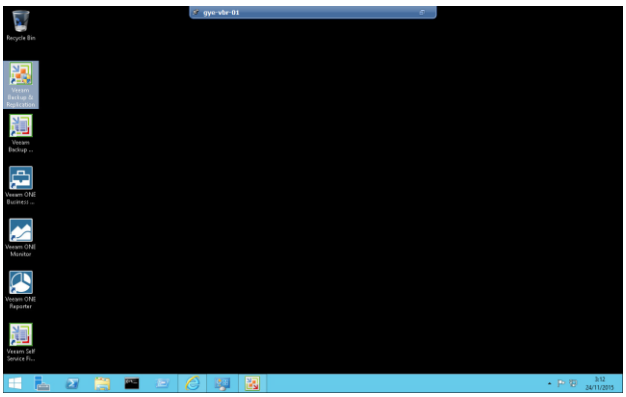
FUENTE: SERVIDOR VEEAM CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

El acceso remoto solicitara las credenciales del administrador de sistemas, en este caso personal del área es el responsable del usuario y contraseña.

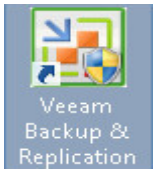
ILUSTRACIÓN No. 25

INTERFAZ DEL ESCRITORIO WINDOWS 2012 R2



FUENTE: SERVIDOR VEEAM CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

El software para monitoreo y activación de cualquier contingencia es el VEEAM BACKUP & REPLICATION 

Desde la consola de administración puede tomar el control de todo su entorno virtual y de backup. Al utilizar todas las características y capacidades de la tecnología de virtualización y backup de Veeam, usted puede descubrir y recibir las alertas de los problemas antes de que afecten a la producción.
Permite:

- Monitoreo en tiempo real y alertas, 24x7: Le envían notificaciones sobre los problemas de backup y rendimiento

- Optimización de los recursos y la planificación de la capacidad: Elimina las conjeturas del proceso de planificación y suministra visibilidad al uso de los recursos

- Informes completamente personalizables: Simplifica el cumplimiento de las políticas de backup y los requisitos de las auditorías

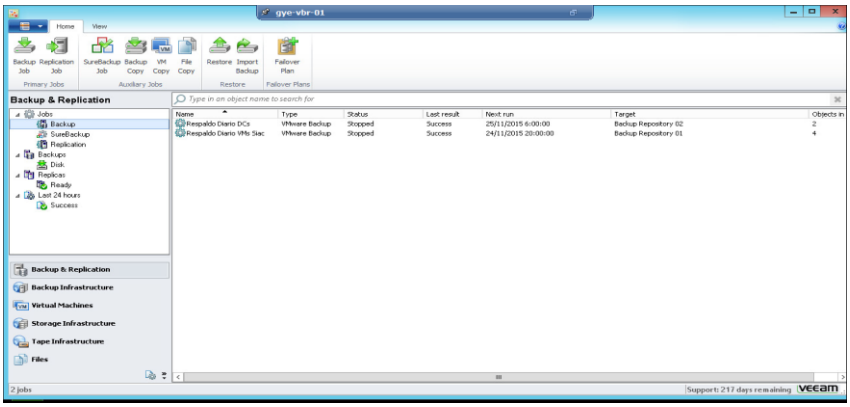
- Aproveche una profunda integración con el soporte vSphere Web Client Plug-in que es el que se usa actualmente en CASA DEL CABLE S.A.

CONFIGURACIÓN

En la siguiente gráfica se muestra todos los componentes de la aplicación, a continuación el detalle de las mismas.

ILUSTRACIÓN No. 26

INTERFAZ DEL SERVIDOR VEEAM SUITE V8



FUENTE: SERVIDOR VEEAM CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

JOBS.- se definen las tareas programadas de manera periódica, existen 3 tareas creadas actualmente.

- **Respaldo Diario DCs:** esta tarea es la encargada de realizar las copias de seguridad de las máquinas virtuales que cumplen la *función de servidor de controlador de dominio* que están identificados en la red con el nombre de:

  - **GYEDC01 (pesa aprox. 240 GB)**
  - **GYEDC02 (pesa aprox. 40 GB)**

  Programación: el respaldo lo realiza todos los días a las 6am.

Tipo de copia de seguridad: las copias son de tipo incremental, es decir copia los últimos cambios efectuados y midiendo tiempos se tarda aproximadamente 30 minutos en guardar los cambios detectados.

Los respaldos que se conservan son de los últimos 7 días de haberse realizado la copia.

Almacenamiento: se encuentran físicamente guardadas en una unidad de disco de red (NAS), dividido en 2 grupos:

300 GB - Repositorio 1: Copias de seguridad de servidores DC.

600 GB - Repositorio 2: Copias de seguridad de servidores críticos.

- **Respaldo Diario VMs SIAC:** esta tarea es la encargada de realizar las copias de seguridad de las máquinas virtuales ¨críticas¨ en la compañía CASA DEL CABLE S.A. que cumplen varias funciones identificados en la red con el nombre de:

    - **GYE-WEB-APP-02:** Servidor Facturación Electrónica
    - **GYEAPP01:** Servidor de aplicaciones SIAC
    - **GYESQL01:** Servidor de Base de datos SIAC
    - **GYEWEBAPP:** Servidor de aplicaciones CRM.

Programación: el respaldo lo realiza todos los días a las 20:00 PM.

Tipo de copia de seguridad: las copias son de tipo incremental, es decir copia los últimos cambios efectuados y midiendo tiempos se tarda aproximadamente 45 minutos en guardar los cambios recientes.

Los respaldos que se conservan son de los últimos 7 días de haberse realizado la copia.

Almacenamiento: se encuentran físicamente guardadas en una unidad de disco de red (NAS), dividido en 2 grupos:

300 GB - Repositorio 1: Copias de seguridad de servidores DC.
600 GB - Repositorio 2: Copias de seguridad de servidores críticos

En el sitio alterno se encuentra creada una partición en el servidor identificada como:

400 GB - Repositorio 3: Repositorio para réplicas en sitio alterno.

- **Réplica SIAC:** tarea encargada de sincronizar las máquinas virtuales SIAC con el sitio alterno ubicado en la sucursal de Guayaquil.

    - **GYEAPP01:** Servidor de aplicaciones SIAC
    - **GYESQL01:** Servidor de Base de datos SIAC

Se escogió replicar los 2 servidores virtuales por ser considerados servicios críticos en la empresa y que pueda afectar la operatividad de la misma.

Otro de los servicios que se encuentran replicando en sucursal es el controlador de dominio secundario, la réplica se realiza mediante la técnica RODC.
Actualmente existen 3 servidores controladores de dominio replicando entre sí.

