VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN GERENCIA DE SISTEMAS

X PROMOCIÓN

TESIS DE GRADO MAESTRA EN GENERENCIA DE SISTEMAS

TEMA: "PLAN DE CONTINGENCIAS PARA EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE CTT-ESPE-CECAI INNOVATIVA SEDE SANGOLQUI."

AUTOR: ING. ALCIVAR VALENCIA, LILIAN ALEXANDRA

DIRECTOR: ING. OSWALDO DÍAZ

SANGOLQUÍ, MAYO DEL 2014

CERTIFICACIÓN DEL DIRECTOR

El suscrito Ing. Oswaldo Díaz Msc., con cedula de identidad No. 0400652020, en calidad de Director de Tesis de la Maestría en Gerencia de Sistemas,

CERTIFICA

Que el presente proyecto de grado que lleva como título**, "PLAN DE CONTINGENCIAS PARA EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE CTT-ESPE-CECAI INNOVATIVA SEDE SANGOLQUI**." realizado por la Ingeniera Lilian Alexandra Alcívar Valencia, de nacionalidad ecuatoriana, con cédula de identidad No. 1714367099, como requisito para la obtención del título de Magíster en Gerencia de Sistemas**,** X Promoción de la ESPE, fue desarrollada bajo mi dirección y asesoría. La misma que cumple con los requerimientos científicos, tecnológicos y académicos, razón por la cual autorizo su presentación y defensa.

Sangolquí, Mayo de 2014

_____

ING. OSWALDO DÍAZ., Msc.

DIRECTOR

Sangolquí - Ecuador, 14 de Mayo del 2014

DECLARACIÓN DE RESPONSABILIDAD

LIILAN ALEXANDRA ALCÍVAR VALENCIA

DECLARA QUE:

El proyecto de posgrado denominado "**PLAN DE CONTINGENCIAS PARA EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE CTT-ESPE-CECAI INNOVATIVA SEDE SANGOLQUI**.", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Mayo del 2014

_____

ING. LILIAN ALEXANDRA ALCÍVAR VALENCIA

AUTOR

AUTORIZACIÓN

Yo,

LILIAN ALEXANDRA ALCÍVAR VALENCIA

Autorizo a la Universidad de las Fuerzas Armadas – ESPE, la publicación, en la biblioteca virtual de la Institución, el trabajo titulado "**PLAN DE CONTINGENCIAS PARA EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE CTT-ESPE-CECAI INNOVATIVA SEDE SANGOLQUI**.", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Mayo del 2014

_____

ING. LILIAN ALEXANDRA ALCÍVAR VALENCIA

AUTOR

Agradecimiento

A Dios, por las bendiciones recibidas y por haberme permitido cumplir con el objetivo de mejorar profesionalmente al estudiar esta Maestría.

A mis hermanos Natalia, Lenin y Edwin, a mis familiares, amigos y amigas que con su cariño y apoyo han sido un pilar fundamental para seguir adelante.

Al Ing. Oswaldo Díaz y al Ing. Germán Ñacato por aportar con su conocimiento y experiencia para llevar a cabo este proyecto y por brindarme su amistad.

Lilian

Dedicatoria

A mis Padres Gabriel y Lilia, porque siempre he contado con ellos, han sido una muestra de amor, abnegación, de lucha y sacrificio, además me han inculcado valores que me han convertido en la persona que soy.

A Patricia Elizabeth Auqui Parra, iniciamos juntas la Maestría, con la ilusión de obtener más conocimientos y mejorar profesionalmente, pero Dios se la llevo a su lado antes de que pudiera cumplir con este objetivo, siempre estarás en nuestros recuerdos y en nuestros corazones.

A todas las mujeres que al igual que yo conviven con el Síndrome de Turner, porque somos unas luchadoras incansables y valientes, capaces de superar las adversidades y cumplir cualquier meta que nos propongamos.

A mis sobrinos David y Camila que con su ternura iluminan mis días y me llenan de alegría, recordándome a cada instante que la verdadera felicidad está en la cosas más sencillas que la vida nos regala.

Lilian

Índice de Contenido

Índice de Tablas

Introducción

Actualmente la tecnología es indispensable para la realización de las actividades de cualquier empresa o institución, debido a que facilita la ejecución de los procesos, además la información y los datos son indispensables en la toma de decisiones. El avance tecnológico ha permitido una evolución en la educación permitiendo facilitar el proceso de enseñanza aprendizaje y vencer las barreras de tiempo y espacio

Innovativa, es una empresa pública adscrita a la Universidad de las Fuerzas Armadas – ESPE, dedicada a prestar servicios de transferencia tecnológica y capacitación a nivel nacional tanto de manera presencial como virtual, la misma que ha ido creciendo con el pasar de los años, y actualmente cuenta con veinte centros de capacitación ubicados en diez provincias del país.

Innovativa depende el buen funcionamiento de su infraestructura tecnológica y de la información para poder brindar un servicio de calidad, la interrupción de los servicios Informáticos por largo tiempo puede ocasionar pérdidas económicas y afectar la credibilidad de sus clientes. Lo que implica que se deben aplicar medidas de seguridad para protegerlas y estar preparados para afrontar los diversos tipos de contingencias, por lo cual se debe contar con un plan de contingencias, que debe considerar los riesgos y vulnerabilidades de la empresa para

proponer controles que permitan prevenir, mitigar y recuperarse de un siniestro a la brevedad posible y continuar prestando sus servicios de manera eficiente y eficaz.

Resumen

El desarrollo del Plan de Contingencias para el Área de Tecnologías de la Información de CTT-ESPE-CECAI INNOVATIVA Sede Sangolquí tiene como objetivo definir los controles de prevención, mitigación y recuperación de destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

Tomado como referencia la información de INNOVATIVA y del Área de Tecnológias de la Información recabada en el proyecto "Estudio de Factibilidad para la elaboración del Plan de Contingencias del Área de Tecnologías de la Información de CTT-ESPE-CECAI INNOVATIVA Sede Sangolquí", se ha realizado análisis de los riesgos encontrados, y se han definido tres tipos de controles que deben ser implementados para que la empresa pueda prevenir, mitigar y recuperar sus activos de TI en caso de enfrentarse a una contingencia.

Se recomienda implementar los controles de prevención en un tiempo de seis meses, además realizar las pruebas de los procesos de mitigación y recuperación.

Abstract

The development of the Contingency Plan for the Area of Information Technologies of CTT- ESPE - CECAI INNOVATIVA Sangolquí,, aims to define the controls for prevention, mitigation and recovery information to protect against damages caused by cutting services, natural or human phenomena.

Taken as reference information INNOVATIVE and Area Information Technology gathered in the project " Feasibility Study for the development of the Contingency Plan Area Information Technology CTT - ESPE - CECAI INNOVATIVE See Sangolquí " , has conducted risk analysis models found and defined three types of controls that should be implemented to enable the undertaking to prevent, mitigate, and recover your IT assets if confronted with a contingency .

It is recommended to implement preventative controls in a time of six months, further testing of mitigation and recovery processes.

CAPÍTULO I

1. Generalidades

1.1. Planteamiento del problema

Innovativa, institución adscrita a la Escuela Politécnica del Ejército ESPE cuya misión es realizar transferencia de tecnología mediante el desarrollo de proyectos y prestación de servicios de capacitación, asesoría y consultoría para contribuir al desarrollo del país; sustentados en el conocimiento, innovación y estímulo de la investigación científica, cuenta con el Departamento de sistemas, que es el encargado de Coordinar, supervisar, gestionar y ejecutar los procesos que permitan fortalecer la plataforma tecnológica de hardware y software del CTT-ESPE-CECAI, mediante el uso de herramientas de tecnologías de información y comunicaciones, que faciliten la administración y aseguramiento de la información institucional.

Sin embargo el Área de TI, no tiene al momento un plan de contingencias que permita resolver inmediatamente los problemas que se suscitan, lo cual implica que este departamento no pueda aportar adecuadamente al cumplimiento de los objetivos estratégicos institucionales y conlleva a un mal uso de los recursos. Además las líneas de negocio que mantiene Innovativa, dependen directamente del correcto funcionamiento de la tecnología y de una pronta recuperación de posibles fallos.

Por lo tanto es necesario empezar a utilizar un plan de contingencias, que sea fiable y seguro para poder cumplir con los objetivos del negocio y satisfacer las necesidades del cliente eficientemente.

1.2. Formulación del problema a resolver

- ¿Cómo se están llevando actualmente los procesos críticos del Área de Tecnologías de Información?
- ¿Qué riesgos informáticos existen en CTT-ESPE-CECAI INNOVATIVA?
- ¿Cómo reaccionar cuando se presente algún desastre informático en CTT-ESPE-CECAI INNOVATIVA?

1.3. Objetivo General

Generar el plan de contingencias de TI de Innovativa para que pueda aportar eficientemente y eficazmente al cumplimiento de los objetivos del negocio.

1.4. Objetivos Específicos

- Conocer lo que existe a nivel mundial y local sobre planes de contingencia informáticos
- Realizar un análisis de las Normas que se deben considerar para generar el plan de contingencias

- Conocer los riesgos informáticos a los que se enfrenta CTT-ESPE-CECAI INNOVATIVA actualmente
- Proponer soluciones a los riesgos informáticos existentes en CTT-ESPE-CECAI INNOVATIVA

CAPÍTULO II

2. Marco Teórico

2.1. Antecedentes del estado del arte

2.1.1. Plan de contingencia informático para la Municipalidad de La Punta

El Plan de Contingencia Informático de la Municipalidad de la Punta establece el objetivo, alcance y metodología desarrollada. Incluye además, las definiciones utilizadas, las políticas de seguridad, el análisis de la situación, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos de TI.

La metodología práctica comprende: la identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

Permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

Ha sido elaborado tomando como base, la Metodología ITIL (INFORMATION

TECNOLOGY INFRASTRUTURE LIBRARY) - Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información, y la Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información del INEI (Instituto Nacional de Estadística e Informática, Perú).

Finalmente, se presentan los anexos como parte complementaria que ayudará a estar preparados frente a cualquier contingencia en los procesos críticos.

Básicamente el plan de contingencias realiza un estudio de los procesos para definir cuáles son los de más alto impacto, 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. (Municipalidad de la Punta, 2010)

2.1.2. Propuesta de Contingencia de sistemas informáticos de la Empresa “T” – Colombia (2012)

Este plan de contingencia pretende indicar los procedimientos a seguir en caso de falla en cualquier componente de la plataforma tecnológica que soporta el sistema de información actual de la compañía, es decir, el ERP J.D. Edwards.

