ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE UN PLAN DE CONTINGENCIA PARA LOS SERVICIOS INFORMÁTICOS BRINDADOS POR GTSI-ESPOL"

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

KEVIN KERTS PAZ OBANDO

CHRISTOPHER AUGUSTO SALINAS ROBAYO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Agradezco a Dios por ser quien me dio la sabiduría y fuerza para poder culminar esta etapa. A mis padres Anita del Rocío Robayo Astudillo y Augusto Constantino Salinas Zambrano, por haberme proporcionado la mejor educación, por enseñarme que con esfuerzo y constancia se pueden alcanzar las metas que uno se propone en la vida.

Christopher Augusto Salinas Robayo

Quiero agradecer a Dios por brindarme las virtudes que me han permitido llegar hasta donde estoy. A mis padres Diana del Pilar Obando Altamirano y Gonzalo Oswaldo Paz Llerena, por apoyarme durante toda mi vida y por enseñarme los valores sin los cuales no sería la persona que soy. A todos los maestros por compartir sus destrezas y estimularnos a ser mejores en cada oportunidad.

Kevin Kerts Paz Obando

DEDICATORIA

Dedico este trabajo a mis padres, Diana del Pilar Obando Altamirano y Gonzalo Oswaldo Paz Llerena, por haberme apoyado en todo momento de mi vida y por haberme guiado por el camino correcto. De igual manera dedico este trabajo a mi novia Dayane Paola Valero Martínez, por motivarme a seguir siendo un excelente estudiante y una gran persona.

Kevin Kerts Paz Obando

Este trabajo va dirigido a la persona que ha sido mi mano derecha en mi camino de vida y profesional, mi mamá Anita del Rocío Robayo Astudillo quien me ha sabido guiar en este largo proceso. Gran parte de este excelente trabajo se lo debo a ella ya que me ha sabido aconsejar para seguir siempre hacia adelante ante toda adversidad.

Christopher Augusto Salinas Robayo

TRIBUNAL DE EVALUACIÓN

_____	_____
MSc. Robert Andrade T.	**MSc. Jorge Magallanes B.**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

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

_____

Kevin Kerts Paz Obando

_____

Christopher Augusto Salinas Robayo

RESUMEN

En el presente proyecto, se muestra el diseño de un Plan de contingencia para mantener la operatividad de los servicios como el SidWeb, Académico, Correo Electrónico y Sistema de Consejerías, los mismos que son gestionados por GTSI - ESPOL para beneficio de toda la comunidad politécnica. Una de las principales razones por la que se lleva a cabo un Plan de Contingencias, es para establecer las medidas que deben ser tomadas antes y después de materializada una amenaza, teniendo como prioridad la continuidad de las actividades en el menor tiempo posible.

En este diseño de plan se detallan los pasos que deben realizarse en caso de ocurrir algún desastre que afecte a la información, explica las fases, equipos de trabajo y fases necesarias para su correcta implementación y mantenimiento a seguir.

El diseño de plan de contingencia propuesto ofrece un servicio de respaldo de información usando tecnologías en la nube (Cloud Computing) para mantener la información segura, pudiendo restaurarla a su estado actual.

ÍNDICE GENERAL

CAPÍTULO 1

1. ASPECTOS GENERALES

1.1 Antecedentes

La ESPOL, por medio de la Gerencia de Tecnologías y Sistemas de Información (GTSI), brinda a los miembros de la comunidad politécnica aplicaciones y servicios, los cuales son fundamentales para cada miembro de la comunidad. Según la gerencia, los servicios críticos brindados por ESPOL son los siguientes:

-Sistema Académico

-Correo Electrónico

-Sidweb

-Sistema de Consejerías Académicas

Estas aplicaciones están involucradas en las actividades críticas y diarias de los usuarios de la ESPOL por lo que son de suma importancia. Por ejemplo, los estudiantes son registrados en sus materias y cursos a través del Sistema Académico, el cual a su vez permite la consulta de sus horarios de materias y exámenes. Mediante el Correo Electrónico se permite la comunicación entre los miembros de la comunidad politécnica además de publicaciones de las actividades que se realizan dentro de la institución. Sidweb permite tanto a los estudiantes y profesores publicar sus tareas y subirlas a la Web para sus revisiones, tomas de exámenes online, y también les permite a los profesores llevar un control del desempeño académico de los estudiantes. El Sistema de Consejerías Académicas de manera semestral permite una evaluación de los estudiantes con su Profesor consejero elegido. Este tipo de aplicaciones Web para son las más importantes para GTSI-ESPOL porque manejan gran cantidad de información de los estudiantes, materias y profesores.

Otros servicios y aplicaciones que no tienen tanta demanda son:

-Los servicios de Postgrados

-Servicio de Archivos

-Servicio Mirror

En su mayoría, las aplicaciones utilizadas por la comunidad politécnica, han sido desarrollados por personal que labora en la Institución y se mantienen operativas en el Data Center ubicado en GTSI.

Actualmente, estos servicios se encuentran operativos sobre una Infraestructura Virtual ya que permite aumentar la escalabilidad, flexibilidad y agilidad de los servicios de IT, al mismo tiempo que representan ahorros significativos. De igual manera, la disponibilidad y el rendimiento de estos servicios aumenta, permitiendo así automatizar operaciones, haciendo que la administración IT sea más simple.

El Centro de Procesamiento de Datos de la ESPOL actualmente cuenta con Servidores Blade los cuales son especialmente ventajosos para instalaciones de entornos de virtualización en clúster y para alojamiento web, distribuyendo sus recursos según los requerimientos de cada servicio que se esté ejecutando.

Sus servidores virtualizados se encuentran distribuidos de la siguiente manera:

Para mantener estable el Servicio del Sistema Académico cuentan con 9 servidores con sistema operativo Windows Server virtualizados, los cuales se encargan de realizar el balanceo de carga principalmente de solicitudes realizadas a la página web del Sistema Académico, las cuales varían siendo su pico más alto 1500 solicitudes en promedio por día.

El Servicio del Sidweb para poder manejar el número promedio de solicitudes diarias, que son alrededor de 200, cuenta con 8 servidores, los cuales 7 de ellos con sistema operativo Windows Server y uno con Sistema Operativo Linux virtualizados, estos se encargar de mantener la disponibilidad de sus servicios en la Página Web.

El servicio de Correos se encuentra distribuido por 5 servidores virtualizados con sistema operativo Windows Server para manejar 6500 solicitudes en promedio por día, actualmente trabaja con Office 365 mediante ADFS, manteniendo el dominio de ESPOL para inicio de sesión al servicio, en el cual solo se encargan de administrar las cuentas de los usuarios.

El Sistema de Consejerías Académicas se encuentra alojado en 2 servidores virtualizados, uno con Sistema Operativo Linux y otro es el encargado del almacenamiento de la Base de Datos en Oracle.

Estos Servidores Blade, se encuentran en un Blade Enclosure que posee las siguientes características:

-32 GHz Procesamiento

-192 GBs de memoria RAM

-7 TBs de almacenamiento

A su vez los servidores virtualizados cuentan con las siguientes características:

-1 GB de memoria RAM

-70 GBs de almacenamiento

Promedio de Solicitudes Diarias	Servicio
150 - 200	Sidweb
6500	Correo Electrónico
1000 - 1500	Sistema Académico

Tabla 1. Promedio de Solicitudes Diarias por Servicio [1]

La Tabla 1 muestra el promedio de solicitudes diarias que reciben los servicios informáticos, ya sean consultas a páginas web como es el caso de Sidweb o el Sistema Académico, o el uso del correo electrónico.

Los servidores se encuentran virtualizados en VMware ESXi, el cual es un software compuesto de un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software hypervisor, los

servicios de red, los servidores que permiten la interacción con el software de gestión, administración y las máquinas virtuales.

El ancho de banda para la transmisión de los datos es de 700 Mbps, y el ISP (Internet Services Provider) contratado con Telconet S.A, el Proveedor del Servicio de Internet, ofreciéndoles un enlace dedicado y también un enlace de "Back-up" para redundancia en caso de caída del enlace principal.

La cantidad de miembros de la comunidad Politécnica que cuentan con acceso a los Servicios Informáticos de ESPOL es de 16500 usuarios aproximadamente, los cuales se distribuyen según su rol en el sistema, permitiendo las respectivas consultas y cambios según el tipo de usuario. Como referencia proporcionada por Gerencia de Tecnologías y Sistemas de Información tenemos que actualmente está distribuida de la siguiente manera, siendo aproximadamente 2000 un grupo entre usuarios Profesores y personal Administrativo, 10000 usuarios estudiantes activos y 4500 graduados.

Cantidad de usuarios	Rol
2000	Profesores / Personal Administrativo
10000	Estudiantes
4500	Graduados
16500	**Total de usuarios que acceden a los servicios informáticos**

Tabla 2. Cantidad Aproximada de Usuarios ESPOL [2]

En la tabla 2 se muestra la cantidad aproximada de usuarios de ESPOL que acceden a los servicios que proporciona GTSI, entre los cuales están profesores, personal administrativo, estudiantes y graduados.

1.2 Justificación

Para cubrir con la demanda actual de solicitudes hacia los Servicios Informáticos brindados por GTSI y para agilizar sus procesos, cuentan con un CPD (Centro de Proceso de Datos), por lo que se tiene como prioridad la disponibilidad de la

información, la misma que es vital para las actividades diarias de todos los miembros de la comunidad politécnica. Al no contar con un Plan de contingencia o de respaldo toda su información se vería en grave riesgo.

Un Plan de Contingencia o también llamado Plan de Recuperación de Desastre (DR), es creado para que la gestión en los CPD sea mucho más simple, brindando tranquilidad a los administradores IT ya que la información podrá estar disponible la mayor cantidad de tiempo posible, ya sea en otro CPD o en un CPD en la nube.

La administración de los recursos e información a través de la nube, es solo parte de las grandes posibilidades que nos ofrecen los servicios en la nube, permitiendo al CPD de GTSI un desarrollo continuo y adaptabilidad a futuros cambios.

1.3 Descripción del Proyecto

1.3.1 Problemática

Un problema que puede afectar gravemente al Centro de Procesamiento de Datos, puede ser un desastre natural el cual afecte físicamente la infraestructura de sistemas y de red, provocando la pérdida total de la información, base de datos, servicios, equipos informáticos, etc. dejando al CPD completamente fuera de servicio.

Actualmente GTSI solo cuenta con un Plan de Respaldo de información, mediante el uso de Cintas Magnéticas de Respaldo, conocidas también como “Back-up tapes”, con capacidad de almacenamiento de 400 GBs. Las cuales, si bien funcionan, no son el método más eficiente y mucho menos la mejor opción para el correcto diseño de un Plan de Contingencia.

Al llegar a su máxima capacidad de almacenamiento se requiere invertir en recursos para la obtención de otra Cinta Magnética generando gastos. A su vez, para recuperar la información en caso de algún problema, el proceso de recuperación utilizando cintas de respaldo es lento, ya que se debe leer toda la información almacenada hasta llegar al punto de restauración, lo cual no lo convierte en la mejor opción en caso de querer recuperar información rápidamente, afectando el tiempo de operatividad y la continuidad de los servicios. Adicionalmente, su tiempo de vida útil es mucho menor al de otras alternativas de solución actuales.

Dada esta información podemos observar que la solución actual de su plan de respaldo funciona, pero no garantiza que el tiempo fuera de servicio sea el menor posible, tampoco garantiza que los datos respaldados sean los más actuales. La cantidad de datos transmitidos y almacenados crece exponencialmente con el pasar del tiempo trayendo a su vez futuros problemas de almacenamiento.

1.3.2 Objetivo General

Realizar el diseño de un plan de contingencia basados en el alojamiento del Centro de Datos en la nube para garantizar la disponibilidad de los servicios informáticos *(SidWeb, Académico, Correo, Consejerías)* que brinda la ESPOL a través de la GTSI.