CUADRO No. 8

SERVIDORES DE DOMINIO REPLICÁNDOSE ENTRE SI

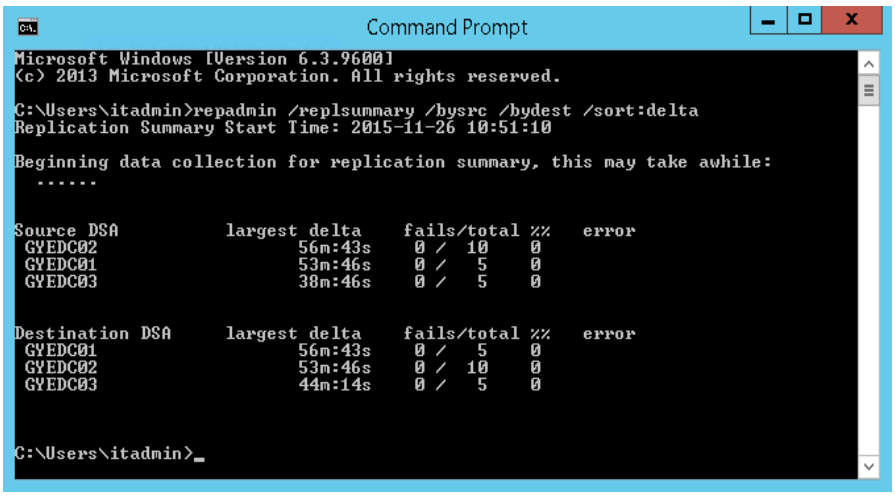
NOMBRE DEL EQUIPO	IP	FUNCIÓN	UBICACION
GYEDC01	192.168.7.1	Controlador de Dominio primario	MATRIZ-MAPASINGUE
GYEDC02	192.168.7.2	Controlador de dominio secundario	MATRIZ-MAPASINGUE
GYEDC03	192.168.5.10	Controlador de dominio secundario	SUCURSAL GYE-9DEOCT

FUENTE: INVENTARIO DE EQUIPOS CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

En la siguiente gráfica se observa las réplicas que están funcionando de manera correcta.

ILUSTRACIÓN No. 27

RÉPLICA DE SERVIDORES DE CONTROLADOR DE DOMINO



FUENTE: SERVIDORES DC CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

BACKUPS.- nos muestran los repositorios configurados para el almacenamiento de las copias de seguridad mencionados anteriormente.

ILUSTRACIÓN No. 28

DETALLE DE REPOSITORIOS DE RÉPLICA Y RESPALDOS

Name	Type	Host	Path	Capacity	Free
Backup Repository 01	Windows	This server	E:\Backups	299.9 GB	148.8 GB
Backup Repository 02	Windows	This server	F:\Backups	599.9 GB	426.7 GB
Backup Repository 3	Windows	gye-vbr-02.ad.casadelcable.com	E:\Backups	399.9 GB	248.1 GB

FUENTE: SERVIDORES DC CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

ILUSTRACIÓN No. 29

DISCO DURO

FUENTE: SERVIDORES DC CDC

Físicamente se almacenan en un disco duro NAS.

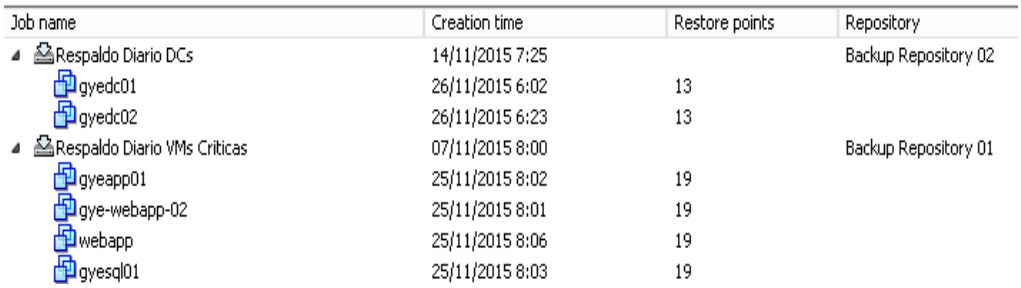
MARCA: SYNOLOGY

MODELO: DS414

CAPACIDAD: 3TB X 4 (RAID1-RAID5-RAID10)

ILUSTRACIÓN No. 30

DETALLE DE SERVIDORES VIRTUALES RESPALDÁNDOSE



Job name	Creation time	Restore points	Repository
Respaldo Diario DCs	14/11/2015 7:25		Backup Repository 02
gyedc01	26/11/2015 6:02	13	
gyedc02	26/11/2015 6:23	13	
Respaldo Diario VMs Criticas	07/11/2015 8:00		Backup Repository 01
gyeapp01	25/11/2015 8:02	19	
gye-webapp-02	25/11/2015 8:01	19	
webapp	25/11/2015 8:06	19	
gyesql01	25/11/2015 8:03	19	

FUENTE: SERVIDORES DC CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

RÉPLICAS.- desde esta opción nos permite monitorear el estado de la replicación de datos hacia el sitio alterno

CUADRO No. 9

DETALLE DE RÉPLICAS DE SERVIDORES VIRTUALES

JOB NAME	STATUS	ORIGINAL LOCATION	RÉPLICA LOCATION
Réplica SIAC	Ready	192.168.7.233	192.168.5.145
Réplica SIAC	Ready	192.168.7.233	192.168.5.145

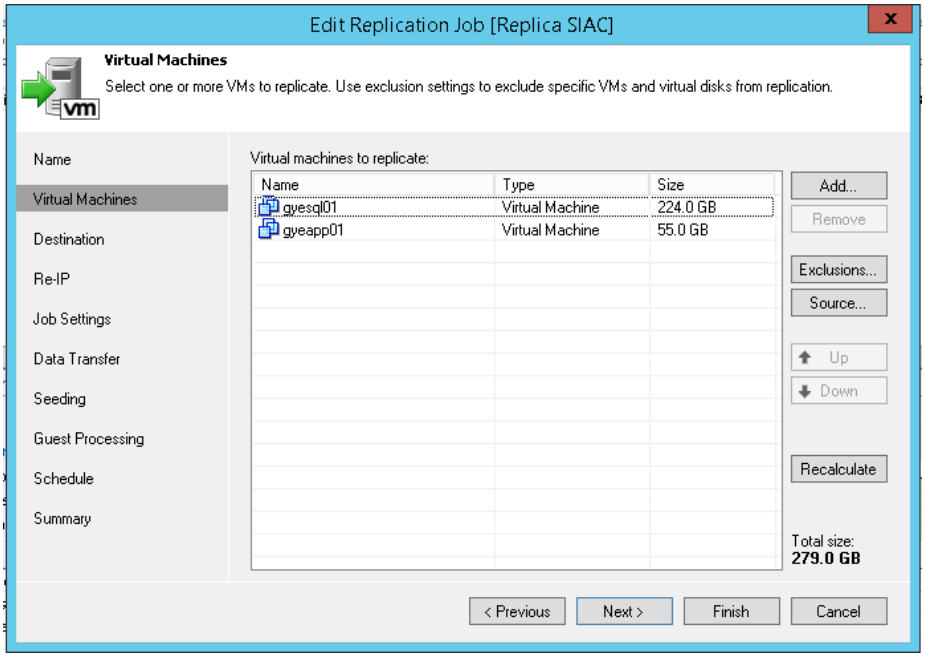
FUENTE: SERVIDORES DC CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

Los servidores virtuales configurados para que se estén replicando son el servidor de aplicaciones SIAC y el de base de datos SIAC.