Los procedimientos específicos, en caso de contingencia, de cada una de las áreas de la compañía que gestionan su información en el ERP, serán elaborados y documentados por cada líder de área y junto con este Plan de Contingencia de TI, conformarán el Plan de Contingencia Integral de la Organización.

El objetivo general es garantizar que los procesos críticos de operación de la compañía puedan continuar desarrollándose, a pesar de no contar con la disponibilidad del sistema de información. Y los objetivos específicos son:

- Establecer el procedimiento que debe seguir el equipo del Departamento de Sistemas para entregar a los usuarios respaldo durante y después del incidente presentado en la plataforma informática del ERP.
- Definir los mecanismos para almacenar la información clave que debe registrarse, así sea de manera manual, continuando con el desarrollo de los procesos críticos de la compañía
- Definir las prácticas ideales para disminuir los tiempos que requiera la puesta en marcha del plan de contingencia durante la presentación de un incidente.

En este plan de contingencias se parte haciendo una descripción de los servicios que presta la empresa y la relación que tienen con las Tic’s, luego ser realiza una valoración de los riesgos , se generan acciones de mitigación del riesgo y acciones de contingencia, además se definen responsables en cada caso,

considerando los servicios de red, los sistemas operativos, las bases de datos, aplicaciones de apoyo, caída de del canal de comunicaciones al data center, fallos en los equipos de red, fallos en los servidores, fluido de energía eléctrica. Fallas en los equipos eléctricos, riesgos de incendio, riesgo de robo de equipos, riesgo de accesos no autorizados al servidor (Ramirez, Londoño, & Gómez, 2012).

2.1.3. Plan de contingencia informático para el Instituto del Mar del Perú (2012-2015)

El objetivo general de este plan de contingencias es garantizar la continuidad de las actividades del IMARPE, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales.

Sus objetivos específicos son:

- Contar con documentación práctica y actualizada que garantice al IMARPE la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.

- Contar con personal debidamente capacitada y organizada para afrontar adecuadamente las contingencias que puedan presentarse en las actividades del IMARPE.

La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

Este plan de contingencias utiliza una metodología de seis fases: Fase 1: Organización, Fase 2: Identificación y priorización de riesgos, Fase 3: Definición de eventos susceptibles de contingencia, Fase 4: Elaboración del Plan de Contingencia, Fase 5: Definición y Ejecución del Plan de Pruebas, Fase 6: Implementación del Plan de Contingencia.

Además propone una organización del plan de contingencias definiendo un grupo responsable y consta de un Comité de contingencia de Seguridad, Contraloría del Plan de contingencia y Seguridad y Coordinación Ejecutora del Plan.

Luego se realiza una identificación y priorización de Riesgos evaluando la probabilidad con la que sucedería, el impacto, la ponderación, la alerta, y se le asigna una categoría de controlables o no controlables, además se los ha clasificado en

riesgos relacionados a siniestros, sistemas de información, recursos humanos y un plan de seguridad física.

Para el desarrollo del plan de contingencias se realiza un flujo general que explica la forma de responder ante la ocurrencia de una contingencia. Y se asigna un responsable para casa evento de contingencia poniendo además su teléfono de contacto y se describen las actividades a desarrollarse para prevenir, ejecutar y recuperarse de la contingencia (Instituto del Mar del Perú, 2012).

2.1.4. Plan de Contingencia informático de la empresa municipal administradora de peaje en Lima (2011)

El principal objetivo de este Plan de Contingencia es la de garantizar la continuidad de las operaciones de la Empresa Municipal Administradora de Peaje de Lima (EMAPE S.A.)

El referido plan tiene como finalidad identificar los riesgos, establecer los procedimientos y mecanismos para preservar la seguridad de los equipos de cómputo, proteger la información almacenada en ellos y garantizar la continuidad de las funciones de la Empresa Municipal Administradora de Peaje de Lima

Este plan inicia identificando las actividades que implican un riesgo, tomando en cuenta factores endógenos y los factores exógenos.

En los factores endógenos se considera, problemas con la tubería de agua y desagüe, daño en el cableado de la red, fallas de Equipo de comunicaciones, inoperatividad de Servidores de Comunicación, Inoperatividad de Servidores de Bases de Datos, Inoperatividad del servido DNS interno, inconvenientes eléctricos, pérdida de la información, Acción de Virus informáticos, alteración de la información.

En cuanto los factores exógenos se consideran : corte de fluido eléctrico, Corte de Servicio de Circuito Digital, Averías el Circuito Digital, Inoperatividad del Servidor DNS Externo, Acción de Virus Informáticos, Incendios, Sismos, Atentados, Hackers.

Luego define los posibles escenarios tomando en cuenta los factores de vulnerabilidad, la estimación de la gravedad y el riesgo.

En el plan de contingencias define las actividades a realizarse previas, durante y después del desastre (Empresa Municipal Administradora de Peaje de Lima, 2011).

2.1.5. Plan de Contingencia informático y seguridad de la información, aplicado en la Universidad nacional de Piura (2009) – Perú

En este Plan de contingencias se proponen los siguientes objetivos:

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

Se ha realizado un análisis de todas las posibles causas a las cuales pueden estar expuestos los equipos informáticos conectados a la RED de la UNP, así como la información contenida en cada medio de almacenamiento. Se realizara un análisis de riesgo y el Plan de Operaciones tanto para reducir la posibilidad de ocurrencia como para reconstruir el Sistema de Información y/o Sistema de Red de Computadoras en caso de desastres.

El Plan incluye la formación de equipos de trabajo durante las actividades de establecimiento del Plan de Acción, tanto para la etapa preventiva, correctiva y de recuperación.

El Plan de Reducción de Riesgos es equivalente a un Plan de Seguridad, en la que se considera todos los riesgos conocidos, para lo cual se hará un Análisis de riesgos.

El plan de contingencias informático de la Universidad de Piura empieza realizando un plan de reducción de riesgos, para lo cual parte de un análisis de riesgo clasificándooslos por bienes susceptibles de daño en los que toma en cuenta el

personal, el hardware, software, datos, documentación, suministro de energía y suministro de telecomunicaciones.

Para cada riesgo se analiza su grado de negatividad, la frecuencia con la que puede ocurrir, el grado de impacto, y el grado de certidumbre. Además la situación actual en la que se encuentra actualmente y las posibles acciones correctivas para mitigar el riesgo.

Los riesgos que se consideran son: Incendio o Fuego, Robo común de equipos y archivos, Sabotaje, Falla en los equipos, Equivocaciones, Acción virus informático, Fenómenos naturales, Accesos no autorizados, Robo de datos, Manipulación y sabotaje.

Luego se realiza un Análisis de las fallas en la seguridad, las protecciones actuales tomando en cuenta las seguridad de la información, le acceso no autorizado la destrucción, la revelación o deslealtad, Modificaciones.

Posteriormente se procede a realizar el plan de recuperación del desastre y respaldo de la información tomando en cuenta las actividades a realizarse previo al desastre en cuanto a establecimientos del plan de acción, Formación de equipos operativos. Las actividades durante el desastre que incluyen u plan de emergencias, formación de equipos, entrenamiento.

Las actividades después del desastre que son: evaluación de daños, priorización de las actividades del plan de acción, ejecución de las actividades, evaluación de resultados y retroalimentación del plan de acción. Se definen las acciones a tomar frente a cada tipo de riesgo (Maza Anton, 2009).

2.1.6. Diseño de las políticas de seguridad de la información y desarrollo del plan de contingencia para el área de sistemas de la Cooperativa de Ahorro y Crédito Alianza del Valle – 2005

El Plan de Contingencias implica un análisis detallado y minucioso de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que se realiza el análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema. Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se puede presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener bien definidas las políticas de seguridad de la información y un Plan de Contingencias lo más completo posible. Para llevar a cabo la elaboración de las políticas de seguridad de la información se seguirá las siguientes actividades:

Evaluación a fondo de las vulnerabilidades, amenazas y riesgos.

Recopilación de material de apoyo

Definir un marco de referencia

Redactar la documentación

A continuación se muestran las principales actividades requeridas para el desarrollo del Plan de Contingencia:

Análisis de Riesgos

Actividades previas al desastre

Actividades durante el desastre

Actividades después del desastre

Distribución y mantenimiento del plan

El objetivo general es Diseñar las políticas de seguridad de la información y Desarrollar el Plan de Contingencia para el Área de Sistemas de la Cooperativa de Ahorro y Crédito Alianza del Valle.

Sus objetivos específicos son:

- Analizar y realizar un estudio de la situación actual de las instalaciones informáticas de la COAC. Alianza del Valle.

- Identificar, analizar los riesgos y sus respectivos impactos que podrían ocasionar la paralización de las operaciones del área de sistemas de la COAC. Alianza del Valle.
- Diseñar políticas de seguridad de información siguiendo los lineamientos propuestos por COBIT y por la metodología a utilizarse en este plan.
- Desarrollar el Plan de Contingencias.

Este trabajo consta de dos partes la primera es un Diseño de las políticas de seguridad de la información para lo cual se realiza un análisis de riesgos y amenazas contra la seguridad considerando la situación actual. La infraestructura física, el hardware, el software, base de datos, redes LAN, red, WAN, una vez analizados los riesgos se emiten las políticas de seguridad que se implementarán para prevenir posibles contingencias.

El plan de acción consta de las actividades previas al desastre o medidas de precaución, en las cuales se toma en cuenta la infraestructura física, el acceso físico al departamento de sistemas, instalaciones eléctricas, detectores de humo y alarmas, extintores de incendio, cableado estructurado, acceso al cuarto de servidores, hardware, software, Comunicaciones,

Luego el plan de acción que es general y contempla una pérdida total se consideran los software, información de base de datos, hardware, comunicaciones, cableado estructurado.

Las actividades durante el desastre o plan de emergencias considera: Vías de salida o escape, plan de evacuación del personal, un plan de puesta a buen recaudo de los activos de la institución, asignación de funciones al personal para saber qué hacer con los equipos y elementos evacuados, programa de prácticas y ensayos periódicos de emergencias.

Las actividades después del desastre toman en cuenta una evaluación de los daños, priorización de las acciones del plan de acción, evaluación de resultados, retroalimentación del plan de acción (Llumiquinga Marcillo & Vallejo, 2005).

2.1.7. Propuesta del plan de contingencia informático para la Universidad Técnica del Cotopaxi

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo, sistemas de información y datos contenidos en los diversos medios de almacenamiento. Con esto se pretende reducir la posibilidad de ocurrencia de riesgos y procedimientos a seguir en caso que se presente algún problema.