1.3.3 Objetivos Específicos

1. Determinar las contramedidas necesarias para mitigar posibles daños futuros basándose en el análisis de las amenazas que pudiesen provocarlos.
2. Diseñar un Plan de contingencias para el Centro de Datos de GTSI-ESPOL, el cual contempla las contramedidas necesarias para salvaguardar la continuidad de los Servicios Informáticos críticos brindados por la institución.
3. Cumplir con los requerimientos especificados por el Consejo de Educación Superior en cuanto al tiempo de operatividad, siendo este mayor al 98.5%.

1.4 Alcances y Limitaciones

1.4.1 Alcance

Este diseño de solución se enfoca en la presentación de las ventajas y beneficios que nos ofrece un Plan de Contingencias utilizando Computación en la Nube para los Servicios Informáticos críticos de GTSI-ESPOL (Sidweb, Sistema Académico, Correo Electrónico, Sistema de Consejerías) en el caso de la materialización de amenazas que afecten la continuidad de los Servicios Informáticos. El diseño explica las fases, equipos de trabajo y fases necesarias para su correcta implementación y mantenimiento.

1.4.2 Limitaciones

La falta de recursos, así como de personal necesarios para llevar a cabo la implementación y mantenimiento de un Plan de Contingencia es una de las mayores limitaciones para este diseño, puesto que es necesario establecer

grupos específicos de miembros de GTSI, los cuales se encargarán de las diferentes secciones del plan y de sus respectivas fases.

1.5 Metodología

1. Categorizar las amenazas y definir las decisiones a tomar, a partir de la materialización de una amenaza midiendo su nivel de probabilidad de ocurrencia y la magnitud del Riesgo, para determinar las contramedidas necesarias para mitigar los posibles daños en el CDP.
2. Dividir por fases los procesos del plan de contingencia que serán ejecutados antes y durante la ocurrencia de alguna catástrofe que afecte la operatividad del CDP.
3. Realizar tablas comparativas mostrando las ventajas y beneficios de contar con un Plan de Contingencia.
4. Considerar alternativas de Cloud Computing con características de alta disponibilidad para mantener el Up-time de los servicios informáticos por sobre el 98.5%.
5. Realizar un análisis de las alternativas que mejor se adaptan a un Plan de Contingencia para brindar altos niveles de disponibilidad, y posteriormente elegir la mejor, tomando en cuenta los siguientes aspectos:
   - Aspecto Técnico
   - Aspecto Económico

CAPÍTULO 2

2. MARCO CONCEPTUAL

Dentro de este marco conceptual se pretende dar una definición de los principales términos e ideas que serán usados en el desarrollo de este proyecto.

2.1 Centro de Procesamiento de Datos

Se denomina Centro de Procesamiento de Datos (CPD) a aquella ubicación donde se encuentran los recursos necesarios (físicos, lógicos y humanos) para procesar la información de una organización, realización y control de las operaciones informáticas.

En el Centro de Procesamiento de Datos se debe llevar una planificación, revisión, implantación y adecuación de los servicios los cuales este provee. Se debe tomar en cuenta las siguientes consideraciones [1]:

Un Centro de Procesamiento de Datos requiere de grandes capacidades de procesamiento y almacenamiento que garanticen el rendimiento de todas las aplicaciones y servicios los cuales van a ser administrados. Los principales equipamientos inherentes a los CDP's tenemos:

1. Sistemas de Refrigeración (Aires Acondicionados de Precisión).
2. Sistemas de Monitoreo Ambiental (Humedad, Temperatura).
3. Soluciones de Cableados Estructurado.
4. UPS (Protección Y Energía de Respaldo).
5. Control de Accesos.
6. Sistema Eléctrico Normal y Regulado.
7. Rack y Accesorios.
8. Gestión y Monitoreo (Softwares de Gestión).
9. Sistemas de Seguridad (Puertas y chapas electromagnéticas).
10. Sistemas de Vigilancia (Cámaras y sensores de movimientos).
11. Sistemas Anti Incendios.

2.2 Normas para la implementación de un CDP:

- TIA 492 según EIA/TIA
- TIER según el instituto Up-time
- UL1449, UL1778, IEC6204-3
- NFPA 255, IEC6204-3, TIA 942 y NEC

Los Centros de Procesamiento de Datos en inglés son conocidos con el término de Data Center, un término habitual hoy para muchos. Estos pueden ser creados y administrados por grandes compañías con el objetivo de tener acceso a la información necesaria para sus procesos y operaciones. Entre los principales en contar con un centro de procesamiento de datos son los bancos ya que ellos deben contar con gran cantidad de información útil sobre sus clientes y sus transferencias que se realizan sobre sus cuentas. En la actualidad toda compañía pequeña mediana o grande suelen contar con un centro de procesamiento de datos, hasta las grandes corporaciones multinacionales suelen contar con múltiples CDP ubicados en diferentes partes del mundo [2].

El proceso que se realiza en un CDP como su nombre indica engloba múltiples procesos y sistemas asociados en los cuales los datos son almacenados, distribuidos y tratados a los administradores para realizar consultas o modificarlos. Estos datos albergan en servidores los cuales son los encargados de mantener un entorno de funcionamiento eficiente y óptimo [2].

2.3 Cloud Computing

Cloud Computing es un tipo de computación basada en Internet, que provee procesamiento compartido de recursos y datos a computadoras y otros dispositivos bajo demanda. El cual se basa en compartir recursos informáticos en lugar de contar con servidores locales o dispositivos personales para poder manejar los recursos informáticos y aplicaciones [3].

2.3.1 Objetivo del Cloud Computing

El objetivo de la computación en la nube es la aplicación de la supercomputación tradicional, o el poder de computación de alto rendimiento, normalmente utilizado por las instalaciones militares e

investigadores, para poder llevar a cabo decenas de miles de millones de cálculos por segundo, ya sea estas en aplicaciones orientadas al consumidor, como financieras, ofrecer información personalizada, permitiendo proporcionar grandes almacenamiento de los datos de inmersión en línea de computadoras. Esta infraestructura de TI compartida cuenta con grandes grupos de sistemas que se encuentran unidos entre sí. Para optimizar esta solución a menudo las técnicas de virtualización se utilizan para maximizar el poder de la computación en la nube [3].

2.3.2 Características que definen el Cloud Computing

- Estandarización de las tecnologías utilizadas para garantizar la eficiencia del servicio.
- Acceso al Servicio ya que el coste de adquisición del servicio es más bajo lo que facilita que no haya tantas barreras de entrada.
- Pago por uso.
- Independiente del dispositivo y del punto de acceso.
- Escalabilidad, permitiendo el crecimiento de la organización adaptándose a las grandes cantidades de información que tiene que gestionar.
- Autoservicio. Los clientes pueden solicitar los recursos que necesitan y estos se aprovisionan en el menor tiempo posible permitiendo un servicio eficiente y rápido sin dejar la operatividad de las organizaciones.
- Mantenimiento más eficiente, ya que este ser realiza por los proveedores o está centralizado y gestionado por profesionales TI.
- Métricas. Los recursos son medibles y serán contabilizados por el uso de cada organización como cliente.

2.3.3 Estándares de Cloud Computing

Las normas para conectar los sistemas informáticos y el software necesario para realizar el trabajo de computación en la nube no se encuentran completamente definidos actualmente, las cuales dejan a muchas empresas a definir sus propias tecnologías de computación en la nube, como observamos en la Figura 2.1 la imagen haciendo referencia a los servicios que ofrece GTSI alojados en la nube.

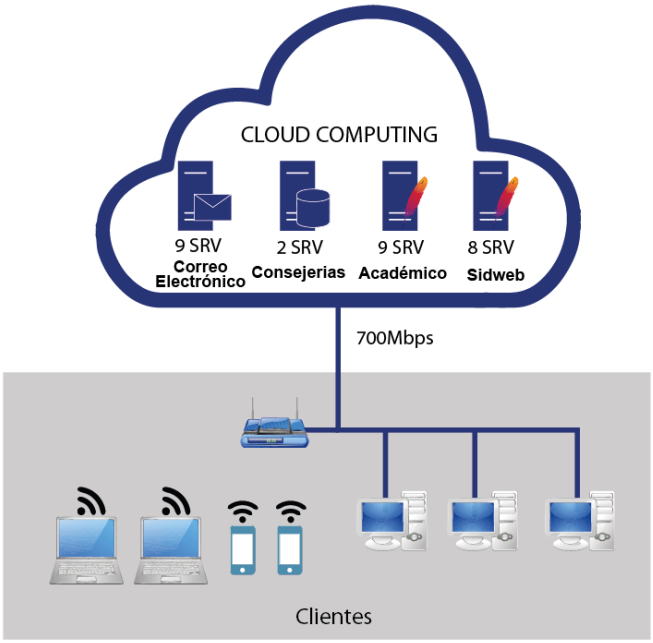


Figura 2.1 Infraestructura de la computación en la nube [1].

2.3.4 Gestión de Cloud Computing

Las estrategias de gestión de la nube suelen incluir múltiples tareas, la seguridad, el cumplimiento de auditoría, supervisión del rendimiento (la latencia, tiempo de respuesta, tiempo de funcionamiento, etc.) y gestión e iniciar y supervisar los planes de recuperación de desastres y de contingencia.

Con la computación en la nube cada vez crece siendo más compleja su gestión y con una amplia variedad de modelos pudiendo ser privada, híbrida, y públicas basados en sistemas en la nube y la infraestructura que

ya está en uso. La colección de herramientas de gestión de la nube de la empresa tiene que ser tan escalable y flexible como su estrategia de computación en la nube [3].

2.3.1 Modelos de Implementación:

El instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos definió cuatro modelos de implementación de la nube:

- Privado
- Publico
- Comunitario
- Hibrido

- **Private Cloud**

La plataforma se encuentra dentro de las instalaciones del usuario sin ofrecer servicio a terceros. Las nubes privadas están en una infraestructura local manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor, red, discos y pueden decidir qué usuarios están autorizados a utilizar la infraestructura. Esta nube, que se encuentra detrás de un firewall y se centra en la seguridad de la nube, el cumplimiento y gestión, no está abierta para el consumo público, ya que se encuentra dentro de un entorno muy controlado [4].

- **Public Cloud**

Los servicios que ofrecen se encuentran en servidores externos al usuario, pudiendo tener acceso a las aplicaciones. Creada para el uso del público en general dentro o fuera de una institución. Toda su infraestructura se encuentra alojada físicamente en el sitio del proveedor, pero a su vez esta puede ser propiedad de una o varias organizaciones como instituciones académicas, industrias entidades gubernamentales o empresas. Se manejan por terceras partes, y los trabajos de muchos clientes diferentes pueden estar mezclados en los servidores, los sistemas de almacenamiento y otras infraestructuras de la nube [4].

- **Community Cloud**

Estas nubes comunitarias son creadas para el uso exclusivo de una comunidad determinada. Una comunidad puede constar de varias organizaciones los cuales comparten los mismos requisitos de seguridad, servicios, misión, factores de cumplimiento.

La infraestructura puede estar ubicada fuera del sitio o dentro de este, y puede ser propiedad de una o más organización que forman parte de una comunidad o simplemente pertenecer a un proveedor.

Existe diferencia entre las nubes públicas y las nubes comunitarias que son las necesidades funcionales, estas pueden ser personalizables dentro de una nube comunitaria y se personalizan para las organizaciones de la comunidad [4].

- **Hybrid Cloud**

Combina los modelos de infraestructuras de nubes públicas, comunitarias y privadas que son entidades únicas. Esto permite a una empresa mantener el control total de sus principales aplicaciones, al tiempo de aprovechar el Cloud Computing en los lugares donde tenga sentido. Estas entidades se unen por la tecnología que permite habilitar la portabilidad de las aplicaciones y los datos.