Entre los 2 servidores virtuales replicándose al sitio alterno usan de espacio en disco 279 GB de 400 GB asignados actualmente.

ILUSTRACIÓN No. 31

INTERFAZ DONDE MUESTRA VM REPLICÁNDOSE



FUENTE: SERVIDORES DC CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

TRANSFERENCIA DE DATOS.- Veeam V8 cuenta con varias características que permiten una copia de datos y transferencia de datos de manera ágil y sencilla, entre su característica principal tenemos **"Aceleración de WAN integrada",** es decir trabaja con cachés en ambos puntos tanto en ORIGEN como DESTINO, de esta manera no satura el canal de datos de 2Mbps asignados para la replicación de datos.

¿Qué es Aceleración de WAN integrada?

Un acelerador WAN reduce la cantidad de datos que necesita transferirse por la WAN usando técnicas de caché y compresión de datos. Básicamente, un acelerador WAN trabaja haciendo caché de los archivos duplicados (o partes de archivos) de forma que puedan referenciarse en el caché global, en lugar de tener que enviarse por la WAN nuevamente. Los aceleradores WAN compensan de forma eficiente el I/O de la red para el I/O de disco, mejorando significativamente el rendimiento de las transferencias de datos sobre la red en

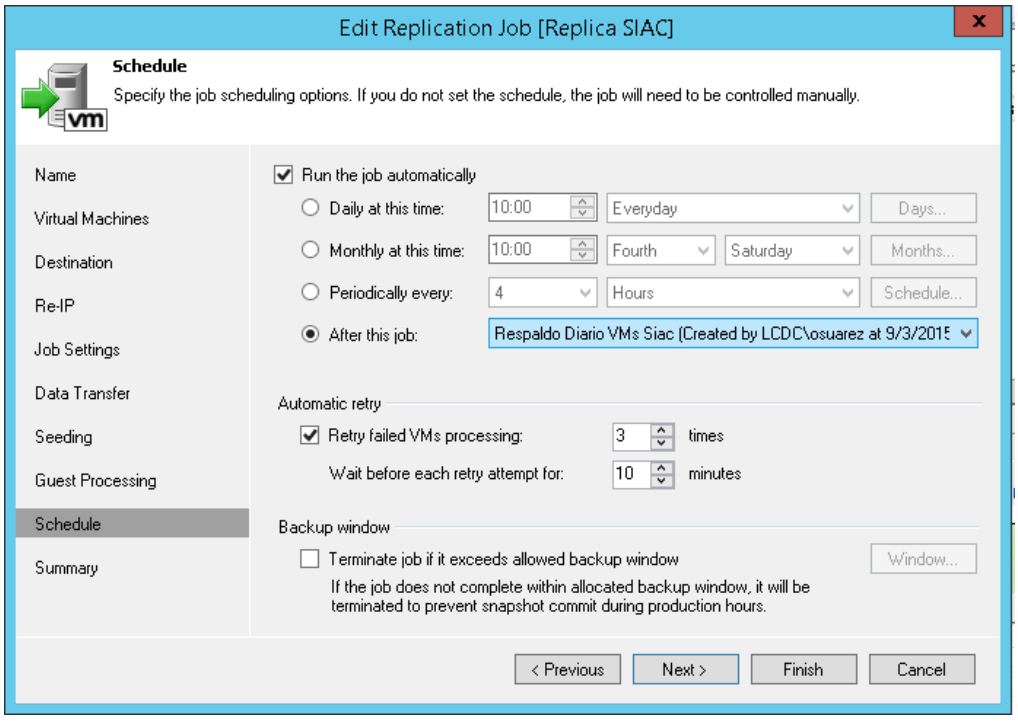
situaciones cuando el ancho de banda representa el principal cuello de botella. (8.0, 2015)

En la gráfica podemos observar el origen y destino y activando la función WAN Accelerators.

PROGRAMACIÓN DE LA RÉPLICA.- la ejecución de la réplica de datos al sitio alterno se la realiza en horarios nocturnos todos los días, en este caso está configurada para que se ejecute luego de haber culminado la tarea del "respaldo diario VMs SIAC", es decir de 20:30 PM en adelante.

ILUSTRACIÓN No. 32

INTERFAZ DONDE MUESTRA CONFIGURACIÓN DE LA PROGRAMACIÓN DE RÉPLICAS



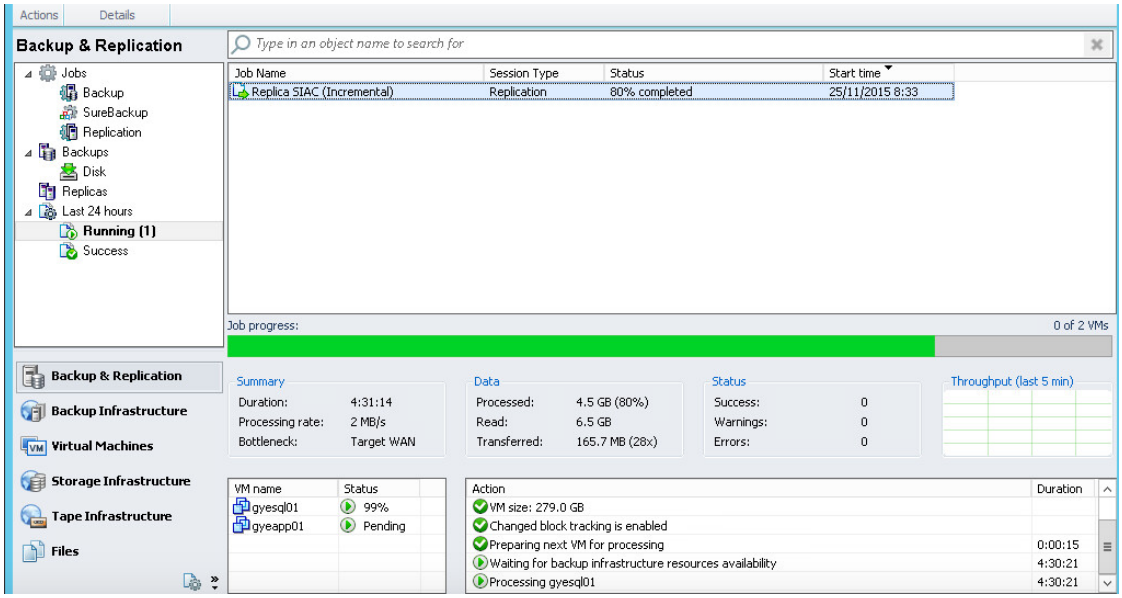
FUENTE: SERVIDOR VEEAM CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

ULTIMAS 24 HORAS.- desde esta opción se monitorea los trabajos ejecutándose o si se realizaron correctamente en las últimas 24 horas como se puede observar en la gráfica.