En el plan de contingencia se hace énfasis al aspecto físico y lógico, es donde se concentra el mayor número de inconvenientes; pero también es necesario establecer pruebas y verificaciones periódicas para que el plan de contingencia esté operativo y actualizado.

Las acciones que contemplan el plan de contingencia son: antes, durante y después, de manera que permita reducir: pérdidas financieras directas / indirectas, pérdidas de la operatividad de la U.T.C., pérdidas de usuarios finales, costos extras para apoyo, costo de compensación, pérdidas de la infraestructura tecnológica, pérdidas de sistemas de información, información errónea o incompleta, bases pobres para la toma de decisiones

Entre otras, que retardan o paralizan las actividades que normalmente desarrolla la institución, provocando pérdidas económicas, retraso en el proceso educativo por falta de infraestructura, lo que es más preocupante, la pérdida de información que es muy difícil de recuperar peor aún si son ocasionados por desastres naturales o atentados.

Es necesario enfatizar a los siguientes puntos del plan:

- Controles detectores de las bases para entender la importancia del plan.
- Obtener el consentimiento de los directivos.
- Definir los requerimientos de recuperación.

- Converger apropiadamente en la prevención de desastres.
- Integrar el plan de contingencia dentro de los planes generales de la organización.

Los objetivos planteados son:

- Concientizar al personal administrativo, docente y estudiantes que están sujetos a cualquier tipo de riesgos y que debemos estar preparados para actuar en forma rápida y oportuna minimizando todo tipo de desastre.
- Proporcionar una guía de contingencia flexible y adaptable a los requerimientos de la universidad.
- Establecer políticas de seguridad que abarquen el aspecto lógico y físico que permitan salvaguarda la integridad de la información e infraestructura.

  (Claudio & Chicaiza, 2003)

2.2. Definición de la línea base.

Una vez analizados los planes de contingencia anteriormente mencionados y comparar con la situación actual de Innovativa, para la realización de este proyecto se ha considerado lo siguiente:

- Al no contar con un plan de contingencias ni políticas de seguridad para el área de TI, se deberá iniciar implementando las medidas básicas de seguridad que se han pasado por alto.

- Para el análisis de riesgos se tomará como referencia la metodología utilizada para la elaboración del Plan de Contingencias de la Universidad de Piura, de la Municipalidad de Punta y de la Cooperativa de Ahorro y Crédito Alianza del Valle.
- Se tomarán en cuenta todos los controles de prevención, mitigación y recuperación que se recomiendan en estos planes y se los adaptará para su implementación en Innovativa.

2.3. Marco teórico

2.3.1. Plan de Contingencia

Un Plan de Contingencia es un conjunto de procedimientos alternativos a la operativa normal de cada empresa, cuya finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la empresa.

Las causas pueden ser variadas y pasan por un problema informático, un fallo en la correcta circulación de información o la falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones.

La orientación principal de un plan de contingencia es la continuidad de las operaciones de la empresa, no sólo de sus sistemas de información. Su elaboración la

podemos dividir en Cinco etapas: Evaluación, Planificación, Pruebas de viabilidad, Ejecución, Recuperación.

Las tres primeras hacen referencia al componente preventivo y las últimas a la ejecución del plan una vez ocurrido el siniestro.

EVALUACIÓN:

1. Constitución del grupo de desarrollo del plan.- Este grupo debe estar liderado por un responsable del plan y formado por los líderes de las áreas que se desean cubrir con dicho plan. Su elaboración ha de desarrollarse con la continua supervisión por parte de la dirección ya que durante la elaboración y/o ejecución de éste, deberán comprometerse recursos y aprobarse procedimientos especiales que requieran un nivel de autorización superior.

2. Identificación de las funciones críticas.- Esta subfase consiste en identificar aquellos elementos de nuestra empresa o funciones que puedan ser críticos ante cualquier eventualidad o desastre y jerarquizarlos por orden de importancia dentro de la organización.

3. Definición y documentación de los posibles escenarios con los que podemos encontrarnos para cada elemento o función crítica. -Puede tratarse de problemas en el hardware, software de base, de telecomunicaciones, software de aplicación propio o

provisto por terceros, etc. También deben incluirse en esta categoría los siniestros provocados por incendios, una utilización indebida de medios magnéticos de resguardo o back up o cualquier otro daño de origen físico que pudiera provocar la pérdida masiva de información. También incluimos en este apartado todos aquellos problemas asociados con la carencia de fuentes de energía y de telecomunicaciones.

4. Análisis del impacto del desastre en cada función crítica.- Consiste en realizar un análisis del impacto de cada problema sobre cada una de las funciones críticas de la organización, teniendo en cuenta las siguientes prioridades:

- Evitar pérdidas de vida.
- Satisfacer las necesidades básicas.
- Reanudar las operaciones lo antes posible.
- Proteger el medio ambiente.
- Lograr las conexiones con los principales clientes y proveedores.
- Mantener la confianza en la empresa.
- Una correcta cuantificación del impacto económico de cada problema ayudará a una correcta selección de la solución alternativa.

5. Definición de los niveles mínimos de servicio.- Se trata de definir los mínimos niveles de servicio aceptables para cada problema que se pueda plantear. Es

importante que dicho nivel se consensue con cada uno de los responsables de las áreas que puedan verse afectadas.

6. Identificación de las alternativas de solución.-En esta subfase deberán identificarse las soluciones alternativas para cada uno de los problemas previsibles. Para ello se puede considerar: Implementar procesos manuales, Contratar las tareas críticas con terceros, Diferir la tarea crítica por un tiempo determinado, Otra medida que permita continuar las operaciones.

7. Evaluación de la relación coste/beneficio de cada alternativa.- De cada alternativa identificada en el punto anterior y sobre la base del impacto económico de cada problema, deberá determinarse la mejor solución desde el punto de vista coste/beneficio para cada proceso crítico y su tiempo de elaboración con un nivel de servicio que satisfaga el nivel mínimo.

PLANIFICACIÓN:

1. Documentación del plan de contingencia.- Es necesario documentar el plan, cuyo contenido mínimo será:

-Objetivo del plan.

-Modo de ejecución.

-Tiempo de duración.

-Costes estimados.

-Recursos necesarios.

-Evento a partir del cual se pondrá en marcha el plan.

-Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

2. Validación del plan de contingencia.- Es necesario que el plan sea validado por los responsables de las áreas involucradas. De igual manera hay que tener en cuenta las posibles consecuencias jurídicas que pudiesen derivarse de las actuaciones contempladas en él.

PRUEBAS DE VIABILIDAD:

1. Definir y documentar las pruebas del plan.- Es necesario definir las pruebas del plan y el personal y recursos necesarios para su realización. Una correcta documentación ayudará a la hora de realizar las pruebas.

2. Obtener los recursos necesarios para las pruebas.- Deben obtenerse los recursos para las pruebas, ya sean recursos físicos o mano de obra para realizarlas.

3. Ejecutar las pruebas y documentarlas.- Consiste en realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles. La capacitación del equipo de contingencia y su

participación en pruebas son fundamentales para poner en evidencia posibles carencias del plan y es necesario documentar las pruebas para su aprobación por parte de las áreas implicadas.

4. Actualizar el plan de contingencia de acuerdo a los resultados obtenidos en las pruebas.- Será necesario realimentar el plan de acuerdo a los resultados obtenidos en las pruebas, teniendo en cuenta que el plan de contingencia general o de continuidad de operaciones de la empresa contiene los planes de contingencia específicos para cada problema definido. Los distintos planes deben integrarse en un todo, considerando las posibles relaciones mutuas.

EJECUCIÓN:

En esta fase hay que tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

RECUPERACIÓN:

Los datos afectados por el siniestro que pudiesen haber quedado desactualizados o corruptos, deben corregirse usando los procedimientos ya definidos. En general, la reiniciación del proceso normal no implica la cancelación del alternativo, salvo que deban utilizarse los mismos recursos. Si esto no es así, durante cierto tiempo, los procesos deberían ejecutarse en paralelo para asegurar que la reiniciación de la operación normal es correcta y, ante cualquier defecto, continuar con el de contingencia.

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante futuras nuevas eventualidades. (Paz, 2010)

2.3.2. NFPA 10 Norma Extintores contra incendios

Las estipulaciones de esta norma se dirigen a la selección, instalación, inspección, mantenimiento y prueba de equipos de extinción portátiles. Los requisitos dados aquí son los mínimos. Los extintores portátiles son una línea primaria de defensa para combatir incendios de tamaño limitado. Son necesarios aun cuando la propiedad está equipada con regaderas automáticas, red hidráulica y mangueras u otros equipos fijos de protección

2.3.3. NFPA 75 Norma para la protección de equipos de Tecnología de la Información.

El propósito de la NFPA 75 (Norma para la Protección de Equipos de Tecnología de la Información) es el de establecer los requisitos mínimos para la protección del equipamiento de Tecnología de la Información y de las áreas para los equipos de tecnología de la información, de los daños ocasionados por el fuego o por sus efectos asociados, es decir, humo, corrosión, calor y agua.

2.3.4. Los Objetivos de Control para la Información y la Tecnología Relacionada (Cobit)

Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados. Estas empresas también entienden y administran los riesgos asociados, tales como aumento en requerimientos obligatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

Las organizaciones deben satisfacer la calidad y seguridad de su información, asi como de todos sus activos. . Las buenas prácticas de Cobit ayudarán a optimizar las inversiones, asegurarán la entrega del servicio.

Cobit brinda un marco de trabajo que garantiza que:

TI están alineada con el negocio

TI habilita al negocio y maximiza los beneficio

Los recursos de TI se usan de manera responsable

Los riesgos de TI se administran apropiadamente

Cobit define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Cobit define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son:

Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar, los cuales contienen treinta y cuatro procesos genéricos que se detallan a continuación.