Una nube híbrida ofrece flexibilidad de adaptación a los servicios que ofrecen los proveedores y reaccionar ante ellos, a petición [4].

2.3.6 Modelos de Servicio de Cloud Computing:

Existen cuatro modelos de servicio de Cloud Computing, cada uno representa una estrategia distinta a la hora de gestionar las TIC.

- **Infrastructure as a Service(IaaS)**

Se provee a las compañías clientes con recursos computacionales, tales como servidores, almacenamiento, red y espacio de data center. Las compañías pagan por el consumo de los recursos [5].

- **Platform as a Service(PaaS)**

Provee un ambiente basado en la nube (Cloud-based Environment) con todo lo necesario para apoyar el ciclo de vida de Aplicaciones basadas en la Nube, sin el costo y la complejidad de comprar y gestionar el Hardware, Software, aprovisionamiento y alojamiento subyacente [5].

- **Software as a Service(SaaS)**

También conocido como ***Cloud-based applications*** se refiere a Software desplegado sobre internet, en este escenario el proveedor licencia aplicaciones para su utilización por varios clientes manteniendo la privacidad de sus datos y la personalización de la aplicación.

SaaS ofrece a la TI mayor oportunidad de ofrecer valor empresarial real a la organización a través de costes de menor valor y más predecibles y ofreciendo una mayor capacidad para centrarse en la innovación y en la diferenciación. Ya que, en lugar de instalar, mantener y actualizar el software y el hardware, el personal de TI simplemente acceder a las aplicaciones con disponibilidad seguridad y rendimiento de clase empresarial a través de la nube [5].

- **TI as a Service (ITaaS)**

Con las metodologías (ITIL, COBIT, etc.) el departamento de IT se ha tratado de verlo como un gasto en vez de una inversión. Para tener un departamento de ITaaS se debe definir los objetivos del departamento en corto, medio y largo plazo de las unidades de la empresa y se definen las acciones que se deben tomar en cuenta por IT para conseguirlos.

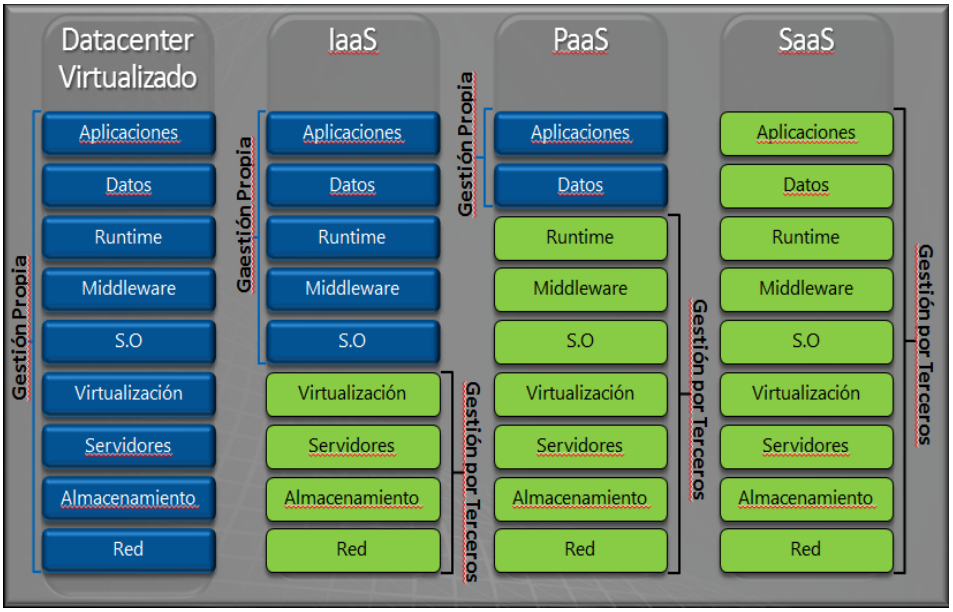


Figura 2.2 Infraestructura por capas según el modelo de servicio [2].

La computación en la nube ha contribuido a que las organizaciones hagan grandes cambios importantes en sus infraestructuras tecnológicas. Este proceso puede ser más generalizado con el pasar del tiempo y a medida que las organizaciones aprovechen los servicios y ventajas que ofrece la computación en la nube, evaluando sus necesidades de datos masivos que deben gestionar en sus centros de datos. Para lograr esto necesitan contar con una infraestructura y los profesionales adecuados de TI que tengan la capacidad de combinar los diferentes modelos de servicios que la nube ofrece y así poder determinar qué modelo sería el mejor para cada servicio, como lo muestra la Figura 2.2 [6].

CAPÍTULO 3

3. PLAN DE CONTINGENCIA

En este capítulo se detalla el Diseño del Plan de Contingencia para los Servicios Informáticos Brindados por GTSI-ESPOL a realizarse. Un Plan de Contingencia es un conjunto de procedimientos alternativos a la operatividad normal de una institución, su finalidad es permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo debido a algún incidente interno o externo. Este incidente puede llegar ser provocado por la inoperatividad por falla mecánica del equipo en los servidores, u otra causa puede ser por catástrofes naturales en cuyo caso todo el Centro de Cómputo quedaría sin dar servicio alguno. El Plan de Contingencias está dividido en fases. Cada fase determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza o riesgo [7].

Personal Autorizado para Declarar Emergencia o Resumir Actividades

La Tabla 3 muestra a los miembros del personal de ESPOL como las personas autorizadas para declarar un Desastre de Sistemas Tecnológicos y la reanudación de las operaciones normales:

Nombre	Cargo
Ms. Sergio Flores	Rector de ESPOL
Ing. Alfonso León Goyburu	Gerente de Tecnología y Sistemas de Información
Ing. Luis Ruiz Vera	Jefe de Infraestructura Tecnológica
Ing. Juan Moreno Velasco	Sub-Gerente de Servicios de Infraestructura Tecnológica y Seguridad Informática

Tabla 3. Personal Autorizado para Declarar Emergencia o Resumir Actividades [3]

3.1 Análisis de Amenazas

En esta sección se describen las posibles amenazas para la continuidad de los Servicios Informáticos brindados por GTSI-ESPOL, realizando un análisis de riesgo basándose en la Figura 3.1 para categorizar las amenazas y definir las decisiones a tomar a partir de la ocurrencia de un evento [8].

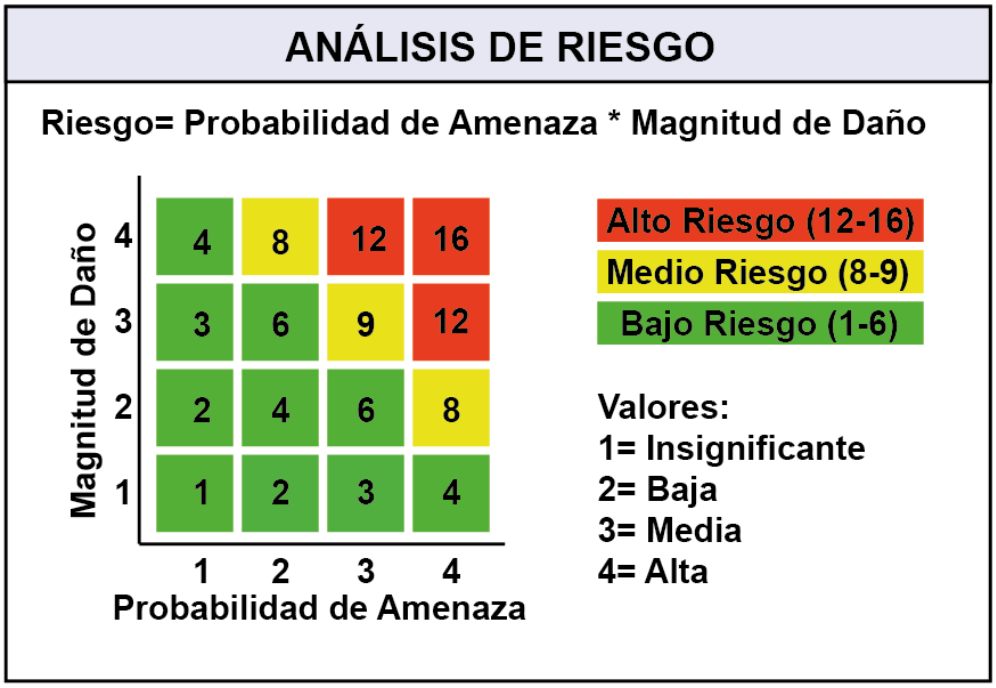


Figura 3.1 Análisis de Riesgo [3]

Amenazas Internas

La Tabla 4 muestra los posibles incidentes que ponen el peligro al personal y/o a los equipos tecnológicos dentro del CPD.

Amenaza	Probabilidad de Ocurrencia	Magnitud de Daño
Incendio	3	4
Pérdida de Energía	2	2

Tabla 4. Amenazas Internas [4]

Incendio- Para el caso particular del CPD de GTSI-ESPOL, un incendio es considerado una amenaza de alta magnitud ya que es muy probable que, de no ser controlado a tiempo, destruya los servidores, así como las actuales cintas de respaldo.

Pérdida de Energía. - La pérdida de energía es considerada una amenaza puesto a que al ser prolongada puede que los sistemas de respaldo dejen de proveer la energía necesaria y se tenga que detener los servicios Informáticos [8].

Amenazas Externas

La Tabla 5 muestra los incidentes que ponen en peligro las instalaciones del CPD:

Amenaza	Probabilidad de Ocurrencia	Magnitud de Daño
Terremoto	3	4
Terrorismo	2	4
Inundación	2	4

Tabla 5. Amenazas Externas [5]

Terremoto. - Puede provocar grandes daños al CPD, incluyendo su destrucción, así como la pérdida de varios o todos sus activos, por lo que es considerada una amenaza de alta magnitud.

Terrorismo. - Como amenaza externa, el terrorismo es considerado como una amenaza de alta magnitud, ya que eventos de este tipo ajenos al CPD pueden destruir las instalaciones junto con sus activos e incluso su personal [8].

Inundación. - Una inundación, aunque es considerada como una amenaza de baja probabilidad de ocurrencia, es considerada como una amenaza de alta magnitud, puesto que puede dañar los activos del CPD [8].

A partir de esta información podemos clasificar las amenazas en medida de su riesgo, como lo muestra la Tabla 6:

Amenazas de Alto Riesgo	Incendio	Terremoto
Amenazas de Mediano Riesgo	Terrorismo	Inundación
Amenazas de Bajo Riesgo	Perdida de Energía	

Tabla 6. Clasificación de Amenazas [6]

3.2 Requerimientos

Mediante un análisis de la Situación Actual planteamos como solución el diseño de un plan de contingencia en el cual se adopte una Infraestructura virtualizada en la Nube *(Cloud Computing)*. Este modelo de Servicio se conoce como IaaS (Infrastructure as a Service).

Con una solución de este tipo podemos escoger que tipo de Sistemas Operativos tendremos, su cantidad y sus características, para el despliegue de los Servidores que proveerán los servicios informáticos, estos servidores serán virtualizados.

De igual manera, el diseño contempla que los respaldos de los servidores se almacenan en la nube, ya que el respaldo en Cloud Computing actualmente ofrece soluciones basadas en duplicación de archivos y compresión, permitiendo hacer el “Back-up” mucho más eficiente y seguro. Y nos brinda una mayor disponibilidad ya que podremos acceder desde cualquier lugar con conexión a internet a la información [9].

Recursos necesarios para llevar a cabo el Plan de Contingencia

Se debe crear un “Equipo de Recuperación” con miembros de GTSI-ESPOL, dicho equipo estará a su vez conformado por un sub-grupo:

Grupo de Emergencia:

Este grupo es responsable de tratar de minimizar daños en el sitio primario (CPD), parte de sus funciones es determinar qué equipos pueden seguir siendo utilizados y cuáles no.