ILUSTRACIÓN No. 33

INTERFAZ DONDE MUESTRA LOG DE RÉPLICA EN PRODUCCIÓN



FUENTE: SERVIDOR VEEAM CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

ILUSTRACIÓN No. 34

INFRAESTRUCTURA UTILIZADA POR EL SOFTWARE VEEAM 8.0 PARA COPIAS DE SEGURIDAD Y RÉPLICA DE DATOS EN UN SITIO ALTERNO

SITIO PRIMARIO
LOCALIDAD: MATRIZ GYE-MAPASINGUE

PLATAFORMA: VMware Vsphere Enterprise 6.0

- **Servidor Controlador de Dominio**
- **Servidor Base de datos SQL 2012**
- **Servidor de Aplicaciones (SIAC)**
- **Servidor Web**
- **Servidor Veeam-01**

DISCO DURO NAS SYNOLOGY

Sirve de repositorio de las copias de seguridad de los servidores virtuales ejecutándose

SITIO SECUNDARIO
LOCALIDAD: SUCURSAL GYE-9DEOCT

PLATAFORMA: VMware Vsphere Enterprise 6.0

- **Servidor Controlador de Dominio Secundario**
- **Servidor Réplica Base de datos SQL 2012**
- **Servidor Réplica de Aplicaciones (SIAC)**
- **Servidor Veeam-02**

ENLACES DE DATOS DE 2 Mbps C/U CON EL PROVEEDOR LEVEL3 Y CLARO

FUENTE: INFRAESTRUCTURA SERVIDORES CDC
ELABORADO POR: William Moscol Criollo

Para la implementación de la herramienta VEEAM V8 se invirtió en hardware que cumpla los requisitos para el correcto funcionamiento del software.

CUADRO No. 10

DATOS TÉCNICOS DE SERVIDORES A UTILIZARSE

SERVIDOR 01			
Marca: IBM	**Modelo:** XSERIES 3550 M3	**Serie:** 06VVF57	**P/N:** 794452U
Procesador: Procesador Intel Xeon 2.40GHz X 12	**Memoria RAM:** 48 GB	**Disco Duro:** 600GBX4 – 300GBX4	
Ubicación: Casa del Cable - Matriz Mapasingue			

FUENTE: INFRAESTRUCTURA SERVIDORES CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

CUADRO No. 11

DATOS TÉCNICOS DE SERVIDORES A UTILIZARSE

SERVIDOR 02			
Marca: IBM	**Modelo:** XSERIES 3650 M3	**Serie:** KQ42L6B	**P/N:** 7945G2U
Procesador: Procesador Intel Xeon 2.60GHz X 8	**Memoria RAM:** 44 GB	**Disco Duro:** 600GB X 4 – 300GB X 4	
Ubicación: Casa del Cable – Sucursal Gye – 9deOct			

FUENTE: INFRAESTRUCTURA SERVIDORES CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

CUADRO No. 12

HARDWARE DE ALMACENAMIENTO

DISCO NAS			
Marca: SYNOLOGY	**Modelo:** DS414	**Serie:**	**P/N:**
Procesador: Mindspeed Comcerto C2000 1.2 GHZ	**Memoria RAM:** 512 MB	**Disco Duro:** 3TB X 4	
Ubicación: Casa del Cable – Matriz Mapasingue			

FUENTE: INFRAESTRUCTURA SERVIDORES CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

PROCEDIMENTO A SEGUIR ANTE UNA CONTINGENCIA INFORMATICA

Una vez explicado a detalle de las tareas, almacenamiento, réplicas e infraestructura en general, se debe especificar el procedimiento a seguir en caso de alguna contingencia del sistema de facturación y aplicaciones en general.

Una de las ventajas del software Veeam V8 es que permite una administración sencilla como por ejemplo el de solo dar un clic para encender un servidor virtual.

1.- Como primer paso se debe ingresar al servidor de réplica ubicado en el sitio alterno (sucursal gye) que puede ser de las siguientes maneras:

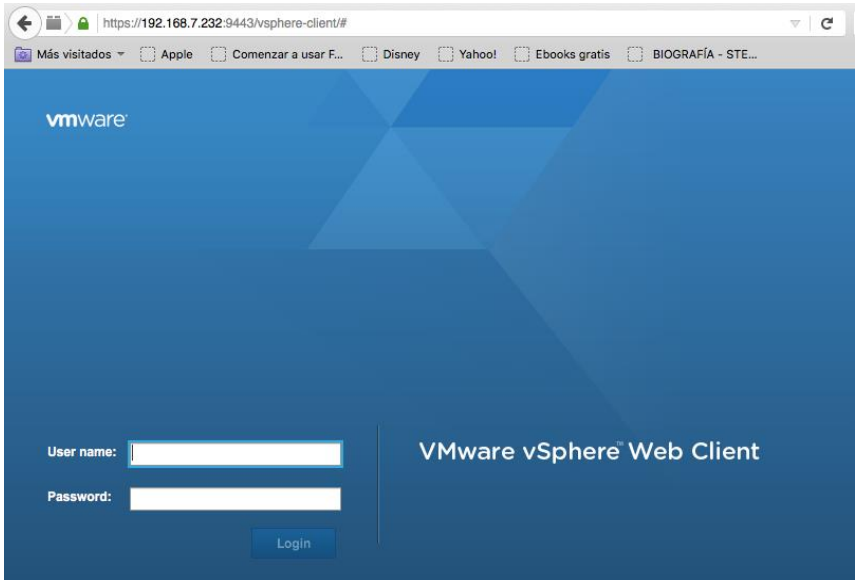
- Desde cualquier browser (Chrome, mozilla, IE) ingresar a la siguiente dirección:

  https://192.168.7.232:9443/vsphere-client/#

- Mediante la dirección adjunta accedemos a la administración de los servidores virtuales.