Planear y Organizar

PO1 Definir un Plan Estratégico de Tecnología de Información

PO2 Definir la Arquitectura de Información

PO3 Determinar la dirección tecnológica

PO4 Definir la Organización y de las Relaciones de TI

PO5 Manejar la Inversión en Tecnología de Información

PO6 Comunicar la dirección y aspiraciones de la gerencia

PO7 Administrar Recursos Humanos

PO8 Asegurar el Cumplimiento de Requerimientos Externos

PO9 Evaluar Riesgos

PO10 Administrar proyectos

PO11 Administrar Calidad

Adquirir e Implementar

AI1 Identificar Soluciones

AI2 Adquirir y Mantener Software de Aplicación

AI3 Adquirir y Mantener Arquitectura de Tecnología

AI4 Desarrollar y Mantener Procedimientos relacionados con TI

AI5 Instalar y Acreditar Sistemas

AI6 Administrar Cambios

Entregar y Dar Soporte

DS1 Definir Niveles de Servicio

DS2 Administrar Servicios prestados por Terceros

DS3 Administrar Desempeño y Capacidad

DS4 Asegurar Servicio Continuo

DS5 Garantizar la Seguridad de Sistemas

DS6 Identificar y Asignar Costos

DS7 Educar y Entrenar a los Usuarios

DS8 Apoyar y Asistir a los Clientes de TI

DS9 Administrar la Configuración

DS10 Administrar Problemas e Incidentes

DS11 Administrar Datos

DS12 Administrar Instalaciones

DS13 Administrar Operaciones

Monitorear y Evaluar

M1 Monitorear los procesos

M2 Evaluar lo adecuado del control Interno

M3 Obtener aseguramiento independiente

M4 Proporcionar auditoría independiente

Cobit define objetivos de control para cada uno de estos procesos, así como para el proceso general y los controles de aplicación. Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos del negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. (IT Governance Institute, 2007)

2.3.5. ISO 17799

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. Define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Integridad. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.

Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. (Villaón Huerta, 2004)

La norma ISO 17799 recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un Sistema de Gestión de la Seguridad de la Información.

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
- Redactada de forma flexible e independiente de cualquier solución de seguridad concreta
- Proporciona buenas prácticas neutrales con respecto a tecnologías o fabricantes específicos.
- Aplicable a todo tipo de organizaciones, con independencia de su tamaño u orientación de negocios

La norma ISO 17799:2005 establece once dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad: Dirigir y dar soporte a la Gestión de la seguridad de la información -directrices y recomendaciones.
2. Aspectos organizativos de la seguridad: Gestión dentro de la Organización (recursos, activos, tercerización, etc.)
3. Clasificación y control de activos: Inventario y nivel de protección de los activos.
4. Seguridad ligada al personal: Reducir riesgos de errores humanos, robos, fraudes o mal uso de los recursos
5. Seguridad física y del entorno: Evitar accesos no autorizados, violación, daños o perturbaciones a las instalaciones y a los datos
6. Gestión de comunicaciones y operaciones: Asegurar la operación correcta y segura de los recursos de tratamiento de información
7. Control de accesos: Evitar accesos no autorizados a los sistemas de información (de usuarios, computadores, redes, etc.).
8. Desarrollo y mantenimiento de sistemas: Asegurar que la seguridad está incorporada dentro de los sistemas de información. Evitar pérdidas, modificaciones, mal uso.
9. Gestión de incidentes: Gestionar los incidentes que afectan la seguridad de la información

10. Gestión de continuidad del negocio: Reaccionar a la interrupción de las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres.
11. Conformidad con la legislación: Evitar el incumplimiento de leyes, regulaciones, obligaciones y de otros requerimientos de Seguridad.

De estos once dominios se derivan los Objetivos de control, resultados que se esperan alcanzar mediante la implementación de controles, que son las prácticas, procedimientos y/o mecanismos que reducen el nivel de riesgo. (Yory, 2006)

CAPÍTULO III

3. Metodología y Técnicas de investigación

El Método de Investigación que se utilizará para realizar este proyecto es el Cualitativo, un método que se caracteriza por explorar los fenómenos en profundidad conduce básicamente en ambientes naturales, no se fundamente en la estadística. Además es un proceso Inductivo, analiza múltiples realidades subjetivas y no tiene una secuencia lineal. (Hernandez, Fernández, & Baptista, 2010)

Las técnicas que se utilizarán son la Observación que consiste en observar minuciosamente un fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis. La Entrevista que consiste en el diálogo entre dos personas, se realiza con el fin de obtener información de una persona entendida en la materia de la investigación. (Huamán Valencia, 2005). Las sesiones de profundidad o grupos de enfoque que consisten en reuniones con grupos pequeños o medianos (de 3 a 10 personas), en las cuales las personas conversan en torno a uno o varios temas en un ambiente relajado e informal. (Hernandez, Fernández, & Baptista, 2010)

Además como el tema será enfocado a una Empresa será visto como un estudio de caso, el cual informa sobre un proyecto, innovación o acontecimiento durante un período prolongado de tiempo contando la evolución de un relato o historia (McKernam, J. 1989:96). Para su desarrollo, el estudio de caso considera tres

momentos importantes: observar, recuperar la información y registrarla y Comprender el fenómeno.

La observación: Es la fase básica del estudio de caso. Cohen, L. y Manion, L. (1999), distinguen dos tipos de investigación de estudios de casos empleando técnicas de observación, estos son: participante y no participante; en el primer tipo el investigador se integra al grupo en estudio; mientras que en la segunda posibilidad el investigador actúa como un espectador, con una visión desde el exterior con respecto al caso. En la actualidad los estudios de caso por observación de participación directa han cobrado gran importancia tanto en la educación como en las ciencias fácticas.

Recuperar la información y registrarla. Esta fase depende en gran medida de las técnicas de recolección de datos tales como cuestionarios, entrevistas, notas de las observaciones físicas del investigador, por mencionar algunos... Es importante señalar la relevancia que reviste el cifrado cualitativo, que hace posible la utilización de documentos en forma sistemática (Goode & Hatt, 1977)

Comprender el fenómeno. Para llegar a la explicación del fenómeno hay que comprenderlo en su contexto. La información es analizada, destacando dos propósitos: f Formar modelos a partir de la información obtenida, el investigador analiza la información obtenida, comprende e informa haciendo una representación

de la situación y buscar modelos que dan significado al estudio. Aquí el investigador realiza comparaciones de los datos obtenidos con la finalidad de buscar rasgos, situaciones que se repiten, distinguiendo sus características para formar nuevos modelos con tendencia a lo que Stake, R. (1999) llama generalización naturalista.

Las características son las partes distintivas de cualquier objeto. A continuación se presentan, tomadas de diversos autores, algunas de estas que refieren al Estudio de Caso.

1. El investigador descubre hechos o procesos que pueden pasar por alto si utilizan otros métodos.
2. Permite al investigador adoptar técnicas que sirvan a la tarea de distribuir, en lugar de imponerlas impidiendo dicha tarea.
3. Se enfoca hacia un solo objeto de estudio, lo que permite un análisis intenso y una abundancia de datos detallados.
4. No prueban hipótesis, pero en cambio, sugieren líneas de investigación subsecuentes.
5. Revela una diversidad y riqueza de conducta humana que sencillamente no está accesible por ningún otro método.
6. No presenta un plan de muestreo
7. La observación es parte fundamental en la obtención de la información.
8. Es rico en descripciones, interpretaciones, explicaciones y narraciones, trabajando más para la comprensión que para la medición, la predicción y el

control científico riguroso de los entornos, las personas estudiadas, las acciones.(Mackernan, 1989). y otros aspectos.

9. No es posible establecer relaciones causa-efecto. El estudio de caso no basa su trabajo en el control de variables; sin embargo una vez finalizado el estudio su producto de trabajo puede dejar en claro que el sistema analizado presenta una situación de causa y efecto, y puede ser tomado como puntos de partida de investigaciones posteriores.
10. Informa sobre la innovación o acontecimiento durante un tiempo prolongado.
11. Está orientado al proceso más que al producto.
12. Busca una comprensión holística del objeto de estudio
13. Los investigadores no se enfocan en el conocimiento de una verdad universal.
14. No se dirige ordinariamente al trabajo de investigación, sino hacia la comprensión de un problema personal.
15. No permite la generalización. Aunque Stake, considera que es posible una generalización naturalista, es decir, aquella que es solo debe ser válida para la población que se ha estudiado, pero no debe extrapolarse (Stake, 1999).
16. Utiliza la triangulación para evitar al máximo falsas percepciones y error en las conclusiones (Stake, 1999).
17. Su redacción es menos erudita y formal y más parecido al discurso periodístico o crítico literario. (Monroy Cornejo, 2009)

CAPÍTULO IV

4. Elaboración del Plan de Contingencia para Área de Tecnologías de la Información de Innovativa

4.1. Importancia del plan de contingencias

En una empresa todos los equipos informáticos y de telecomunicaciones se encuentran expuestos a riesgos provenientes de diversos factores tanto humanos, físicos o desastres naturales, que podrían impedir el funcionamiento normal de los procesos, y además pérdida de información valiosa e importante, para poder reaccionar de manera eficaz y eficiente ante cualquier emergencia es importante contar con un plan de contingencias que es un conjunto de procedimientos alternativos cuya finalidad es la de permitir continuar con las operaciones de la empresa y garantizar la integridad de los activos físicos, lógicos y sobre todo el personal considerando las acciones que deben tomarse antes, durante y después del siniestro.

En el caso de Innovativa, el contar con el permanente servicio de internet, el mantener sus aplicaciones funcionando permanentemente y contar con procedimientos de respaldo eficientes y seguros es imprescindible para brindar un buen servicio a sus clientes, por lo cual estos puntos serán considerados en el plan de contingencias.

4.2. Alcance

Considerando que es el primer plan de contingencias informático a ser implementado en el Área de TI de Innovativa y que no existen políticas de seguridad definidas se enfatizará en que se cumplan con las normas mínimas de seguridad y control para proteger tanto al personal, los bienes y la información.

4.3. Objetivos

- Garantizar la continuidad de las operaciones de Innovativa.
- Definir los controles de prevención, mitigación y recuperación destinados a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

4.4. Análisis de riesgos

El análisis del riesgo está basado en la información de la situación actual de Innovativa y el Área de TI, obtenida en el proyecto de "Estudio de Factibilidad para la elaboración del Plan de Contingencias del Área de Tecnologías de la Información de CTT-ESPE-CECAI INNOVATIVA Sede Sangolquí". La misma servirá para la toma de decisiones.

En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: el tipo, la probabilidad y

grado de impacto del riesgo.. Estos elementos permitirán categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

Los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte, hora y negocio. Los tipos de contingencias se han clasificado en tres grupos:

- Naturales: causados por fenómenos de la naturaleza tales como mal tiempo, terremotos, etc.
- Tecnológicas: causados por fallas en las instalaciones o equipos tales como incendios eléctricos, fallas de energía y fallas en las comunicaciones, perdidas de información.
- Sociales: causados por los seres humanos como actos terroristas, sabotajes y errores.