Requerimientos Tecnológicos

Requerimientos Tecnológicos previos a la selección de un Proveedor de Cloud Computing.

- **Servidores**

  Las características de los Servidores a virtualizarse en la Infraestructura en la Nube son los observamos en la Tabla 7:

	Sidweb	Académico	Correo	Consejerías
Cantidad de Serv.	8	9	5	2
Procesamiento	1 Core	1 Core	1 Core	1 Core
RAM	1 GB	1 GB	1 GB	1 GB
Almacenamiento	90 GB	90 GB	90 GB	90 GB

Tabla 7. Características de Servidores Virtualizados [7]

A esto se suma la variedad de Sistemas Operativos, pudiendo ser estos MS Windows Server o alguna distribución de Linux.

- **Ancho de Banda**

  Se busca un proveedor que nos ofrezca la Infraestructura en la nube, además de capacidad para enlace de datos mayor o igual a 700 Mbps, que es lo que el CPD de GTSI requiere para su correcto funcionamiento.

- **Respaldos**

  La finalidad de este requerimiento es tratar de mitigar la magnitud de los daños provocados por la materialización de amenazas antes de que estas ocurran.

- **Inventario**

  Se debe realizar el inventario de los bienes que posee GTSI-ESPOL, tanto Hardware como Software. El Inventario de Hardware debe Incluir equipos de computación con sus características y equipos de red. El inventario de Software, debe incluir, aplicaciones y sus respectivas licencias de uso, manuales. De igual manera, se debe llevar un control de los respaldos creados.

- **Realización de Respaldos**

  Los Respaldos de los servidores para cada uno de los servicios críticos se realizarán de la siguiente manera:

Servicios	Tipo de Respaldo	Frecuencia de Realización
Sistema Académico	Respaldo almacenado en la nube	Todos los días
Sidweb	Respaldo almacenado en la nube	Todos los días
Correo	Respaldo almacenado en la nube	Todos los días
Sistema de Consejerías	Respaldo almacenado en la nube	Todos los días

Tabla 8. Respaldo de Información [8]

La Tabla 8 muestra los Servicios a los que se les realizará el respaldo correspondiente, estos respaldos serán almacenados en la nube de BackupNet y se realizarán todos los días durante la madrugada, para no afectar las operaciones normales de la ESPOL.

- **Centro de Procesamiento de Datos alterno**

  El requerimiento principal para la correcta ejecución de este Plan de Contingencia, es contar con la existencia de un CPD alterno, en el cual se pueda continuar con las operaciones de los Servicios informáticos críticos brindados por GTSI. Dada la importancia de este requerimiento, se recomienda el uso de un Centro de Procesamiento de Datos en la Nube.

3.3 Análisis de Soluciones

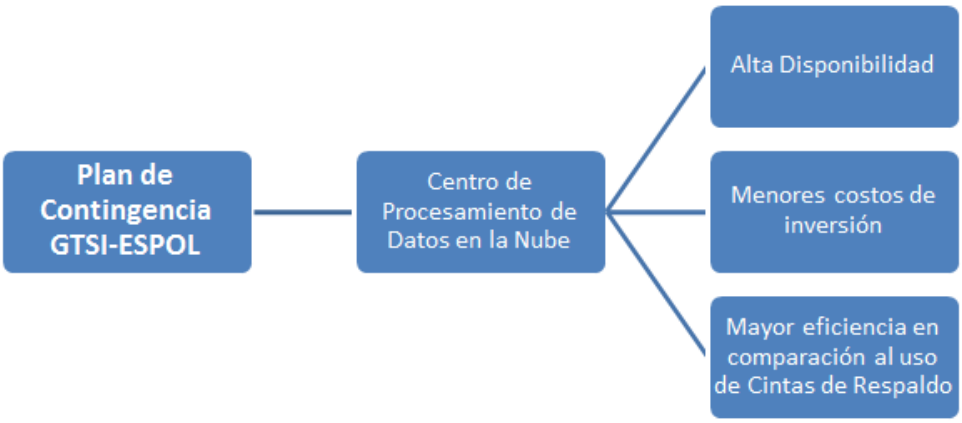


Figura 3.2 Beneficios CDP en la Nube [4]

En la Figura 3.2 se representan los principales beneficios que ofrece el Plan de Contingencia para GTSI-ESPOL basado en un Centro de Procesamiento de Datos alojado en la Nube.

El valor que representa la información y los datos es primordial para la continuidad de GTSI-ESPOL como institución de velar por los servicios informáticos para el personal interno de ESPOL. Ya que, si falla un equipo del Core de operatividad para la ESPOL, puede significar pérdida de gran cantidad de información y de registros, por esta razón es importante respaldar nuestra información y contar con un plan de contingencias para saber qué pasos debe

seguir el personal administrativo y técnico de GTSI-ESPOL para solucionar lo más pronto posible la caída del servicio.

La pérdida de información por unos minutos puede representar grandes daños como los siguientes:

- Desconfianza de los clientes o usuarios.
- Pérdida de Reputación como institución TI.
- Problemas en procesos administrativos.
- Problemas en parte operacional.
- Grandes pérdidas económicas.

Previo a la selección de la Solución de Cloud Computing que se aplicará en el Plan de Contingencia se realiza un análisis de los proveedores del Servicio de Cloud Computing, TELCONET S.A. con su servicio de BackupNet, y también Amazon con su servicio AWS (Amazon Web Services) para Back-up y recuperación de desastres. El análisis y la comparativa se realiza en base a los beneficios que ofrecen cada uno para el diseño de un Plan de Contingencia eficiente que cumpla con los requerimientos para garantizar la continuidad operatividad y salvaguardar la información de GTSI - ESPOL.

Alternativa 1 - Cloud BackupNet

Entre los proveedores que nos ofrecen estas soluciones de Cloud Computing tenemos Telconet S.A con su servicio BackupNet. BackupNet es un servicio de respaldo vía internet en servidores y equipos de almacenamiento pertenecientes a Telconet S.A [10].

El servicio que ofrecen es conocido como respaldo en la nube, o en inglés también llamado como Cloud Back-up y este cumple con los estándares de la nube pública que son:

- Acceso al servicio vía internet
- Las características del servicio son predefinidas, estando basadas en una suscripción en donde sus parámetros que corresponden al tipo de cliente y a la segmentación del cliente.
- Los datos respaldados de los clientes se encuentran en equipos de almacenamiento dedicados al servicio, pero a su vez cuentan con volúmenes dedicados al servicio son compartidos entre todos los usuarios.
- Cada cliente tiene acceso a su información únicamente.
- Es responsabilidad del usuario del servicio la correcta instalación y configuración de la información a respalda, así como su horario.
- Telconet S.A. ha implementado una infraestructura redundante para dar el servicio, sin embargo, no es responsable por la pérdida de la información provocada por el mal funcionamiento de los equipos o por las fallas de programación del software que brinda el servicio.
- El usuario del servicio es responsable de la integridad de la información que respalda, el proveedor del servicio no es responsable por la misma.
- Los servidores que brindan el servicio son dedicados a brindar el mismo, pero a su vez son compartidos entre todos los usuarios que gozan del servicio [11].

Ventajas y Desventajas

Ventajas

- Permite escalabilidad Dinámica
- Facilidad de implementación
- Acceso remoto

Desventajas

- Para acceder a la nube se lo realiza a través de internet, los requisitos de ancho de banda son claramente elevados.
- Esta tecnología de Cloud Back-up que nos ofrece Telconet S.A nos brinda beneficios que muestra la Tabla 9, por los cual deberíamos respaldar nuestra información en la nube:

Características	Descripción
Alta disponibilidad	La información está directamente disponible continuamente. En caso de perder la información local, puede empezar a recuperarse inmediatamente.
Seguro	El cifrado de datos, la conexión a internet segura y el almacenamiento en un CDP sólido y seguro garantizando privacidad máxima.
No requiere inversiones iniciales	Este servicio por tasas fijas mensuales se puede tener almacenamiento seguro sin la necesidad de invertir en hardware o software.
Informes automáticos, monitoreo fácil	Los informes automáticos en el software cliente y correo electrónico aseguran que siempre esté al tanto del estado de sus respaldos.

Tabla 9- Características BackupNet [9]

Los precios del servicio están basados en suscripciones al mismo, los cuales son segmentados en usuarios tipo:

A) Estación de Trabajo

B) Servidor

Los precios del servicio también están basados en las características de los servidores.

Alcance del Servicio

Sistemas Operativos Microsoft Compatibles con el Servicio

- Microsoft Windows XP, Vista, Windows 7, Windows 8 (todas las ediciones 32 y 64 bit)
- Microsoft Windows Server 2003, 2008, 2008R2, SB 2011 (todas las ediciones 32 y 64 bit)
- Prerrequisitos: Microsoft .NET Framework 2.0

BackupNet puede respaldar la información de un Servidor Exchange siempre y cuando el Agente se encuentre instalado en el servidor donde reside la aplicación Exchange y este tenga permisos de salida al internet de 3 formas:

- A) Mediante un plugin ESE mail store back-up (API provista por Microsoft)
- B) Mediante la opción a nivel de carpetas (permite elegir los casilleros a respaldar)
- C) Mediante VSS, realiza un back-up de archivos .edb y .stm del sistema

Microsoft SQL Server 2005/2008/2008 R2

BackupNet puede respaldar la información de un Servidor Microsoft SQL siempre y cuando el Agente se encuentre instalado en el servidor donde reside la aplicación SQL y el mismo no tenga restricción de salida al internet

- Requiere credenciales SQL con permisos de usuario por instancia instalada.
- El usuario debe tener roles de Sysadmin, db_backupoperator y db_owner.
- BackupNet solo realiza back-up de las bases locales
- BackupNet no puede respaldar o restaurar la tempdb

- BackupNet realiza respaldos totales e incrementales, asignados por default [11].

Sistemas Operativos Linux

Sistemas Operativos Soportados

- RedHat Linux
- SUSE
- DEBIAN
- Derivados de Debian como Ubuntu

Prerrequisitos:

- Soporte de JAVA 1.6 o superior (Sun u Oracle Java)
- Ambiente de Consola Gráfica

Prerrequisitos:

- Soporte de Java 1.6 o superior (Sun u Oracle Java)
- Ambiente de Consola Gráfica

Alternativa 2 - AWS Cloud

Las soluciones de almacenamiento de Amazon Web Services (AWS) están diseñadas para entregar almacenamiento seguro, escalable y duradero a los negocios que buscan conseguir eficacia y escalabilidad en sus entornos de back-up y recuperación sin necesidad de que cuenten con una infraestructura on-premise, según muestra la Figura 3.3 con AWS se paga lo que se usa.

Casos de usos de Back-up y de Recuperación de Desastres

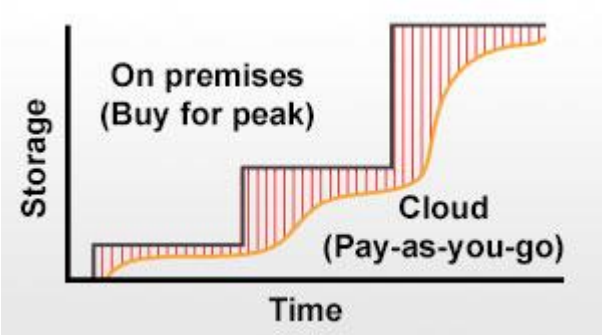


Figura 3.3 Análisis estadístico de costos AWS [5]

Seguridad en los servicios AWS Cloud

Las certificaciones de seguridad de AWS, como SOC1, le permiten proteger los datos como es debido. Las normas como AES 256, que permite cifrar los datos inactivos, garantizan que nadie pueda ver dichos datos. Amazon Virtual Private Cloud le permite crear una subred privada para bases de datos y servidores de aplicaciones, a fin de tener mayor control sobre la seguridad de las cargas de trabajo que resultan críticas.