ILUSTRACIÓN No. 35

ACCESO WEB AL SERVIDOR VCENTER



FUENTE: INFRAESTRUCTURA SERVIDORES CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

- Ingresamos los siguientes datos:

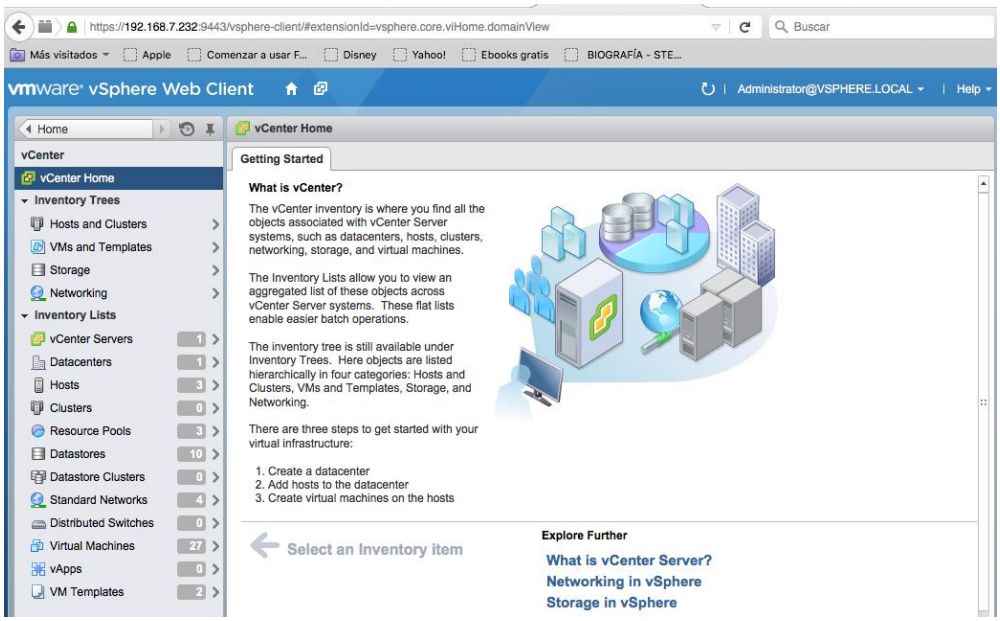
    - User name: administrator@vsphere.local
    - Password: xxxxx

- Luego se elige la opción VCENTER HOME, aquí es donde nos va a mostrar los servidores virtuales ejecutándose o que se encuentren apagados.

- Se muestra el listado de servidores físicos activos y estos a su vez contienen servidores virtuales ejecutándose.

ILUSTRACIÓN No. 36

INTERFAZ WEB DEL SERVIDOR VCENTER DE CDC

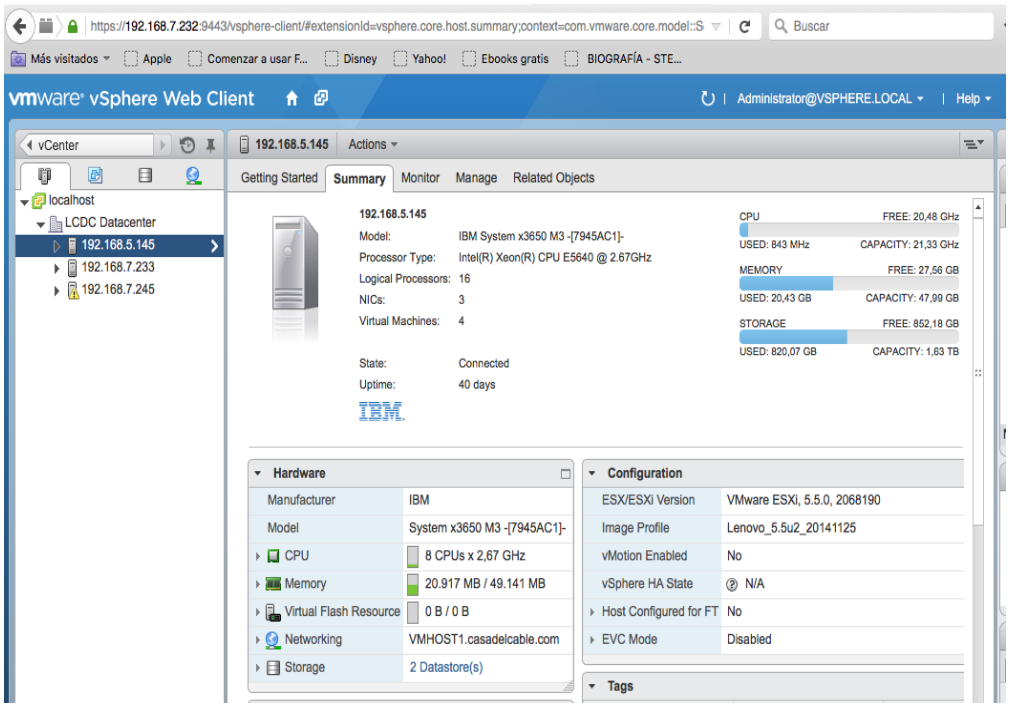


FUENTE: INFRAESTRUCTURA SERVIDORES CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

ILUSTRACIÓN No. 37

DETALLE DE LOS HOST VM EN DESDE LA INTERFAZ WEB



FUENTE: INFRAESTRUCTURA SERVIDORES CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

192.168.5.145 – UBICADO EN EL SITIO ALTERNO – SUCURSAL GYE

192.168.7.233 – UBICADO EN MATRIZ GYE

192.168.7.245 – UBICADO EN MATRIZ GYE

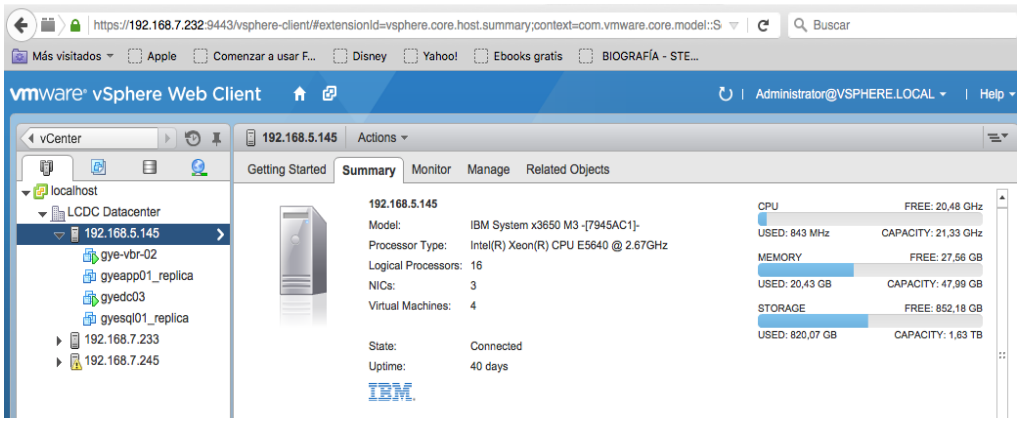
- Clic sobre en el menú desplegable ▼ 192.168.5.145, muestra los servidores virtuales ejecutándose e identificamos los que estén en producción y los que estén apagados.