4.5. Bienes susceptibles a daños

Los bienes que podrían ser afectados son: personal, hardware, software y utilitarios, datos e información, documentación, suministro de energía eléctrica, suministro de telecomunicaciones. Las contingencias que pueden producirse son:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, provocado por causas naturales o humanas.

- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- Pérdida, alteración, divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico.

4.6. Identificación de riesgos

Se considera un riesgo o amenaza a todo evento que pueda ocurrir y tenga la capacidad e afectar en forma negativa las instalaciones, procesos y actividades de Innovativa.

4.6.1. Incendios

Pueden producir grandes pérdidas no solo materiales si no también humanas, puede ser generado por una negligencia del personal, una falla en algún equipo eléctrico o electrónico también por la falta de seguridad en las conexiones eléctricas.

4.6.2. Sismos

La ubicación geográfica cercana al volcán Cotopaxi hace que se deba considerar este riesgo ya que pondría en peligro al personal y a todos los activos que Innovativa posee.

4.6.3. Falla en la conexión de red

Parte de la red de comunicaciones se encuentra integrada por equipos como switches, módems, etc. El daño o la inoperatividad de algunos de estos componentes pueden impedir el acceso de los equipos a los servicios y aplicaciones que brinda la red como internet, correo electrónico, aplicaciones en línea, transferencia de archivos.

Puede ser ocasionada por fallas de hardware, configuración y/o software que impiden el acceso a servicios como internet, correo electrónico, aplicaciones en línea como son ESIGEF e INCOP, transferencia de archivos.

4.6.4. Inundaciones

No existe mayor riesgo de que ocurra en las instalaciones, pero si se llegara a producir una inundación, los daños serian cuantiosos. Puede suceder por descuido del personal y debido a la proximidad de los servicios higiénicos a las oficinas como muestra la figura 1, si el agua toma contacto con aparatos como regletas, reguladores

de voltaje, etc. podrían causar un corto circuito causando daños totales o parciales en los equipos y posiblemente perdida de información.

4.6.5. Inoperatividad de los Servidores

Existen aplicaciones que se encuentran instaladas y almacenan sus datos en el Servidor como por ejemplo Eset empoit security , Olympo, ATRIB , Lince, Nómina, al existir algún daño no se podrá acceder a su información impidiendo el desarrollo normal de las actividades y una prestación de servicios eficiente.

4.6.6. Inconvenientes eléctricos.

La falla en el sistema eléctrico impide el uso de aparatos eléctricos y electrónicos, lo cual dificulta la prestación de servicios y además puede causar daños reparables e irreparables a los mismos.

4.6.7. Pérdida de Información

La pérdida de información generaría graves consecuencias para Innovativa, esta se podría dar por daño en los equipos y/o medios de almacenamiento físico, por cortes de energía eléctrica, por errores involuntarios, o pérdida de documentación por parte de los usuarios.

4.6.8. Acción de virus informático

Los virus informáticos pueden causar graves daños a los sistemas operativos y a la información almacenada en los equipos, los mismos que pueden infiltrarse a través del correo electrónico, navegación por internet, a través del uso de memoras USB, discos externos u otro dispositivo de almacenamiento infectado.

4.6.9. Alteración de la información

Puede producirse por un control deficiente del acceso de los usuarios a las aplicaciones, por falta de experticia en el manejo de la aplicación por parte del usuario.

4.6.10. Robo común de equipos y archivos

Actualmente el acceso a las instalaciones se encuentra restringido a una tarjeta magnética y el ingreso al Centro de Datos se lo asegura por medio de un candado y un teclado de acceso, una violación de estas seguridades podría provocar la pérdida de los bienes de la empresa y de información.

4.6.11. Robo de información y datos

La incursión de hackers o personal insatisfecho a las aplicaciones puede implicar la manipulación y sustracción de información que puede utilizarse de forma mal intencionada, lo cual traería graves consecuencias para la institución.

4.6.12. Ausencia parcial o permanente del Personal de tecnología de la Información

Esta contingencia debe ser considerada ya que actualmente las funciones de TI recaen en dos personas, es decir que cuentan con poco personal.

Se puede dar por motivos de enfermedad, calamidad doméstica, renuncia, etc. y si no se cuenta con otra persona con el conocimiento necesario y capacitado para realizar las actividades pueden suscitarse problemas como suspensión de servicios y falta de acceso a la información.

4.7. Probabilidad del riesgo

Es la probabilidad de que una condición se produzca realmente, la tabla 1 muestra la clasificación que se la ha dado para la elaboración de este plan.

Tabla 1: Probabilidad del riesgo

Probabilidad de ocurrencia	Descripción
Muy Frecuente	Incidentes repetidos
Frecuente	Incidentes aislados
Poco Frecuente	Sucede alguna vez
Remota	Poco probable que suceda

4.8. Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia. La tabla 2 indica los tipos de impacto considerados para este plan de contingencias.

Tabla 2: Impacto del riesgo

Impacto	Descripción
Muy Severo	Pérdida de información crítica, daño serio, patrimonial
Grave	Pérdida de información sensible, retraso o interrupción, pérdida patrimonial
Moderado	Pérdida de información sensible, pérdida patrimonial
Leve	Pérdida de información y/o equipamiento no sensitivo.

4.9. Matriz de riesgos

La tabla 3 indica el tipo de riesgo, la probabilidad de su ocurrencia y el grado de impacto de cada uno de los riesgos.

Tabla 3: Matriz de riesgos

Riesgo	Tipo de riesgo	Probabilidad de ocurrencia	Grado de impacto
Incendios	Tecnológicos	Remota	Muy Severo
Sismos	Naturales	Remota	Muy Severo
Inundaciones	Sociales	Aleatoria	Grave
Fallas en la conexión de red	Tecnológicos	Poco Frecuente	Moderado
Inoperatividad de los Servidores	Tecnológicos	Poco Frecuente	Moderado
Inconvenientes eléctricos.	Tecnológicos	Frecuente	Moderado
Pérdida de Información	Tecnológicos	Poco Frecuente	Grave
Acción de virus informático	Sociales	Poco Frecuente	Grave
Alteración de la información	Sociales	Poco Frecuente	Grave
Robo común de equipos y archivos	Sociales	Remota	Grave
Robo de información y datos	Sociales	Poco Frecuente	Grave
Ausencia del Personal de TI	Sociales	Poco Frecuente	Moderado

4.10. Controles de prevención

Se ha enfatizado en los controles de prevención, debido a que estos permitirán evitar que se produzcan las contingencias y en caso de producirse Innovativa estará mejor preparada para afrontarlas, La tabla 4 muestra los controles que se deben ir implementando.

Tabla 4: Controles de prevención

Nº	Control de prevención	Responsable
1	Definir un sitio alternativo para el funcionamiento de la empresa en caso de que sus instalaciones se vean afectadas, que se conocerá como el Centro de Operaciones de Emergencia, se recomienda llenar un formato con los datos del sitio para que sea de fácil contacto ver Anexo1.	Director Ejecutivo
2	Establecer un sistema de vigilancia mediante cámaras de seguridad, el cual registre todos los movimientos de entrada y salida del personal.	Especialista en Sistemas
3	Instalar identificadores mediante tarjetas de acceso que permitan identificar al personal que ingresa.	Especialista en Sistemas
4	Portar siempre el carnet de identificación que se entrega a cada empleado de Innovativa.	Subdirector Administrativo
5	Administrar el ambiente físico (mantenimiento, monitoreo y reportes incluidos) Cobit DS12	Subdirector Administrativo
6	Definir e implementar procesos para mantenimiento y autorización de acceso físico a las instalaciones de Innovativa Cobit DS12, ISO 17799 9.1.2	Subdirector Administrativo
7	Diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión física, disturbios civiles y otras formas de desastre natural o creado por el hombre ISO 17799 9.1.4	Subdirector Administrativo
8	Verificar periódicamente las condiciones de los equipos de seguridad instalados en Innovativa.	Especialista en Sistemas
9	Elaborar, socializar y realizar simulacros de un plan de evacuación, deben acogerse al Plan de Emergencia del campus Matriz-Sangolquí de la ESPE.	Subdirector Administrativo
10	Reportar de inmediato si se detecta cualquier anomalía en los equipos de seguridad y en las instalaciones eléctricas.	Todo el personal
11	Rotular las vías de evacuación.	Subdirector Administrativo
12	Proporcionar las facilidades (equipos, procedimientos y técnicas) para realizar copias de respaldo.	Especialista en Sistemas

Puede obtener estas normas aquí:
Cobit : http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
ISO/IEC17799 : https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Continua ⟶

13	Realizar respaldos que permanezcan dentro de las instalaciones de Innovativa se recomienda llenar un formato de control de la realización de cada respaldo ver Anexo 2.	Especialista en Sistemas
14	Tener respaldos de la información en un sitio remoto, se recomienda llenar una ficha con los datos del sitio en donde reposarán los respaldos ver Anexo 3 y Anexo 8.	Especialista en Sistemas
15	Realizar pruebas periódicas de los respaldos de la información, verificando su funcionalidad ver Anexo 4.	Especialista en Sistemas
16	Revisar que las normas y procedimientos con respecto a respaldos, seguridad de equipos y datos se cumpla.	Especialista en Sistemas
17	Tener a la mano elementos de iluminación.	Subdirector Administrativo
18	Tener a la mano los números telefónicos de emergencia de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.	Subdirector Administrativo
19	Instalar una fuente alternativa de energía como un UPS.	Especialista en Sistemas
20	Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.	Especialista en Sistemas
21	Ubicar los servidores en un Data Center que cumpla con estándares de seguridad.	Especialista en Sistemas
22	Revisar el desempeño y la capacidad actual de los recursos de TI Cobit DS3.	Especialista en Sistemas
23	Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI (Cobit DS3).	Especialista en Sistemas
24	Realizar pronósticos de desempeño y capacidad de los recursos de TI Cobit DS3.	Especialista en Sistemas
25	Monitorear y reportar continuamente la disponibilidad, el desempeño y la capacidad de los recursos de TI (Cobit DS3).	Especialista en Sistemas

Puede obtener estas normas aquí:
Cobit : http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
ISO/IEC17799 : https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Continua ⟶