Velocidades de transferencias que proporciona AWS

AWS soporta varios métodos para cargar y recuperar datos, entre otros: Internet, una conexión de red directa con AWS Direct Connect la cual nos ofrece conexiones entre 1 y 10 Gbps y el servicio AWS Import/Export en el que importaremos los datos en S3. Además, en el caso de los back-ups de datos de aplicaciones, AWS Storage Gateway ayuda a realizar back-up de los datos en AWS.

Gestión de los datos remotamente mediante AWS

Las soluciones de almacenamiento de AWS le permiten elegir en qué región residirán los datos para minimizar la latencia y los costos, así como para satisfacer los requisitos normativos. Tendrá el control total de los datos. Con 11 regiones y diferentes zonas de disponibilidad, una opción que permite distribuir los datos entre las zonas de disponibilidad designadas para mayor protección, dispone de flexibilidad en relación con el lugar en que se almacenan los datos.

Replicación de los datos usando AWS

Amazon S3 y Amazon Glacier replican los datos automáticamente en varios centros de datos y son soluciones diseñadas para ofrecer una durabilidad del 99,999999999%. Las soluciones de almacenamiento de AWS están diseñadas para entregar una sólida protección de datos, para que su compañía nunca tenga que preocuparse por el lugar donde están ubicados los datos. Como muestra la Figura 3.4, la replicación de los datos a través de la red WAN, desde el CDP local al CDP de AWS realizando el respectivo back-up de los datos [12].

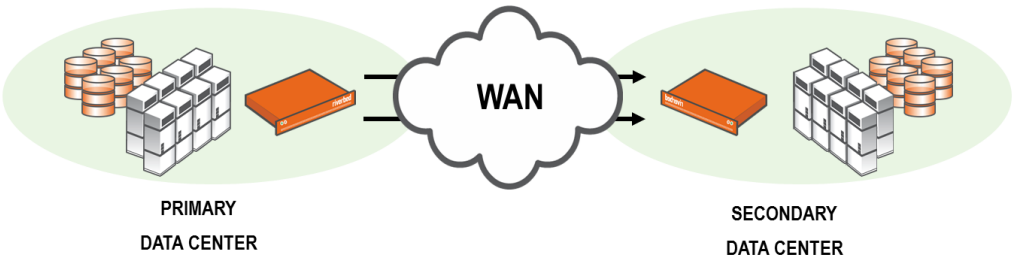


Figura 3.4 Replicación de los datos de un CDP [6]

Zonas de disponibilidad y regiones de AWS

Toda la infraestructura de AWS está compuesta de zonas de disponibilidad y regiones como observamos en la Figura 3.5. Una región es la ubicación física donde se encuentra en el mundo y AWS dispone de varias zonas de disponibilidad. Estas zonas están compuestas de uno o varios centros de datos, cada uno de ellos con alta redundancia, conectividad y redes, alojadas en instalaciones independientes.

En estas zonas se pueden operar múltiples aplicaciones de producción con alta disponibilidad y bases de datos, ofreciendo tolerancia a fallos y mayor capacidad de redundancia ya que son múltiples centros de datos trabajando a la vez [13].

Figura 3.5 Mapa de Infraestructura Global AWS Amazon [7]

Figura 3.6 Centros de Datos de Telconet en Ecuador [8]

Actualmente Amazon cuenta con una infraestructura global de AWS, como lo muestra la Figura 3.5, ya que opera en 35 zonas de disponibilidad en 13 regiones geográficas de todo el mundo, y aún se encuentra expandiéndose a lo largo del año a 9 zonas de disponibilidad y 4 regiones más online. Mientras que Telconet, como lo muestra la Figura 3.6, cuenta con 2 CPD o Cloud Centers en el Ecuador, uno ubicado en Guayaquil y otro ubicado en Quito.

Figura 3.7 Comparativa de beneficios BackupNet vs AWS Amazon S3 [9]

La Figura 3.7 muestra una comparativa entre ambos proveedores, en la que se puede notar que AWS (Amazon Web Services) nos ofrece mayor confiabilidad para la información y los servicios que pueden ser enviados a su Nube.

Análisis de Costos

BackupNet			
Servicio	**Cantidad**	**Subtotal (mensual)**	**Total(mensual)**
Costo enlace 1 Gbps	1	$ 230,00	$ 230,00
Costo por Servidor Linux	2	$ 8,35	$ 16,70
Costo por Servidor Windows	22	$ 11,14	$ 245,08
TOTAL DE COSTOS MENSUALES			**$ 492,00**

Tabla 10. Costos mensuales BackupNet [10]

AWS			
Servicio	**Cantidad**	**Subtotal (mensual)**	**Total(mensual)**
Costo enlace 1 Gbps	1	$ 219,00	$ 219,00
Costo por Servidor Linux	2	$ 9,49	$ 18,98
Costo por Servidor Windows	22	$ 13,14	$ 289,08
TOTAL DE COSTOS MENSUALES			**$ 527,00**

Tabla 11. Costos mensuales AWS [11]

Las Tablas 10 y 11 muestran los costos mensuales entre ambos proveedores de los servicios que se requiere para la implementación del Plan de Contingencia. La información referente a los servicios brindados por AWS fue obtenida a través de su calculadora de precios online [14].

3.4 Selección de la alternativa

Analizando esta información nos damos cuenta de que AWS, a pesar de tener muchas zonas de Disponibilidad estas no se encuentran cerca del territorio nacional, a excepción de la zona de Sao Paulo, lo que implica un mayor costo en los enlaces que se necesiten para realizar las replicaciones. Por otro lado, Telconet posee solo dos CPD, ambos en territorio nacional, además, ESPOL ya cuenta con enlaces de datos con este proveedor, por lo que podrían usarse para la replicación de Servidores, fuera de horarios de oficina. Con respecto a los costos, Telconet nos ofrece un valor menor (6.64%) en comparación con AWS.

Debido a esto BackupNet ha sido seleccionada como la Solución de Cloud Computing sumando varios beneficios para la implementación del Plan de Contingencia.

Otro beneficio particular es:

- La proximidad del CPD de Telconet, hace posible que el personal designado por GTSI-ESPOL pueda visitar el CPD de Telconet durante la implementación, para llevar el control de la misma.

3.5 Activación del Plan de Contingencia

Este Plan será activado en respuesta a amenazas tanto internas como externas, que puedan comprometer la integridad de los Sistemas Tecnológicos del Centro de Datos ubicado en GTSI-ESPOL. Su finalidad es mitigar la magnitud de los daños debido a la materialización de amenazas.

Fase de Evaluación de Desastre

La evaluación del desastre se realiza desde el inicio de la catástrofe y continúa hasta que la catástrofe esté bajo control y la magnitud de los daños pueda ser evaluada.

Actividades Principales:

- Notificar el evento
- Verificar el aviso
- Determinar el tipo de nivel de emergencia

Fase de Continuación de Operaciones en un CPD alterno

Cuando la decisión de activar el Plan de Contingencia es tomada, se mueve el CPD a otra localización. La principal función es continuar con las operaciones normales en el CPD alterno, como lo muestra la Figura 3.8. Cabe recalcar que en caso de una catástrofe de alta magnitud en la que no se pueda formalmente declarar la emergencia, el CPD en la nube podrá manejar las consultas o accesos a los servicios, puesto a que los Servidores que brindan estos servicios informáticos deben encontrarse operativos en todo momento.

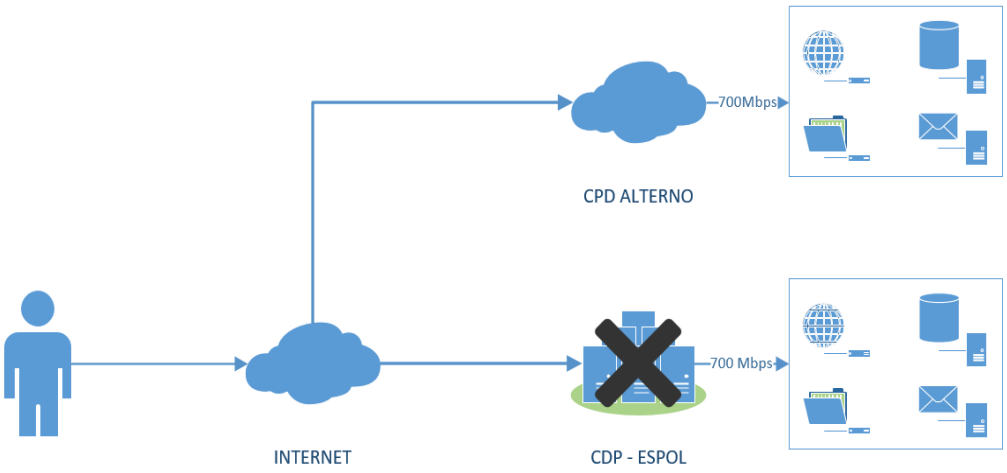


Figura 3.8 Diagrama de CPD Alternativo [10]

Fase de Recuperación

La finalidad de esta fase es restaurar el estado de las cosas tal como estaban antes de ocurrida la catástrofe.

Esta Fase depende principalmente de la existencia de respaldos de los servidores, por lo que se asume la existencia de información de respaldo almacenada fuera del CPD primario. El método de restauración será como lo muestra la Tabla 12.

Servicios	Método de Restauración de Información
Sistema Académico	Recuperación desde Respaldo almacenado en BackupNet
Sidweb	Recuperación desde Respaldo almacenado en BackupNet
Correo	Recuperación desde Respaldo almacenado en BackupNet
Sistema de Consejerías	Recuperación desde Respaldo almacenado en BackupNet

Tabla 12. Método de Restauración [12]

Fase de Retorno a las Instalaciones de GTSI-ESPOL

Una vez hayan sido Restaurados los Servidores de GTSI, basándose en el plan de contingencias se procederá a continuar con las actividades normales del CPD, brindando los servicios informáticos ya mencionados, procurando continuar la realización de las siguientes actividades:

- Creación periódica de Respaldos.
- Realizar un inventario de Respaldos.

Reanudación de Operaciones Normales

Una vez que la amenaza haya pasado, los equipos hayan sido reparados o reemplazados, o un nuevo Centro de Procesamiento de Datos haya sido construido y adecuado, el personal autorizado puede declarar la finalización del desastre y se puede proceder con la reanudación de Operaciones normales.

CAPÍTULO 4

4. EJECUCIÓN Y PRESUPUESTO

4.1 Ejecución

Para la ejecución de este Plan de Contingencia se estima un tiempo aproximado de dos meses, tiempo en el cual el personal de GTSI y el proveedor de la solución de Cloud Computing deben coordinar y realizar las actividades planeadas, así como realizar una etapa de pruebas, previo a la aprobación del trabajo.

Para esta implementación se ha dispuesto tomar varios miembros de GTSI, los cuales supervisarán las actividades realizadas por el proveedor mediante ATPs (Pruebas de Aceptación) y reportes por cada servicio llevado a la nube. El formato para de ATPs podrá ser encontrado en la sección de anexos [15].

Nombre	Duración	Inicio	Fin
IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA	44d	01/03/2017	01/05/2017
Fase de Inicio	**14d**	**01/03/2017**	**20/03/2017**
Revisión de Requerimientos por Parte del Proveedor	14d	01/03/2017	20/03/2017
Fase de Implementación	**19d**	**21/03/2017**	**14/04/2017**
Creación y Despliegue de VMs	7d	21/03/2017	29/03/2017
Configuración de Servidores	6d	03/04/2017	10/04/2017
Pruebas de Aceptación por parte del Proveedor	4d	11/04/2017	14/04/2017
Fase Final	**11d**	**17/04/2017**	**01/05/2017**
Periodo de Pruebas	5d	17/04/2017	21/04/2017
Pruebas de Aceptación Final	6d	24/04/2017	01/05/2017

El detalle de la plantación puede ser revisado en la sección de anexos.