SERVIDOR VIRTUAL EN PRODUCCION

SERVIDOR VIRTUAL APAGADO

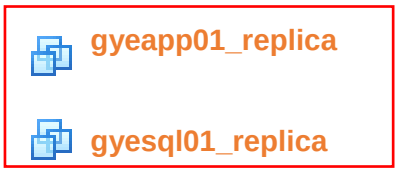
ILUSTRACIÓN No. 38

SERVIDORES VIRTUALES EJECUTANDOSE



FUENTE: INFRAESTRUCTURA SERVIDORES CDC
ELABORADO POR: WILLIAM MOSCOL CRIOLLO

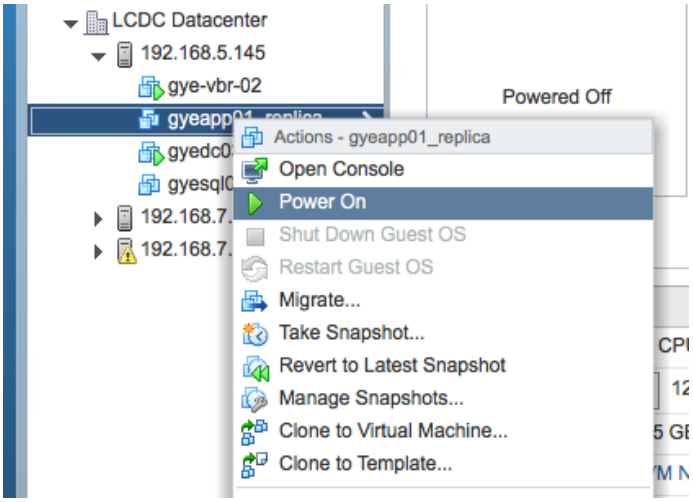
- Identificamos los servidores virtuales apagados, los mismos que son las réplicas que se estaban en producción en matriz.



- Clic derecho sobre el nombre del servidor y elegimos la opción **POWER ON,** ya con esto el servidor pasa a producción y en un intervalo de 10 a 15 min que dura el encendido pueden acceder a la aplicación.

ILUSTRACIÓN No. 39

VENTANA POWER ON



FUENTE: INFRAESTRUCTURA SERVIDORES CDC

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

CRITERIOS DE VALIDACIÓN DE LA PROPUESTA

Presentación De Resultados De La Entrevista

Se elaboraron 8 preguntas abiertas (Ver Anexo 1), dirigidas a las personas responsables del área administrativa, sistemas y gerencia general; las cuáles serán las responsables de validar que la entrega de este proyecto haya cumplido las expectativas.

Se eligieron a los responsables del área mencionada por el motivo que conocen la problemática del plan de contingencia IT ya que los usuarios reportan directamente a dirección administrativa y expresan su malestar por no tener las contingencias adecuadas.

Se describen los nombres de los entrevistados y sus cargos:

Entrevistado 1: Sr. Daniel Faour, Gerente General
Entrevistado 2: Mgs. Celine Faour, Directora Administrativa
Entrevistado 3: Ing. Oscar Suárez, Asesor de Sistemas, Ondú S.A.

CUADRO No. 13

CUESTIONARIO DE PREGUNTAS REALIZADAS DURANTE LA ENTREVISTA A GERENCIA

Pregunta / Entrevistado	Entrevistado 1	Entrevistado 2	Entrevistado 3
1. ¿Conoce Ud. acerca de los planes de contingencia IT?:	Si, si conozco, a nivel mundial son normas estrictas que deben cumplirse en la seguridad de la	Si, si conozco.	Claro, en la actualidad bajo normas internacionales las empresas deben

	información de la compañía,		tener un plan DRP.
2. ¿Cree Ud. Necesario la implementación de un plan de contingencia IT en la empresa Casa del Cable S.A.?	Si lo veo necesario porque pueden pasar eventualidades en la plataforma IT	La empresa desea obtener una certificación ISO 9000 la cual exige contar con un plan IT de contingencia.	Por normas IT y por la continuidad del negocio es necesario
3. ¿Qué factores no han permitido el desarrollo de un plan de contingencia IT para su empresa?	Recientemente se adquirió el hardware, el factor actual sería tiempo	Es cuestión de organizarnos y empezar a trabajar en el plan IT	Todo es un proceso y debe ejecutarse todo a su debido tiempo
4. ¿Cuáles son sus expectativas de un plan de contingencia IT?	Tener una continuidad del negocio y reducir errores	Contar con el personal debidamente capacitado para solventar la emergencia de sistemas	Que el impacto se reduzca en lo mínimo posible y de esta manera garantizar la continuidad del negocio de nuestro cliente.
5. ¿Cuál piensa Ud. que son los procesos críticos informáticos, en caso de alguna incidencia?	Todo proceso es crítico en mi empresa, desde la labor que realiza bodega hasta la labor que realiza administración	Considero procesos críticos el área de facturación, cobranzas, importaciones, me urge una contingencia de esos procesos en el sistema SIAC	Casa del cable cuenta con un software donde todos sus procesos son críticos, es decir la replicación de la base de datos es lo ideal.

6. ¿En dónde desearía ubicar los equipos de contingencia IT?	En la época del año 2008 almacené la data donde un proveedor que no me resultó y no cumplió mis objetivos, por tal motivo sugiero en otra localidad de la empresa.	Se tiene planificado realizarlo en la sucursal de GYE ubicado en Baquerizo Moreno y 9 de Oct.	Por el tráfico de datos se recomienda en un sitio alterno a matriz ubicado en la misma ciudad de Guayaquil
7. ¿Cuál es el tiempo de respuesta que Ud. Espera ante un plan de contingencia IT?	5 minutos	15 minutos	15 minutos
8. ¿Conoce acerca de los costos de implementación de un plan de contingencia IT?	Sí, quiero el que me mejor se adapte a la necesidad de la empresa	No, no conozco	Si, si conozco, se debe evaluar dependiendo la necesidad del cliente.

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

CAPÍTULO IV

CRITERIOS DE ACEPTACIÓN DEL PRODUCTO O SERVICIO

El proyecto en sí se lo considera factible porque en CASA DEL CABLE S.A. ha tenido pérdidas de información por no contar con un plan de contingencia IT, así permite un ahorro en tiempo y costo.

En cuanto a los criterios de aceptación podemos definir:

Análisis de requisitos de hardware de almacenamiento para el sitio alterno de contingencia

> Se considera criterio de aceptación un análisis de los equipos que van hacer adquiridos para el almacenamiento de la réplica de datos, un cuadro comparativo donde se indiquen ventajas y desventajas, precios y requisitos de hardware.

Detalle de los servidores virtuales a replicar entre producción y contingencia

> Consideramos un criterio de aceptación el documento donde conste el detalle de los datos a replicar que en nuestro caso sería el servidor base de datos y el servidor de aplicaciones.