26	Realizar un análisis de la brecha para identificar incompatibilidad de los recursos de TI Cobit DS3.	Especialista en Sistemas
27	Identificar los responsables de cada uno de los equipos eléctricos y electrónicos ver Anexo 5.	Especialista en Sistemas
28	Contratar un seguro para los equipos de computación el cual permita recuperar los equipos aplicando la garantía, en el caso de presentarse algún desastre.	Subdirector Administrativo
29	Contar con un stock de los cables, equipos eléctricos y electrónicos indispensables para que puedan reemplazar a los averiados.	Especialista en Sistemas
30	Delegar personal del Departamento de TI que se encargue del manejo de todo Software (oficina, desarrollo, mantenimiento, drives, de su instalación en las PC's con su respectivo software corporativo.	Especialista en Sistemas
31	Mantener los manuales del software en un lugar accesible para el personal del departamento de sistemas.	Especialista en Sistemas
32	Desarrollar procedimientos de planeación de administración de la configuración Cobit DS9	Especialista en Sistemas
33	Recopilar información sobre la configuración inicial y establecer líneas base Cobit DS9	Especialista en Sistemas
34	Verificar y auditar la información de la configuración (incluye la detección de software no autorizado) Cobit DS9	Especialista en Sistemas
35	Actualizar el repositorio de la configuración Cobit DS9	Especialista en Sistemas
36	Identificar dueños de sistemas y de datos Cobit PO4 ver Anexo 6	Especialista en Sistemas
37	Definir, establecer y operar un proceso de administración de identidad (cuentas) Cobit DS5, ISO 17799 11.2.1	Especialista en Sistemas
38	Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios Cobit DS5, ISO 17799 11.2.4	Especialista en Sistemas
39	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica.	Especialista en Sistemas

Puede obtener estas normas aquí:
Cobit : http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
ISO/IEC17799 : https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Continua ⟶

40	Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves ISO 17799 11.3.1.	Especialista en Sistemas
42	Definir, mantener e implementar procedimientos para restauración de datos Cobit DS11	Especialista en Sistemas
43	Generar políticas que regulen el uso y acceso del Servicio de Internet.	Especialista en Sistemas
44	Llevar un registro electrónico de Altas/Bajas de Usuarios, con sus permisos	Especialista en Sistemas
45	Informar al Departamento de Tecnologías y Comunicaciones de renuncias, despidos, reemplazos del personal para su registro y accesos a la red y los sistemas	Subdirector Administrativo
46	Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas del Departamento de Tecnología y Comunicaciones	Especialista en Sistemas
47	Elaborar una agenda de direcciones, teléfonos y direcciones electrónicas de los proveedores y mantenerla en una parte visible ver Anexo 7.	Especialista en Sistemas
48	Extraer diariamente un logístico sobre el volumen de correo transportado.	Especialista en Sistemas
49	Extraer diariamente un logístico sobre las conexiones de red.	Especialista en Sistemas
50	Adquirir las licencias para el correcto funcionamiento del software en los equipos.	Especialista en Sistemas
51	Definir, mantener e implementar procedimientos para desechar de forma segura, medios y equipos Cobit DS9	Especialista en Sistemas
52	Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red Cobit DS5	Especialista en Sistemas
53	Definir y documentar los procesos de administración del proveedor Cobit DS2	Especialista en Sistemas
54	Monitorear la prestación del servicio del proveedor Cobit DS2	Especialista en Sistemas

Puede obtener estas normas aquí:
Cobit : http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
ISO/IEC17799 : https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Continua ⟶

55	Desarrollar documentación de soporte técnico para operaciones y personal de soporte Cobit AI4	Especialista en Sistemas
41	Probar que las claves son de buena calidad sometiéndolos a pruebas que garanticen su resistencia a un ataque diccionario	Especialista en Sistemas
57	Mantener actualizado del inventario de los equipos eléctricos y electrónicos	Especialista en Sistemas
58	Mantener la temperatura adecuada en el Data Center	Especialista en Sistemas
59	Desarrollar un plan para el mantenimiento de las aplicaciones de software Cobit AI2	Especialista en Sistemas
60	Utilizar métodos de autenticación para controlar el acceso de usuarios remotos ISO 17799 11.4.2.	Especialista en Sistemas
61	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración. ISO 17799 11.4.4	Especialista en Sistemas
62	Realizar evaluaciones de vulnerabilidad de manera regular Cobit DS5	Especialista en Sistemas
63	Identificar y Categorizar las necesidades de capacitación de los usuarios Cobit DS7	Especialista en Sistemas Subdirector Administrativo
64	Construir un programa de capacitación Cobit DS7	Subdirector Administrativo
65	Realizar actividades de capacitación, intrusión y concienciación Cobit DS7	Especialista en Sistemas Subdirector Administrativo
66	Llevar a Cabo evaluaciones de la capacitación Cobit DS7	Especialista en Sistemas Subdirector Administrativo

Puede obtener estas normas aquí:
Cobit : http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
ISO/IEC17799 : https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Continua ⟶

67	Identificar y evaluar los mejores métodos y herramientas para impartir la capacitación (Cobit DS7)	Especialista en Sistemas Subdirector Administrativo
68	Desarrollar manuales de procedimiento del usuario final Cobit AI4	Especialista en Sistemas
70	Verificar periódicamente que las tuberías de agua estén en perfecto estado.	Subdirector Administrativo
71	Ubicar los servidores a un promedio de 50 cm de altura.	Especialista en Sistemas
72	Instalar los tomacorrientes a un nivel razonable de altura.	Especialista en Sistemas
73	Documentar la estructura de la red.	Especialista en Sistemas
74	Realizar un mantenimiento preventivo de las instalaciones eléctricas cada seis meses.	Especialista en Sistemas
75	Elaborar un mapa de diseño del cableado eléctrico	Especialista en Sistemas
76	No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.	Especialista en Sistemas
77	Instalar un antivirus en todos los equipos.	Especialista en Sistemas
78	Monitorear los reportes del Antivirus	Especialista en Sistemas
79	Revisar que los medios de almacenamiento que se hayan prestado no estén contagiados con virus.	Especialista en Sistemas
80	Aplicar filtros para restricción de correo entrante, revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.	Especialista en Sistemas

Puede obtener estas normas aquí:
Cobit : http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
ISO/IEC17799 : https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Continua ⟶

81	Estar actualizado sobre los diferentes tipos de virus existentes en el medio, sus características, síntomas en si la descripción del virus a propagarse.	Especialista en Sistemas
82	Centralizar en una sola aplicación todas las tareas de instalación, actualización y configuración del antivirus en cada punto de la red	Especialista en Sistemas
83	Colocar detectores de humo	Subdirector Administrativo
84	Colocar extintores de fuego en las instalaciones, basándose en la norma NPFA 10 de Extintores Portátiles contra incendios.	Subdirector Administrativo
85	Capacitar al personal en el uso de extintores de incendios	Subdirector Administrativo
86	No concentrar grandes cantidades de papel	Todos los usuarios
87	No arrojar las colillas de cigarrillos a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.	Todos los usuarios
88	No almacenar sustancias y productos inflamables.	Todos los usuarios
89	Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.	Todos los usuarios
90	Identificar la ubicación de las estaciones manuales de alarma contra incendio.	Todos los usuarios
91	Identificar la ubicación de los extintores.	Todos los usuarios
92	Resguardar la documentación en archivadores que tengan las debidas seguridades.	Todos los usuarios
93	Colocar un sello de seguridad en el CPU para que no sea abierto por personal no autorizado.	Especialista en Sistemas
94	Destruir los reportes malogrados, sobre todo de contenido relevante.	Todos los usuarios
95	Eliminación de quemadores de CD y bloqueo de puertos USB, etc. en estaciones de trabajo que no lo requieran.	Especialista en Sistemas

4.11. Controles de mitigación

La tabla 5 muestra los controles de mitigación deberán ser aplicados en caso de suscitarse la contingencia.

Tabla 5: Controles de mitigación

Nº	Control de mitigación	Responsable
1	Comunicar al personal responsable de activar la contingencia.	Director Ejecutivo
2	Si es necesario, poner en marcha el plan de evacuación.	Director Ejecutivo
3	Se deberá (si el tiempo lo permite) apagar los computadores, los servidores y equipos electrónicos.	Todos los usuarios
4	Verificar que todo el personal se encuentre bien.	Subdirector Administrativo
5	De ser necesario llamar a los organismos de socorro.	Subdirección Administrativa
6	En caso de daños del personal prestar asistencia médica inmediata	Subdirección Administrativa
7	Si es posible el encargado de los respaldos deberá ponerlos a buen recaudo.	Especialista en Sistemas
8	Si las instalaciones no pueden ser usadas, realizar el trámite para mudarse al centro de operaciones de emergencia.	Director Ejecutivo
9	Si los equipos indispensables están dañados reponerlos para poder iniciar las operaciones lo más pronto posible.	Especialista en Sistemas
10	Denunciar el robo a las autoridades pertinentes.	Subdirector Administrativo
11	Presentar las evidencias que se tengan y colaborar con las autoridades en la investigación.	Subdirector Administrativo
12	Tener cuidado de que los cables entren en contacto con el agua, mantenerse alejado de esos sitios.	Todos los usuarios
13	Desconectar la electricidad cuidando la integridad.	Especialista en Sistemas

Continua ⟶

14	Rescatar todos los equipos que se pueda.	Todos los usuarios
15	Ejecutar proceso para detectar falla en la conexión de red ver Anexo 11.	Especialista en Sistemas
16	Realizar un inventario de lo sustraído.	Subdirector Administrativo
17	Revisar las políticas de seguridad.	Subdirector Administrativo
18	Desconectar la estación infectada de la red.	Especialista en Sistemas
19	Entregar al usuario un equipo de reemplazo hasta que se solucione el problema.	Especialista en Sistemas
20	Verificar que no existan más estaciones de trabajo infectadas.	Especialista en Sistemas
21	Alertar al cuerpo de bomberos de la situación.	Subdirección Administrativa
22	Los empleados designados con anterioridad para la utilización de extinguidores pondrán en marcha su responsabilidad en ese momento.	Subdirector Administrativo
23	Si no se puede salir, mantenerse al ras del piso, cubrir tu boca y nariz con un pañuelo bien mojado y respira a través de él,	Todos los usuarios
24	Abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.	Todos los usuarios
25	Si es posible mojar la ropa.	Todos los usuarios
26	Verificar si las puertas están calientes antes de abrirlas, si lo están, buscar otra salida.	Todos los usuarios
27	Si se le encienden las ropas, no corra, tiéndase en el suelo y échese a rodar.	Todos los usuarios
28	El UPS entrará en funcionamiento por un espacio de 20 min.	Especialista en Sistemas
29	Respaldar en el disco duro la información que se haya generado hasta ese momento	Todos los usuarios
30	Respaldar en otro medio de almacenamiento los documentos importantes.	Todos los usuarios

Continua ⟶

31	En el uso de sistemas en línea dejar de hacer transacciones.	Todos los usuarios
32	Si el corte es por un daño en las instalaciones reportar al técnico correspondiente para que proceda a reparar el daño.	Especialista en Sistemas
33	Pedir a los técnicos de la ESPE que se suministre energía a través de la planta eléctrica para no cortar las operaciones.	Especialista en Sistemas
34	Mientras dure el sismo o terremoto, manténgase alejado de objetos que puedan caer.	Todos los usuarios
35	Ubicarse junto a un mueble resistente como un escritorio, en caso contrario localizar una esquina o columna de hormigón que ofrezca seguridad.	Todos los usuarios
36	Terminado el sismo o terremoto salir de las instalaciones.	Todos los usuarios
37	El personal que este mejor preparado debe hacer uso de los manuales y documentación existente para poder solucionar los problemas más urgentes que se susciten.	Director General
38	Suspender el ingreso de personas que no trabajen en la institución	Director General
39	Brindar acceso remoto al personal de TI para que pueda brindar servicios desde otro lugar	Especialista en Sistemas

4.12. Controles de Recuperación

Los Controles de Recuperación se muestran en la tabla 6, son los que permitirán reanudar las operaciones normales y la buena prestación de servicios de Innovativa, luego de haber sucedido la contingencia.