4.2 Presupuesto

Se ha realizado un estudio que muestra el valor monetario de los servicios necesarios para el diseño del Plan de Contingencia. Este estudio no incluye los salarios mensuales de los miembros de GTSI que participen en la implementación del Plan de Contingencia.

Servicio	Cantidad	Subtotal (mensual)	Total(mensual)
Costo enlace 1 Gbps	1	$ 230,00	$ 230,00
Costo por Servidor Linux	2	$ 8,35	$ 16,70
Costo por Servidor Windows	22	$ 11,14	$ 245,08
TOTAL DE COSTOS MENSUALES			**$ 481,00**

Tabla 13. Costos mensuales BackupNet [13]

Los costos de mantenimiento o soporte técnico se calculan de manera independiente al valor total mensual que muestra la Tabla 13, estos costos podrían variar según el tipo de servicio que se solicite.

CONCLUSIONES Y RECOMENDACIONES

Mediante el análisis de las soluciones tecnológicas que mejor se adaptan a un Plan de Contingencia, se pudo observar que las alternativas de Cloud Computing en sus diferentes modelos de servicio e implementación, cumplen objetivo principal de salvaguardar la continuidad operativa de los Sistemas de Información.

En el diseño de este plan de contingencia se logró mostrar las posibles amenazas que pueden afectar la continuidad operativa de los Sistemas de Información y las medidas necesarias a tomarse con respecto a su magnitud de daño.

Se debe considerar mantener la creación constante de respaldos de la Información para que en caso de alguna catástrofe sea mucho más sencilla la recuperación ante la mismo.

Se logró destacar, que no existe un plan de contingencias único para todas las organizaciones, esto puede cambiar según el tipo de infraestructura que tenga la institución y al tipo de industria o funciones a la que se dedica.

Por motivos de presupuesto la Implementación de este Plan de Contingencia no se puede realizar en este momento, por lo que este diseño queda como un modelo a seguir, en caso de que se realice la implementación.

A nivel nacional CNT (Corporación Nacional de Telecomunicaciones) cuenta con un CPD, que permite almacenamiento de datos tanto para las entidades públicas como para las privadas, por lo que podría beneficiar de cierto modo a ESPOL al ser una institución pública.

Los costos de Soporte Técnico por parte del proveedor no se encuentran detallados en este documento, debido a que los mismos deben ser negociados por el Administrador del Proyecto de parte del proveedor.

Se recomienda la constante actualización del Plan de Contingencia para Servicios Informáticos de GTSI-ESPOL, para obtener los mejores resultados posibles.

BIBLIOGRAFÍA

[1] Wikipedia Org., (2016, Agosto 14). Centro de procesamiento de datos [online].

Disponible en:

https://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos

[2] Data Center Knowledge, (2016, Enero 6). Data Center Design: Which Standards to Follow? [online]. Disponible en:

http://www.datacenterknowledge.com/archives/2016/01/06/data-center-design-which-standards-to-follow/

[3] Wikipedia Org., (2016, Agosto 13). Cloud Computing [online]. Disponible en: https://en.wikipedia.org/wiki/Cloud_computing

[4] DOSControl, (2016, febrero 7). Tipos de nubes Cloud Computing [online]. Disponible en: http://doscontrol.com/cloud-computing/tipos-de-nubes

[5] Marc Fabregat, (2010, diciembre 28). La nube IaaS, SaaS, PaaS, SaaS, ITaaS [Online]. Disponible en: http://goo.gl/TO5X3S

[6] Protejete, (2014, septiembre 5). Gestión de Riesgo Seguridad Informática [online]. Disponible en: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

[7] Guy Witney Krocker, (2002, Agosto 5). Disaster Recovery Plan Testing: Cycle the Plan, Plan the Cycle [online]. Disponible en:

https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-testing-cycle-plan-plan-cycle-563

[8] Wikipedia Org., (2016, Agosto 13). Amenazas para un CDP [online]. Disponible en:

https://es.wikipedia.org/wiki/Terrorismo#Armas_terroristas

[9] German Pacio, (2014, Octubre 7). Recuperación de Desastres Data Center [online]. Disponible en: http://www.datacentershoy.com/2014/10/recuperacion-de-desastres-en-el-data.html

[10] Telconet S.A., (2013, Febrero 23). BackupNet Telconet S.A. [online]. Disponible en: http://www.telconet.net/servicios/cloudpublica/backupnet

[11] Telconet S.A. Backupnet, (2013, Enero 8). Características de BackupNet [online]. Disponible en: http://www.backupnet.ec/caracteristicas

[12] AWS Amazon, (2016, Agosto 20). Infraestructura global de AWS [online]. Disponible en: https://aws.amazon.com/es/about-aws/global-infrastructure/

[13] AWS Amazon, (2016, Agosto 7). Zonas de disponibilidad y regiones de AWS [online]. Disponible en: https://aws.amazon.com/es/about-aws/global-infrastructure/

[14] AWS Amazon, (2016, Enero 3). Cotización de costos de servicios AWS. Disponible en: http://calculator.s3.amazonaws.com/index.html

[15] TechNet Magazine, (2016, Agosto 16) Cloud Computing: las pruebas de la nube [Online]. Disponible en:

https://technet.microsoft.com/es-es/magazine/hh395480.aspx

ANEXOS

GLOSARIO

GTSI - Gerencia de Tecnologías y Sistemas de Información

TI - Tecnologías de Información

WAN - Wide Area Network

LAN - Local Area Network

CDP - Centro de Procesamiento de Datos

GCI - Global Cloud Index

DR - Disaster Recovery

ISP - Internet Services Provider

Máquina Virtual - Es un software que simula a una computadora y puede ejecutar programas como si fuese una computadora real.

ITIL - Information Technology Infrastructure Library

COBIT - Objetivos de Control para la Información y Tecnologías Relacionadas.

NIST - Instituto Nacional de Normas y Tecnología

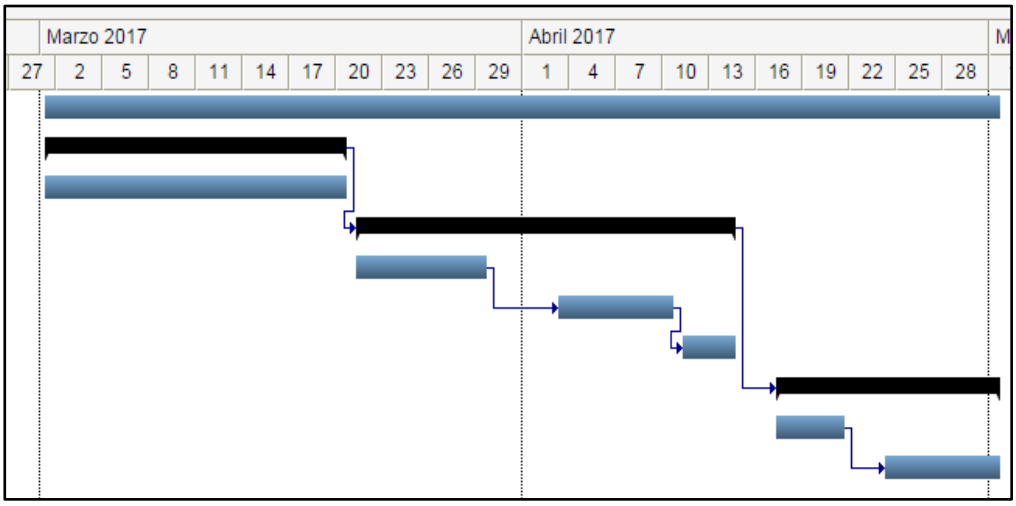
UPS - Uninterruptible Power Supply

TIC – Tecnologías de la Información y la Comunicación

ATP - Acceptance Test Protocol

1.- Planificación para la Implementación.

Nombre	Duración	Inicio	Fin
IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA	44d	01/03/2017	01/05/2017
Fase de Inicio	**14d**	**01/03/2017**	**20/03/2017**
Revisión de Requerimientos por Parte del Proveedor	14d	01/03/2017	20/03/2017
Fase de Implementación	**19d**	**21/03/2017**	**14/04/2017**
Creación y Despliegue de VMs	7d	21/03/2017	29/03/2017
Configuración de Servidores	6d	03/04/2017	10/04/2017
Pruebas de Aceptación por parte del Proveedor	4d	11/04/2017	14/04/2017
Fase Final	**11d**	**17/04/2017**	**01/05/2017**
Periodo de Pruebas	5d	17/04/2017	21/04/2017
Pruebas de Aceptación Final	6d	24/04/2017	01/05/2017



2.- Formato de ATP

PROTOCOLO DE PRUEBAS DE ACEPTACIÓN

PROYECTO:

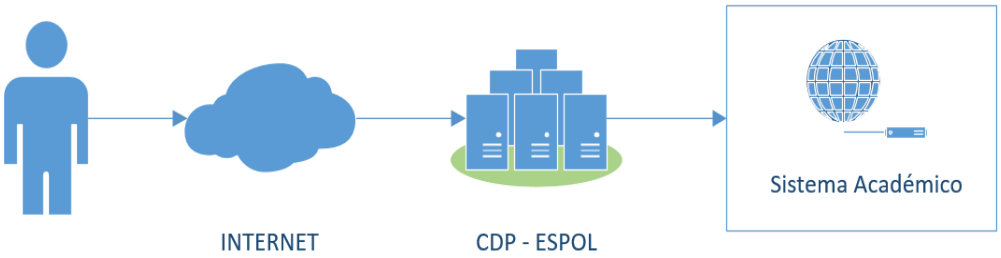
“Infraestructura Virtual de Contingencia en la Nube para los Servicios Informáticos brindados por GTSI-ESPOL”

SISTEMA ACADÉMICO

Tabla de Contenido

Modelo de Implementación Actual

El Servicio del Sistema Académico se encuentra operativo sobre una infraestructura virtualizada, y cuenta con 9 Servidores con Windows Server 2012 R2, los cuales se encargan del balanceo de carga de las solicitudes hacia este servicio.