Implementación de la réplica de datos a un sitio alterno utilizando el software VEEAM V8

> Consideramos un criterio de aceptación el informe del plan de contingencia IT donde se indique el detalle de los datos replicados, el hardware y software utilizado.

Elaboración de un plan de contingencia IT o DRP para las aplicaciones SIAC y base de datos SQL.

Consideramos como criterio de aceptación la documentación del DRP donde se especifique:

- Introducción
- Objetivos
- Funcionamiento de la aplicación Veeam V8
- Especificaciones técnicas de hardware
- Monitoreo de la aplicación
- Como proceder ante una contingencia IT

Pruebas del plan de contingencia IT o DRP

En este caso se considera como criterio de aceptación la evaluación mensual, trimestral o semestral del plan de contingencia IT. Documentos o bitácoras previamente firmadas de que el proceso se dio sin novedades.

Medir estadísticas de riesgos y costos

El criterio de aceptación es el informe semestral estadístico de los riesgos a lo que estuvo expuesta la empresa y que gracias al plan de contingencia se logró mitigar, controlar la situación.

MATRIZ CON SUS CRITERIOS DE ACEPTACIÓN

CUADRO No. 14

CRITERIOS DE ACEPTACIÓN

TEMA:	Identificación de amenazas y vulnerabilidades para la elaboración del plan de contingencia IT de la compañía CASA DEL CABLE S.A			
OBJETIVO GENERAL:	Establecer el plan de contingencia IT de la empresa CASA DEL CABLE S.A, identificando las amenazas y vulnerabilidades a las que está expuesto actualmente, procurando su mejoramiento para beneficio de la empresa y de los usuarios.			
OBJETIVO ESPECÍFICO	**OBJETIVO 1**	**OBJETIVO 2**	**OBJETIVO 3**	**OBJETIVO 4**
	Identificar riesgos y debilidades a lo que está expuesta la empresa en el caso de un corte de fluido eléctrico y establecer los pasos a seguir en el manual para la continuidad del negocio.	Definir estrategias para el diseño de un ambiente de réplica de datos de las aplicaciones críticas SIAC y base de datos de la empresa	Presentar las mejoras resultantes de la aplicación basado en los estándares IT NORMA ISO 22301.	Documentar el plan de recuperación de desastres de las aplicaciones SIAC y controlador de dominio.
CRITERIO DE ACEPTACIÓN	Revisar Aplicaciones, revisar base de datos, revisar seguridad IT actualmente instalada	Estudio de varias opciones de réplica de datos en sitios alternos midiendo sus tiempos de respuesta, costo e implementación	Informe Final de que norma se adapta al momento de la instalación del software para la réplica de datos.	Manual de como activar la contingencia en el sitio alterno. Informe del análisis de pruebas del plan de contingencia IT de la empresa.

TAREA	-- Definir requerimientos de la aplicación. -- Levantar información según los formatos definidos. -- Se realizó el estudio de la empresa y sus procesos para identificar las amenazas y sus procesos más sensibles ante emergencias. En base a esto Se procedió a estructurar el plan.	--Se elaboraron pruebas en base a problemas recurrentes y no recurrentes, y la comprobación de los tiempos.	Se realizó el diseño final de la aplicación del plan ante diversas contingencias y se remitió el informe hacia la directiva para su aprobación y ejecución.	Verificación de manual entregado y siguiendo paso a paso el detalle del manual
MÈTODO	--Inductivo. -- Fundamentos ITIL, Gestión de la continuidad del servicio de las aplicaciones críticas. --investigación proyectiva con la finalidad de analizar situaciones o problemas en un ambiente determinado, para finalmente elaborar el modelo que nos guie a la solución del problema.	--Inductivo. -- Fundamentos ITIL-Gestión de la continuidad del servicio. --Entrevista: técnica ideal para la recopilación de datos, con el objetivo de obtener varios puntos de vista técnicos del área de sistemas, así como de los responsables del área de tecnología.	--Inductivo. Fundamentos ITIL, Gestión de la continuidad del servicio --Observación de registros considerada como notable en esta investigación, ya que Casa del Cable S.A. poseen políticas internas. Existe también la necesidad de recopilar y analizar los sistemas existentes de registros.	--Inductivo. Fundamentos ITIL, Gestión de la continuidad del servicio --Observación de registros considerada como notable en esta investigación, ya que Casa del Cable S.A. poseen políticas internas.

TIEMPO	6 semanas	4 semanas	3 semanas	4 semanas
RECURSO	2 personas de sistemas, y equipos de pruebas	2 personas de sistemas, y equipos de pruebas	2 personas de sistemas, y equipos de pruebas	2 personas de sistemas, y equipos de pruebas
CONCLUSIONES	El plan de contingencia IT se desarrolló satisfaciendo a la necesidad de la empresa Casa del Cable S.A.	Se identificaron los riesgos en base a la metodología ITIL -Gestión de la continuidad del servicio, se tomaron los correctivos necesarios previos al informe final.	El plan de contingencia IT cumple con los aspectos básicos para su implementación en la empresa Casa del Cable S.A.	En la actualidad existen varias herramientas para contingencia IT pero no sirven de nada si no se le da el seguimiento respectivo.
RECOMENDACIONES	Se recomienda la revisión del Plan de Contingencia IT, y el seguimiento a la puesta en marcha.	Se recomienda aplicar las medidas correctivas para la elaboración del informe final, y realizar las adecuaciones físicas pertinentes.	Se recomienda que la Dirección de la empresa realice revisiones anuales de la aplicación del plan, para su mejora en base al crecimiento del negocio.	Se recomienda que el personal de sistemas realice el monitoreo a diario de la réplica de datos y respaldos

ELABORADO POR: WILLIAM MOSCOL CRIOLLO

CONCLUSIONES

El problema del flujo eléctrico siempre ha sido una gran debilidad en los centros de cómputo por tal motivo es de prioridad alta realizar las gestiones posibles para tener protección a nivel eléctrico, de esta manera conservar los equipos de cómputo y tener una continuidad del negocio.

En la actualidad ya no se ve como una opción el tener un centro de datos alterno, actualmente es una obligación bajo normas o políticas de la empresa de contar con un plan de contingencia IT.
Tener respaldos y réplicas de nuestros datos nos permite ser más reconocidos en el mercado, más competitivos a la hora de cualquier tipo de eventualidad.
Nos ayuda a preservar la imagen y prestigio de la empresa,

Otro de los requerimientos solicitado fue el de reducir al máximo todo posible riesgo informático, una vez ya teniendo todo los procesos documentados podemos mitigar los errores y no volver a repetir el proceso para la solución del problema.

El plan de contingencia utilizado en el proyecto saca a relucir los beneficios que nos sigue otorgando la tecnología de virtualización, permitiendo así un tiempo de respuesta mucho más rápido que el de tener instalado el S.O. principal en el hardware del equipo.
Las soluciones de virtualización al ser prácticamente “portables en su recuperación” es decir deben ir de la mano con una solución de continuidad del negocio.