Tabla 6: Controles de Recuperación

Nº	Control de Recuperación	Responsable
1	Evaluación de los daños ocasionados sobre las instalaciones	Subdirector Administrativo
2	Limpieza de las áreas afectadas.	
3	Ejecutar proceso para identificar bienes afectados ver Anexo 9.	Subdirector Administrativo
4	Tramitar la garantía de los equipos sustraídos o dañados o comprar los equipos indispensables para la continuidad de las operaciones	Subdirector Administrativo Especialista en Sistemas
5	Ejecutar proceso para restitución o reparación de bienes afectados ver Anexo 10	Subdirector Administrativo Especialista en Sistemas
6	Ejecutar proceso para control de virus informático ver Anexo 12	Especialista en Sistemas
7	Revisar la infraestructura del edificio para evitar que vuelva a ocurrir una nueva filtración de agua.	Subdirector Administrativo
8	Identificar si el daño es interno o externo, en el caso de ser interno el técnico realizará el cambio y/o reparación de las instalaciones afectadas y verificará cada uno de los puntos eléctricos y sus conexiones. En el caso de ser externo El responsable de sistemas deberá comprobar el correcto funcionamiento delos servidores, de los computadores de cada departamento y de la conexión de la red.	Especialista en Sistemas
9	Sistemas de Proveedores.- De producirse una falla al momento de la operación de estos sistemas por efecto del programa ejecutable (cliente) o base de datos, deberá ser comunicado y coordinado inmediatamente con el proveedor, para su corrección. Sistemas de Innovativa.- De producirse una falla al momento de la operación de estos sistemas, el Jefe de Informática asumirá, delegará o coordinará los trabajos de corrección o modificación.	Especialista en Sistemas
10	Ejecutar proceso para restaurar servidores ver Anexo 13.	Especialista en Sistemas
11	Efectuar las pruebas necesarias con el usuario.	Especialista en Sistemas

4.13. Plan de Contingencias

En las tablas 4,5 y 6 se ha definido los diferentes tipos de controles y se les ha designado un código, a continuación para cada riesgo identificado, se ha procedido a definir los diferentes controles a implementar.

4.13.1. Incendios

Activos	Controles de prevención	Controles de mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	7,16,28,29,50,57	3,9,14	3,4,5
Servidores	7,21	3,9,14	3,4,5
Software	13,14,15,16		
Información	12,13,14,15,16,42	7	
Personal	4,9,27,63,64,65,66,67,85,86,87,89,90,91	1,2,4,5,6,21,22,23,24,25,26,27	11,12
Instalaciones	1,2,5,6,7,10,11,18,83,84,88	8,13	1,2

4.13.2. Sismos

Activos	Controles de prevención	Controles de mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,29,50,57	3,9,14	3,4
Servidores	21	3,9,14	3,4
Software	13,14,15,16		
Información	12,13,14,15,16	7	
Personal	4,9,27,63,64,65,66,67	1,2,4,5,6,34,35,36	11,12
Instalaciones	1,5,11,17,18	8,13	1,2

4.13.3. Inundaciones

Activos	Controles de prevención	Controles de mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,29,50,57	3,9,14	3,4,5
Servidores	21,71	3,9,14	3,4,5
Software	13,14,15,16	31	3
Información	12,13,14,15,16,42	7,29,30	
Personal	4,9,27,63,64,65,66,67	1, 2,4,5,6	11,12
Instalaciones	1,5,10,11,18,69,70,72	8,12,13	1,2,7

4.13.4. Falla en la conexión de red

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,29,32,33,34,35,56 ,61,62	9	3,4,5
Servidores	21,32,33,34,35,61,62	9	3,4,5
Software	13,14,15,16,33,34	31	
Información	12,13,14,15,16,49	29,30	
Personal	27,30,36,43,47,55,60,63 ,64,65,66,67	1	11,12
Instalaciones	1,5,10	15	

4.13.5. Inoperatividad de los Servidores

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,29,32,33,34,35,56,61,62	9	
Servidores	21,22,23,24,25,26,32,33,34,35,61,62	9	5
Software	13,14,15,16,30,33,34,35	31	3,9,10
Información	12,13,14,15,16,42	29,30	11,12
Personal	27,30,31,36,43,47,55,60,63,64,65,66,67	1	
Instalaciones	1,5,10,58	8	

4.13.6. Inconvenientes eléctricos.

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,19,20,28,29,50	3,9,28	3,4,5
Servidores	21	3	3,4,5
Software	13,14,15,16	31	3
Información	12,13,14,15,16	29,30	
Personal	27,47,63,64,65,66,67	1,32,33	11,12
Instalaciones	1,5,10,74,75,76	13	1,2,8

4.13.7. Pérdida de Información

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,56		
Servidores	21		3
Software	13,14,15,16		3
Información	12,13,14,15,16,41,42		
Personal	3,4,27,30,31,36,37,38,39,40,43,45,46,60,63,64,65,66,67	1	11,12
Instalaciones	2,5,6,10		

4.13.8. Acción de virus informático

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,32,33,34,35,61,62	9,18,19,20	6
Servidores	21,32,33,34,35,61,62	9	6
Software	13,14,15,16,33,34,35,77,80,82		3,6
Información	12,13,14,15,16,42,48,52		6
Personal	27,31,36,37,38,43,45,55,60,63,64,65,66,67,78,79,81	1	11,12
Instalaciones	5		

4.13.9. Alteración de la información

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,32,33,34,35,61,62		
Servidores	21,32,33,34,35,61,62		
Software	13,14,15,16,33,34,35		
Información	12,13,14,15,16,41,42		
Personal	3,4,27,30,31,36,37,38,39,40,43,44,45,46,55,60,63,64,65,66,67,68	1	11, 12
Instalaciones	2,5,6		

4.13.10. Robo común de equipos y archivos

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,29,57,93	9,16,19	3,4,5
Servidores	21	9,16	3,4,5
Software	13,14,15,16		
Información	12,13,14,15,16		
Personal	3,4,27,36,45	1,10,11,17	11,12
Instalaciones	1,2,5,6,8,10,92		1,2

4.13.11. Robo de información y datos

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,61,62,95		
Servidores	21,61,62		
Software	13,14,15,16	16	
Información	12,13,14,15,16,41,42,48	16	
Personal	3,4,27,31,36,37,38,39,40,43,44,45,55,60,94	1,10,11,17	11,12
Instalaciones	2,5,6,8,10	38	1,2

4.13.12. Ausencia parcial o permanente del Personal de tecnología de la Información

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	32,33		
Servidores	32,33		
Software			
Información	12,47		
Personal	27,31,36,45,46,55,63,64,65,66,67	1,37	
Instalaciones		39	11,12

4.14. Pruebas o ensayos

La realización de las pruebas tiene como objetivos:

- Incrementar la conciencia y el conocimiento del plan
- Validar, actualizar y corregir el plan para que se adapte a las necesidades y cumpla con los requerimientos.
- Entrenar al personal con el propósito de minimizar el tiempo de respuesta y de recuperación ante una contingencia.
- Verificar la disponibilidad de los datos y recursos críticos almacenados fuera de las instalaciones de Innovativa.
- Comunicar de manera formal a las autoridades pertinentes de los resultados de los ensayos y proponer mejoras.

Se recomienda realizar pruebas de los planes de evacuación, que se deberán coordinar con la Universidad de las fuerzas Armadas – ESPE y tener un informe sobre las mismas para asegurarse que en caso de una contingencia el personal este bien capacitado y conozca los sitios seguros.

El Jefe del Área de TI, deberá proponer un plan anual para la realización de ensayos para ser aprobado y ejecutado.

En esta planificación se deben tomar en cuenta todos los riesgos considerados en el Plan de Contingencias y gestionar el presupuesto correspondiente de ser necesario.

La ejecución de cada prueba deberá ser documentada en el formato recomendado en el Anexo 14.