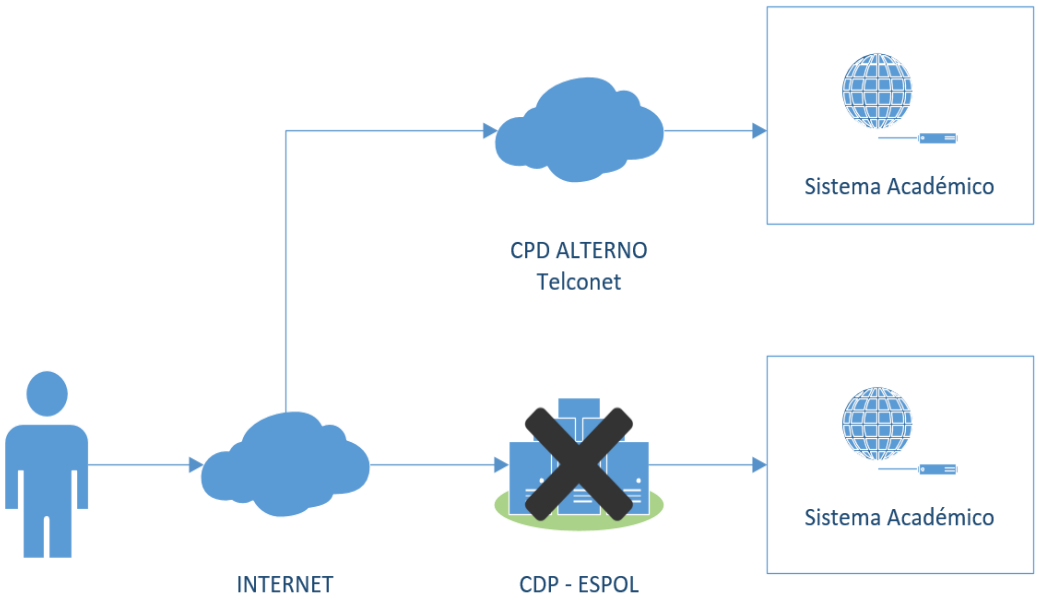


Modelo de Implementación Lógico

Interfaz Web del Sistema Académico

Diseño de la Solución

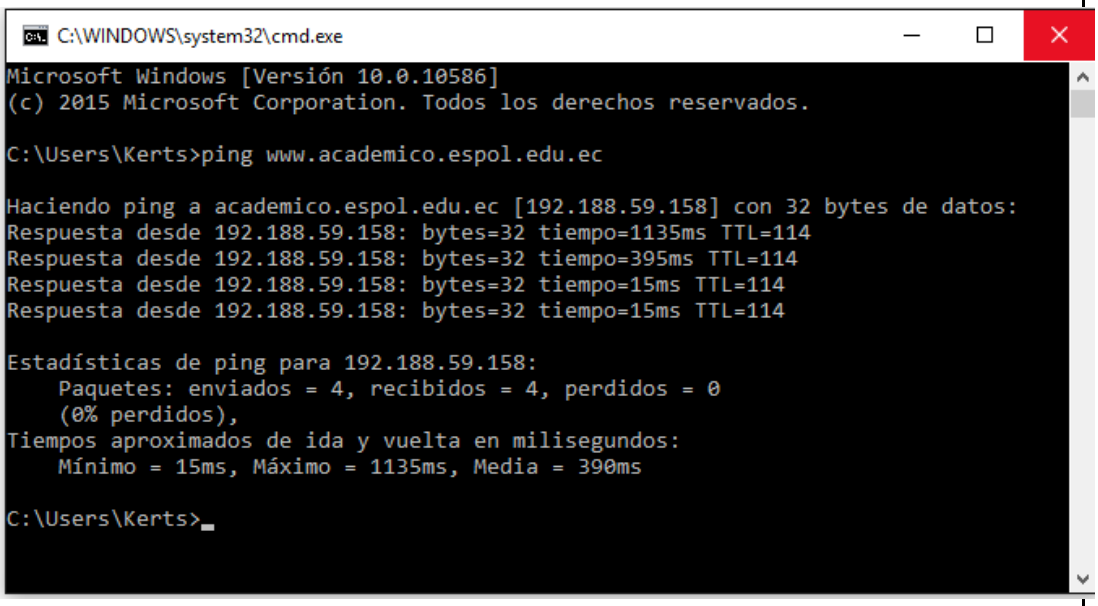
El servicio del Sistema Académico se encuentra operativo de la misma manera, pero sobre una infraestructura virtualizada en la nube.



Modelo de Implementación lógico de la Solución

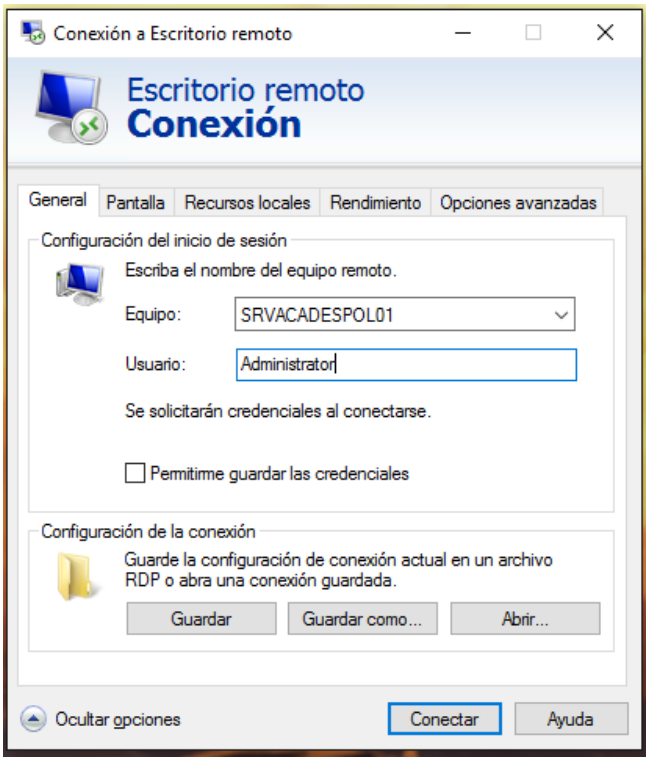
Pruebas End-to-End

Pruebas de conectividad Extremo a Extremo entre los Servidores Virtuales que brindan el Servicio del Sistema Académico y una máquina cliente.

Pruebas de Ping
Procedimiento: Realizar pruebas de conectividad Extremo a Extremo mediante el uso del comando “ping” desde la interfaz de línea de comando de un computador cliente: ping www.academico.espol.edu.ec
Resultado: 
Pruebas de conexión a escritorio remoto

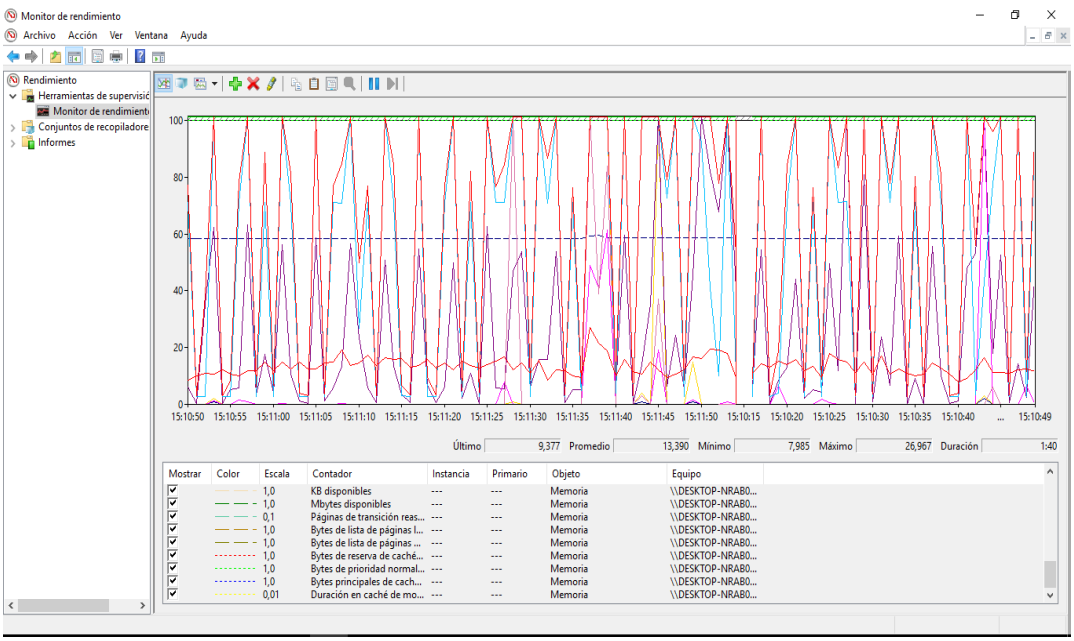
Procedimiento:

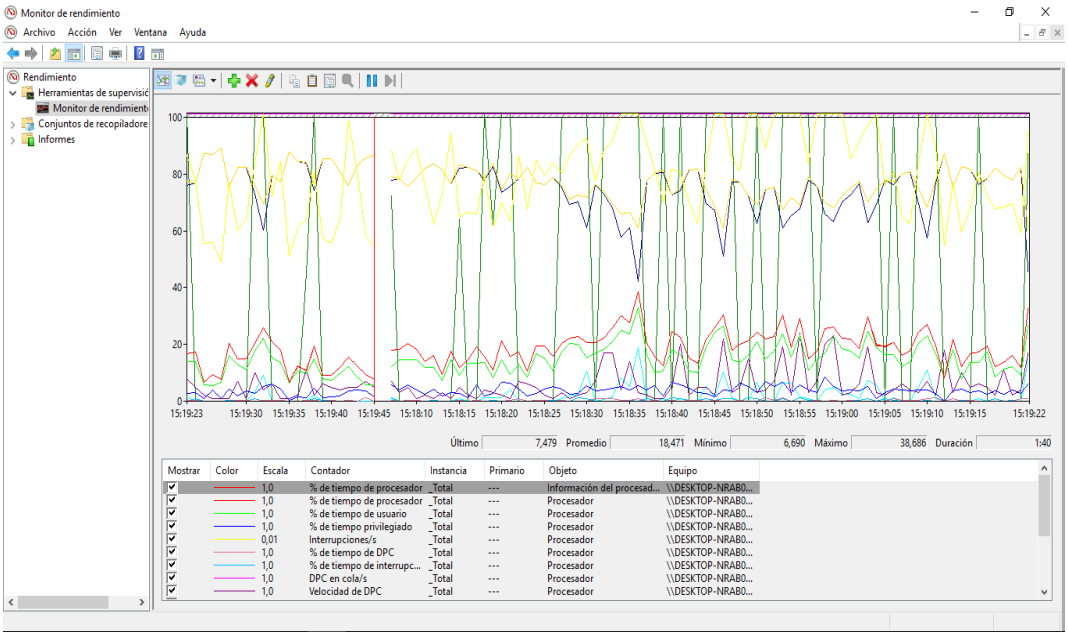
Realizar pruebas de conexión a escritorio remoto hacia los Servidores del Sistema académico mediante el uso de “Remote Desktop Connection Client”



Pruebas de Servidores Virtuales

Pruebas de performance de rendimiento.

Pruebas de rendimiento de Memoria
Procedimiento: Comprobar el uso de la Memoria RAM del Servidor usando “Performance Monitor”
Resultado: 

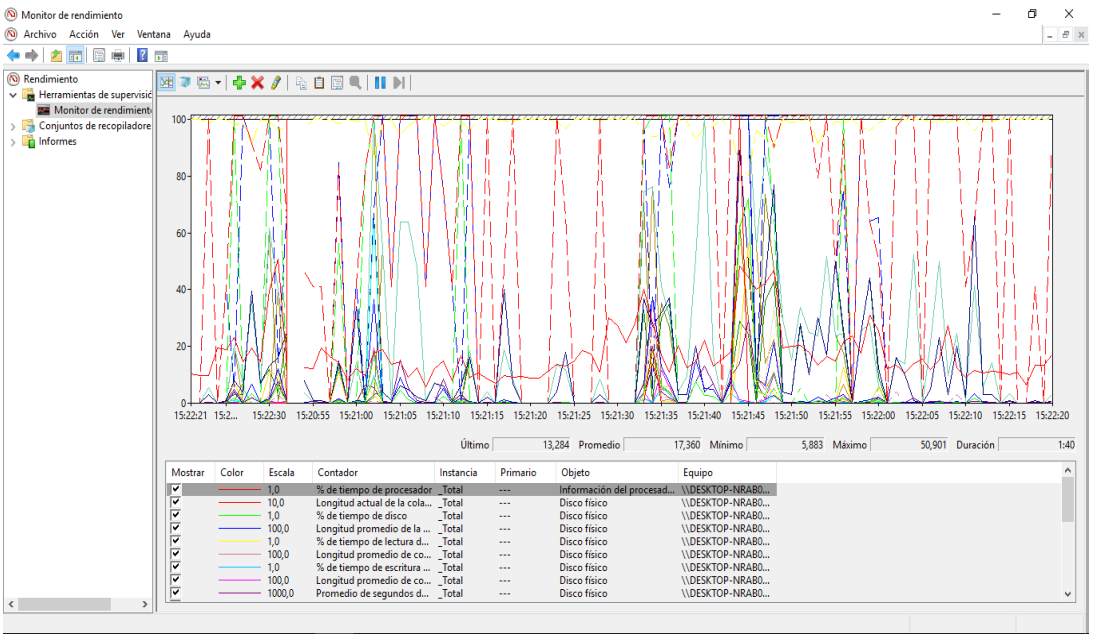
Pruebas de rendimiento de Procesador
Procedimiento: Comprobar el uso del Procesador del Servidor usando “Performance Monitor”
Resultado: 

Pruebas de rendimiento de Disco Duro

Procedimiento:

Comprobar el uso del Disco Duro del Servidor usando “Performance Monitor”

Resultado:



Aprobación de las Pruebas

Nombre de la Prueba	AP	RP	N/A
Pruebas End-to-End			
Pruebas de Ping			
Pruebas de Conexión a Escritorio Remoto			
Pruebas de Servidores Virtuales			
Pruebas de Performance de Memoria			
Pruebas de Performance de Procesador			
Pruebas de Performance de Disco Duro			

Aprobación del Documento

	Nombre	Firma	Fecha
ESPOL - Fiscalizador			
Telconet			

3.- Disaster Recovery Plan Template, by Sungard

Plan section:

Recovery Strategies and Activities

After the initial introductory section, there are usually a number of modules about the strategies outlined in the plan, as well as the specific personnel undertaking the recovery and the recovery activities.