RECOMENDACIONES

Dentro del desarrollo del proyecto aplicando diversas metodologías se puede realizar las siguientes recomendaciones:

El daño por corte de fluido eléctrico se los considera muy peligroso ya que se puede presentar en cualquier momento y por tal motivo la protección debe realizarse desde la conexión externa hasta llegar al panel eléctrico interno, lo mencionado en el proyecto solo protege los datos por tanto se recomienda instalaciones de tierra, supresores de pico y generadores eléctricos.

Debe existir un monitoreo constante, diario, cotidiano de los respaldos de servidores virtuales y de igual manera su replicación con el sitio alterno.
Realizar pruebas periódicas del plan de contingencia IT, puede ser mensual, trimestral, como el cliente desee manejarlo, de esta manera promover los buenos hábitos de la tecnología.

Se recomienda una tercera opción de respaldo como son las soluciones en la nube.

Mediante una bitácora analizar los requerimientos más solicitados y tener a la mano el “diccionario de soluciones”.
El sistema operativo en la que se ejecutan los servidores son es en una plataforma de tecnología virtualizada (VMware Vsphere) lo que hace adaptable a cualquier software de replicación de datos y respaldos de servidores.

BIBLIOGRAFÍA

8.0, V. (12 de 09 de 2015). *Software Veeam*. Obtenido de Software Veeam: https://www.veeam.com/es/

ABC. (08 de 07 de 2015). *ABC*. Recuperado el 01 de 09 de 2015, de ABC: http://www.abc.es/tecnologia/20150708/abci-hacking-team-hackeado-201507071942.html

Areitio, J. (2008). *Seguridad de la información.* Madrid: Paraninfo.

Constitución de la República del Ecuador. (3 de Febrero de 2008). *Asamblea Nacional Ecuador.* Recuperado el Septiembre de 2015, de Asamblea Nacional: http://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Cruz, P. (09 de 09 de 2012). *interempresas.net*. Recuperado el 11 de 11 de 2015, de interempresa.net: https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

Definicion.de. (1 de 12 de 2008). *Definición.de*. Recuperado el 25 de septiembre de 2015, de Definicion.de: http://definición.de/plan-de-contingencia/

Delgado, X. (1998). *Auditoría Informática.* Costa Rica: EUNED.

Estado, C. G. (1 de Diciembre de 2009). *Normatividad de Control Interno*. Recuperado el 25 de Septiembre de 2015, de Contraloría General del Estado: http://www.contraloria.gob.ec/documentos/normatividad/ACUERDO%20039%20CG%202009%205%20Normas%20de%20Control%20Interno.pdf

Estado, L. O. (11 de 2009 de 2009). *Contraloría General del Estado.* Recuperado el 25 de Septiembre de 2015, de Contraloria General del Estado: http://www.contraloria.gob.ec/documentos/normatividad/LEYORGACGEyREFORMAS2009.pdf

Frias, A. (23 de Mayo de 2015). *Diario Sur*. Recuperado el 2015, de www.diariosur.es: http://www.diariosur.es/turismo/201505/23/fallo-informatico-afecta-facturación-20150523141028.html

Maestre, G., Osorio, M., Trillos, A., & Palencia, E. (2012). *Metodología para la formulación del plan de contingencia de TI para Instituciones de Educación Superior*. Bucaramanga: Universidad Cooperativa de Colombia, Sede Bucaramanga.

Microsoft Corporation. (9 de 03 de 2014). Obtenido de https://technet.microsoft.com/es-es/library/bb418854.aspx

Morales, M. B. (27 de 11 de 2013). *marfibamo.blogspot.com*. Obtenido de http://marfibamo.blogspot.com/2013/11/la-investigacion-proyectiva.html

Ontiveros, G. (21 de 04 de 2014). *Prezi.com.* Obtenido de https://prezi.com/2t1uui1ozyau/investigacion-exploratoria/

OSIATIS S.A. (13 de 09 de 2015). *Gestion de los servicios TI*. Recuperado el 11 de 11 de 2015, de ITIL V3:

http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti.php
ownerdba. (12 de 6 de 2012). *Wordpress*. Obtenido de https://dbasqlserver.wordpress.com: https://dbasqlserver.wordpress.com/2012/06/04/diferencias-entre-snapshot-logshipping-mirroring-replication-y-failover-clustering/
Peña, A. Q. (01 de 12 de 2006). *Ubiobio.* Obtenido de http://www.ubiobio.cl/miweb/webfile/media/267/3634305-Metodologia-de-Investigacion-Cualitativa-A-Quintana.pdf
Piattini, M. &. (2001). *Google Academics.* Recuperado el 2015, de Google Academics: https://scholar.google.es/scholar?q=MARIO+G.+PIATTINI+SOF-009&btnG=&hl=es&as_sdt=0%2C5
Retrospect. (01 de 2015 de 2015). *Retrospect.* Recuperado el 13 de 09 de 2015, de Retrospect: http://download.retrospect.com/partners/sales_tools/data_sheets/retrospect_10_12/Retro_10_Win_Data_Sheet_ES.pdf
Sampieri, R. H. (1997). *Psicologia Experimental.* Mexico: MCGRAW-HILL . Obtenido de https://psicologiaexperimental.files.wordpress.com/2010/03/metodologia-de-la-investigacion.pdf
Spafford. (2000). *Manual de Seguridad en Redes.* Argentina: Arcert.
Telconet S.A. (1 de 02 de 2015). *Telconet.ec*. Obtenido de Servicios Telconet: http://www.telconet.net/servicios/datacenter
Urriola, A. (12 de 05 de 2010). *Monografias*.
VMware. (10 de 01 de 2015). *VMware.com*. Obtenido de VMware.com: http://www.vmware.com/virtualization/what-is-virtualization.html

ANEXO. 1

LA ENTREVISTA: "IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES PARA LA ELABORACIÓN DEL PLAN DE CONTINGENCIA IT DE LA COMPAÑÍA LA CASA DEL CABLE S.A."

Cuestionario de preguntas realizadas durante la entrevista a gerencia:

1. ¿Conoce Ud. acerca de los planes de contingencia IT?:
2. ¿Cree Ud. Necesario la implementación de un plan de contingencia IT en la empresa Casa del Cable S.A.?
3. ¿Qué factores no han permitido el desarrollo de un plan de contingencia IT para su empresa?
4. ¿Cuáles son sus expectativas de un plan de contingencia IT?
5. ¿Cuál piensa Ud. que son los procesos críticos informáticos, en caso de alguna incidencia?
6. ¿En dónde desearía ubicar los equipos de contingencia IT?
7. ¿Cuál es el tiempo de respuesta que Ud. Espera ante un plan de contingencia IT?
8. ¿Conoce acerca de los costos de implementación de un plan de contingencia IT?