Examples of sections that you may want to consider for your own BC/DR plan include:

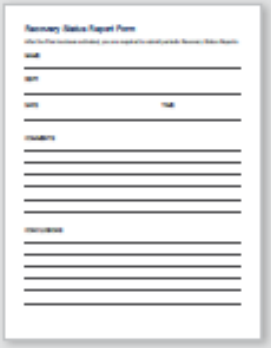
- **Recovery Strategy Summary:** In this section, a plan will typically outline the broad strategies to be followed in each of the scenarios identified in the plan introduction section. As an example, if "loss of work area" is identified as a possible failure scenario, a potential recovery strategy could be to relocate to a previously agreed-upon or contracted alternate work location, such as a Sungard AS work area recovery center.
- **Recovery Tasks:** This section of the plan will usually provide a list of the specific recovery activities and sub-activities that will be required to support each of the strategies outlined in the previous section. For example, if the strategy is to relocate to an alternate work location, the tasks necessary to support that relocation effort could include identifying any equipment needs, providing replacement equipment, re-issuing VPN tokens, declaration of disaster, and so on.
- **Recovery Personnel:** Typically, a BC/DR plan will also identify the specific people involved in the business continuity efforts, for example, naming a team lead and an alternate team lead, as well as the team members associated with any recovery efforts. This section of the plan will also include their contact information, including work phone, cellphone, and email addresses. Obviously, because of any potential changes in personnel, the plan will need to be a "living" document that is updated as personnel/workforce changes are made.
- **Plan Timeline:** Many plans also include a section in the main body that lays out the steps for activating a plan (usually in the form of a flow chart). For example, a typical plan timeline might start from the incident detection, then flow into the activation of the response team, the establishment of an incident command center, the notification of the recovery team, followed by a decision point around whether or not to declare a disaster. A plan timeline may also assign the recovery durations or recovery time objectives required by the business for each activity in the timeline. Figure 1 provides an example timeline for an IT disaster recovery organization is given below for critical Tier 1 systems and the resumption of business operations.
- **Critical Vendors and their RTOs:** In this section, a plan may also list the vendors critical to day-to-day operations and recovery strategies, as well as any required recovery time objectives that the vendors must meet in order for the plan to be successful.
- **Critical Equipment/Resource Requirements:** A plan may also detail the quantity requirements for resources that must be in place within specified timeframes after plan activation. Examples of resources listed might include workstations, laptops (both with and without VPN access), phones, conference rooms, etc.

Plan section:

Appendices

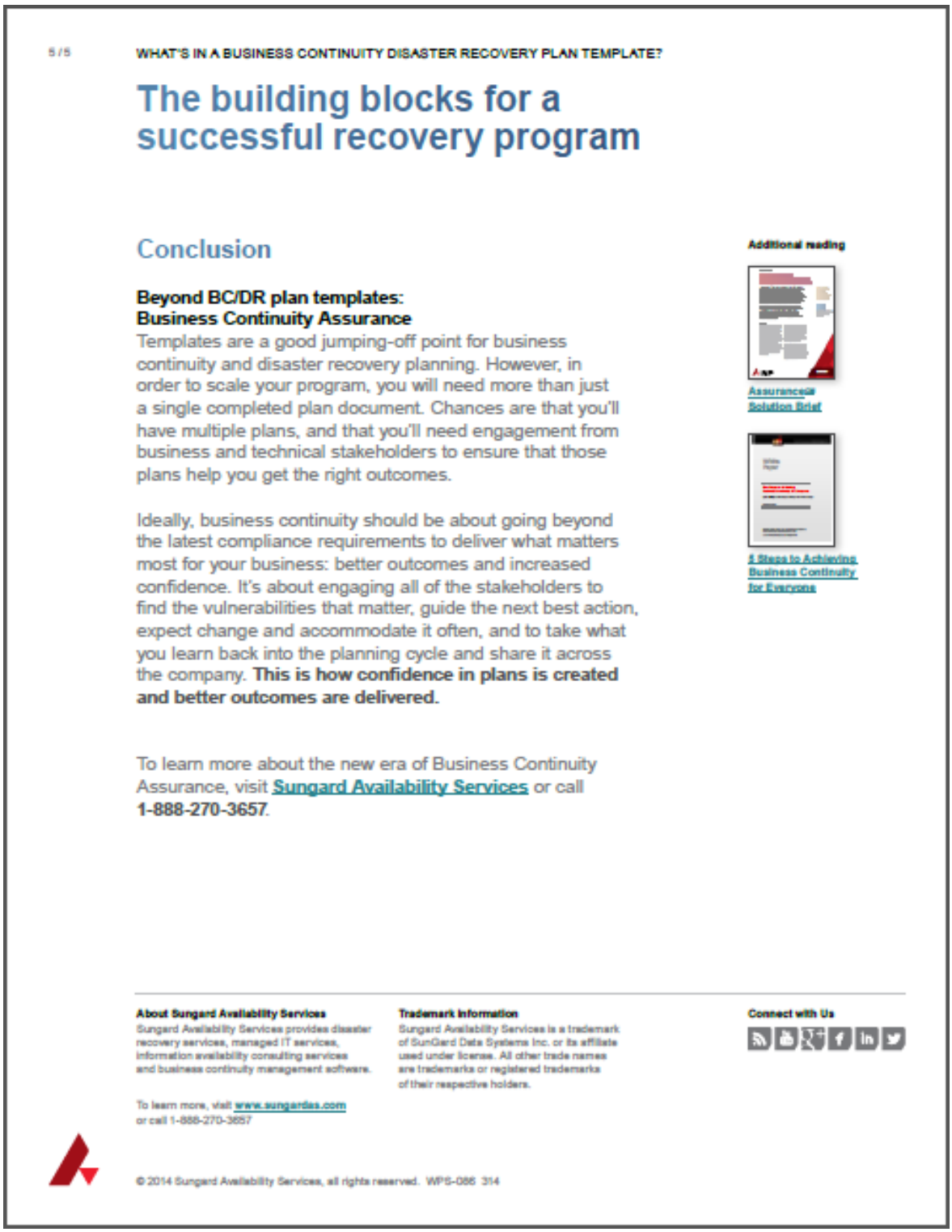
Every plan contains appendices unique to the entity for which the plan was created, so there is not a great deal of standardization in the appendices. In general, a plan's appendix is an excellent place to include the details specific to the successful recovery of the specific entity for which the plan is being created. Below we have provided examples of the types of information included in plan appendices, which you can customize according to the needs and functions of your specific group, department, business unit, or company.

Figure 2:
Example recovery status report form



Include details that are specific to your organization's recovery success in the appendix of your BC/DR Plan.

- **Business Continuity Site Information:** If your plan calls for "failing over" to an alternate work location, it may be a good idea to include information about that alternate work site in the plan's appendix. The details of the site might include:
  - Commencement date (including last contract renewal date)
  - Location of the facility
  - Details about the office environment, such as number of workstations, servers, telephony, printers, internet access, and other equipment provided
  - Site contact details
  - How the site is invoked and the personnel authorized to invoke it
- **Maps of meeting points:** For those plans specifying a meeting location for employees, maps of the routes and alternate routes to those locations are useful.
- **Vendor Contact Information:** Many plans include the details of how to reach the vendors listed as critical to normal operations or recovery operations.
- **Forms:** If there are forms required by the plan, such as an incident report form, injury summary form, disaster-related expense tracking forms, consolidated status report forms, manual purchase order forms, etc., the plan appendix is a useful place to locate them. Figure 2 provides an example of a Recovery Status Report Form.
- **Communication Plans:** Successful plans will include the individuals responsible for communications during the time in which the plan is invoked, as well as the groups or constituents with which they are responsible for communicating. For example, it would be desirable to specify both internal and external communicators. For internal communicators, you will need to identify the person communicating with the command team and with employees, as an example. For external communicators, best practices include identifying the individual in charge of communications with the media, with customers, with partners, and with vendors, etc.
- **Disaster Declaration Procedures:** If there are business continuity or disaster recovery vendors contracted, the plan appendix may be a good place to include any relevant disaster recovery procedures, such as Sungard AS Recovery Services.
- **Employee Contact Information:** Instead of inserting the contact details of the employees in the Recovery Strategies and Activities section of the plan (which can often take up many pages and become unwieldy), you can also leverage the plan's Appendices as an alternate location for this information, as well as any phone tree procedures or call lists.
- **Process Flows:** During plan activation, employees must often follow alternative processes or procedures (because primary processes are down or unavailable). Therefore, the plan appendices is a good place to list any out-of-process flows or procedures. For example, how to create manual purchase orders, how to take use corporate credit cards, how to access fuel/cash access cards.
- **Checklists:** Checklists that provide useful reminders of "what to do" are often found in plan appendices. During an unexpected outage, human beings are often operating under higher levels of stress and anxiety, so offering them an easy-to-access checklist of to-dos can smooth and even automate the recovery process towards a successful result. Examples of checklists might be the steps involved in accessing an application via the Internet, or how to redirect call volumes in a call center.



5 / 5

WHAT'S IN A BUSINESS CONTINUITY DISASTER RECOVERY PLAN TEMPLATE?

The building blocks for a successful recovery program

Conclusion

Beyond BC/DR plan templates: Business Continuity Assurance

Templates are a good jumping-off point for business continuity and disaster recovery planning. However, in order to scale your program, you will need more than just a single completed plan document. Chances are that you'll have multiple plans, and that you'll need engagement from business and technical stakeholders to ensure that those plans help you get the right outcomes.

Ideally, business continuity should be about going beyond the latest compliance requirements to deliver what matters most for your business: better outcomes and increased confidence. It's about engaging all of the stakeholders to find the vulnerabilities that matter, guide the next best action, expect change and accommodate it often, and to take what you learn back into the planning cycle and share it across the company. **This is how confidence in plans is created and better outcomes are delivered.**

To learn more about the new era of Business Continuity Assurance, visit Sungard Availability Services or call **1-888-270-3657**.

Additional reading

Assurance@ Solution Brief

8 Steps to Achieving Business Continuity for Everyone

About Sungard Availability Services

Sungard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software.

To learn more, visit www.sungardas.com or call 1-888-270-3657

Trademark Information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us

4.- Plantilla para la clasificación y valoración de Magnitud de Daños, Plantilla de Valoración de Probabilidad de Ocurrencia de Eventos