4.15. Anexos

Anexo 1

Ubicación del Centro de Operaciones de Emergencia

Lugar			
Ubicación			
Dirección			
Teléfonos			
Contacto	**E-mail**	**Teléf. convencional**	**Teléf. celular**
Responsable:		**Fecha:**	

Anexo 2

Control de respaldo de datos

Fecha	Hora	Nombre Respaldo	Medio de almacenamiento	Información Respaldada	Responsable

Anexo 3

Sitio alterno de respaldo de datos

Lugar			
Ubicación			
Dirección			
Teléfonos			
Responsable de realizar los respaldos			
Responsable de almacenar los respaldos			
Frecuencia con la que se realizan los respaldos			
Contacto	**E-mail**	**Teléf. convencional**	**Teléf. celular**
Responsable:		**Fecha:**	

Anexo 4

Control de funcionamiento de los respaldos de la información

Fecha	Hora	Nombre respaldo	Fecha respaldo	Medio de almacenamiento	Información respaldada	Responsable

Anexo 5

Designación Usuarios de los Equipos

Nº	Responsable	Cargo	Ubicación física	Código del equipo	Fecha asignación	Fecha entrega

Anexo 6

Dueños de los sistemas y las bases de datos

Nº	Responsable	Cargo	Ubicación física	Nombre del sistema o base de datos	Fecha asignación	Fecha entrega

Anexo 7

Información de proveedores

Empresa				
Servicios				
Teléf. empresa				
Fax empresa				
Dir. empresa				
e-mail empresa				
Contacto	**E-mail**	**Teléf. convencional**	**Teléf. celular**	**Observación**
Responsable:		**Fecha:**		

Anexo 8

Proceso para la realización de respaldos de la información

Respaldo de archivos de usuarios y correo electrónico

Responsable: Especialista en sistemas

Periodicidad: Semanal

Nº	Actividad	Almacenamiento	Ubicación
1	Toda la documentación de cada usuario se respalda diariamente y automáticamente utilizando el software Cobian Backup	disco en red	Data Center
2	Identificar los archivos a respaldar		
3	Generar una copia magnética	Cintas	
4	Etiquetar la Cinta como “Respaldo Usuarios ‘Fecha ‘”		
5	Verificar que se han copiado todos los archivos y que pueden ser utilizados para su restauración		
6	Si la copia no es buena realizar otra		
7	Llenar el formato para Control de Respaldo de Datos		
8	Almacenar la copia en el lugar destinado dentro de la institución y fuera de la institución		

Respaldo de las bases de datos

Responsable: Especialista en Sistemas

Periodicidad: Semanal

Nº	Actividad
1	Identificar los archivos a respaldar
2	Generar una copia magnética
3	Etiquetar la Cinta como “Respaldo BDD ‘Fecha ‘”
4	Verificar que se han copiado todos los archivos y que pueden ser utilizados para su restauración
6	Si la copia no es buena realizar otra
7	Llenar el formato para Control de Respaldo de Datos
8	Almacenar la copia en el lugar destinado dentro de la institución y fuera de la institución

Respaldo de los cursos de la plataforma Moodle

Responsable: Web Master

Periodicidad: Cada Semana

1. En el explorador de internet digitar la siguiente url: http://www.innovativa-virtual.edu.ec/campus1/ , aparecerá la pantalla que se muestra en la figura 1.

Figura 1: pantalla de ingreso

2. Ingresar el **Username, Passoword** y presionar el botón **Login,** aparecerá la pantalla mostrada en la figura 2, seleccionar el curso que se desea respaldar.

Figura 2: pantalla de selección de curso

3. En la pantalla que se muestra en la figura 3, seleccionar la opción **Copia de seguridad**

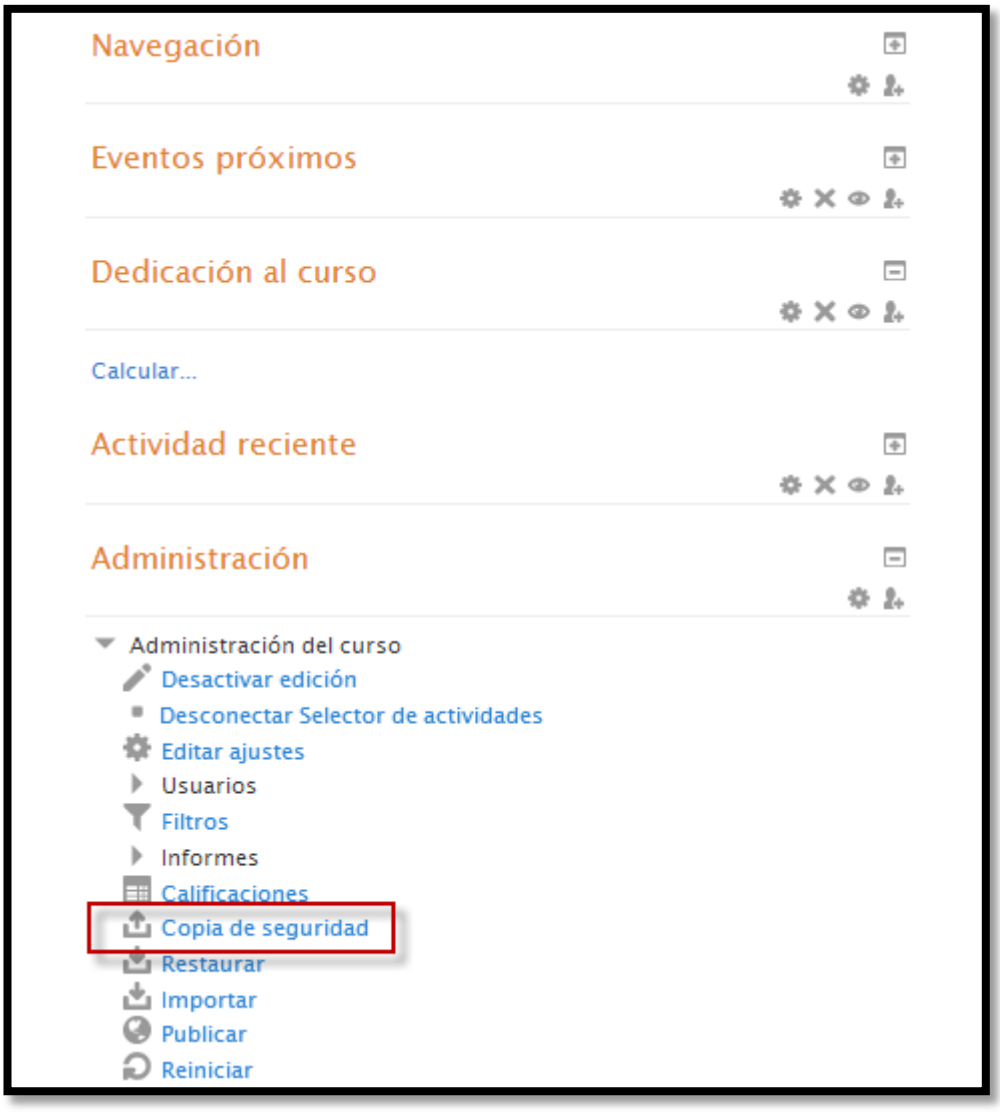


Figura 3: pantalla de copia de seguridad

4. En la nueva pantalla, seleccionar las opciones indicadas en la figura 4, y presionar el botón siguiente.

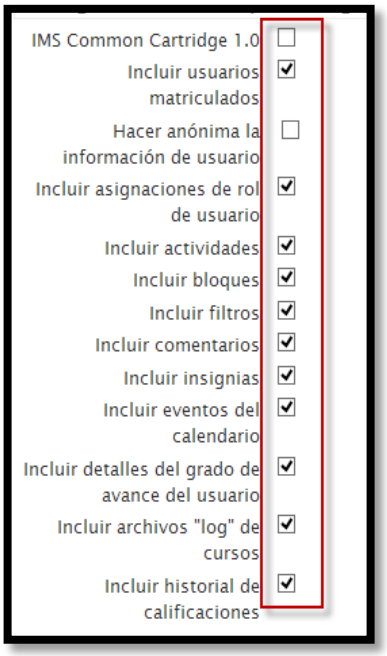


Figura 4: pantalla de configuración de la copia

5. En la pantalla mostrada en la figura 5, presionar el botón siguiente.

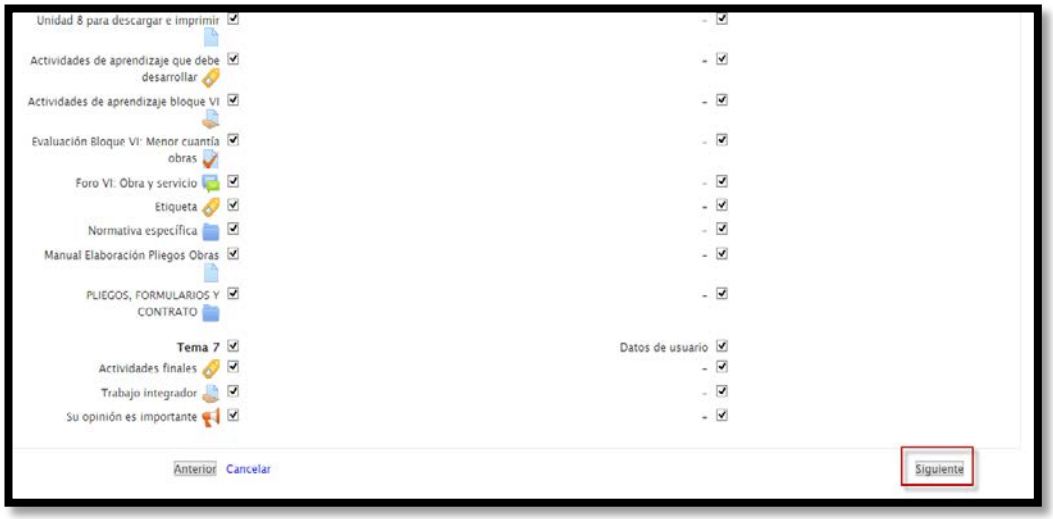
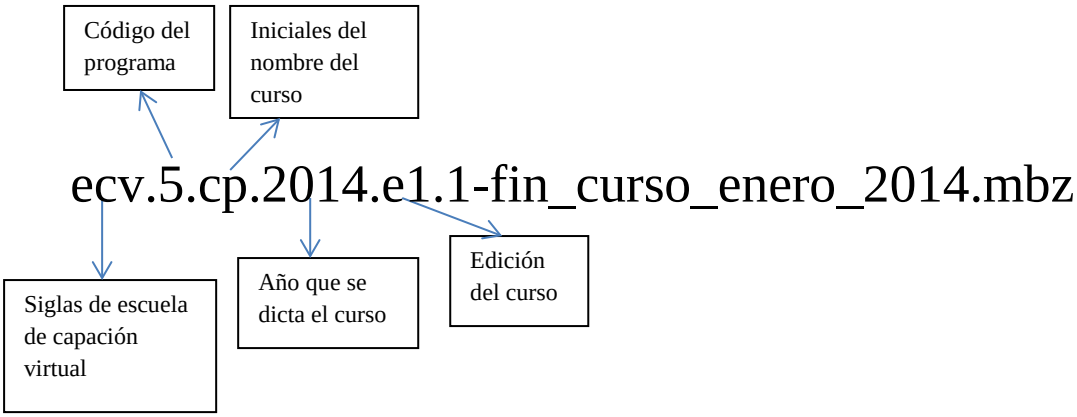


Figura 5: pantalla de confirmación de la copia de seguridad

6. En la pantalla que se muestra en la figura 6, escribir el nombre del archivo, con extensión mbz, el estándar para etiquetar los archivos de respaldo es:



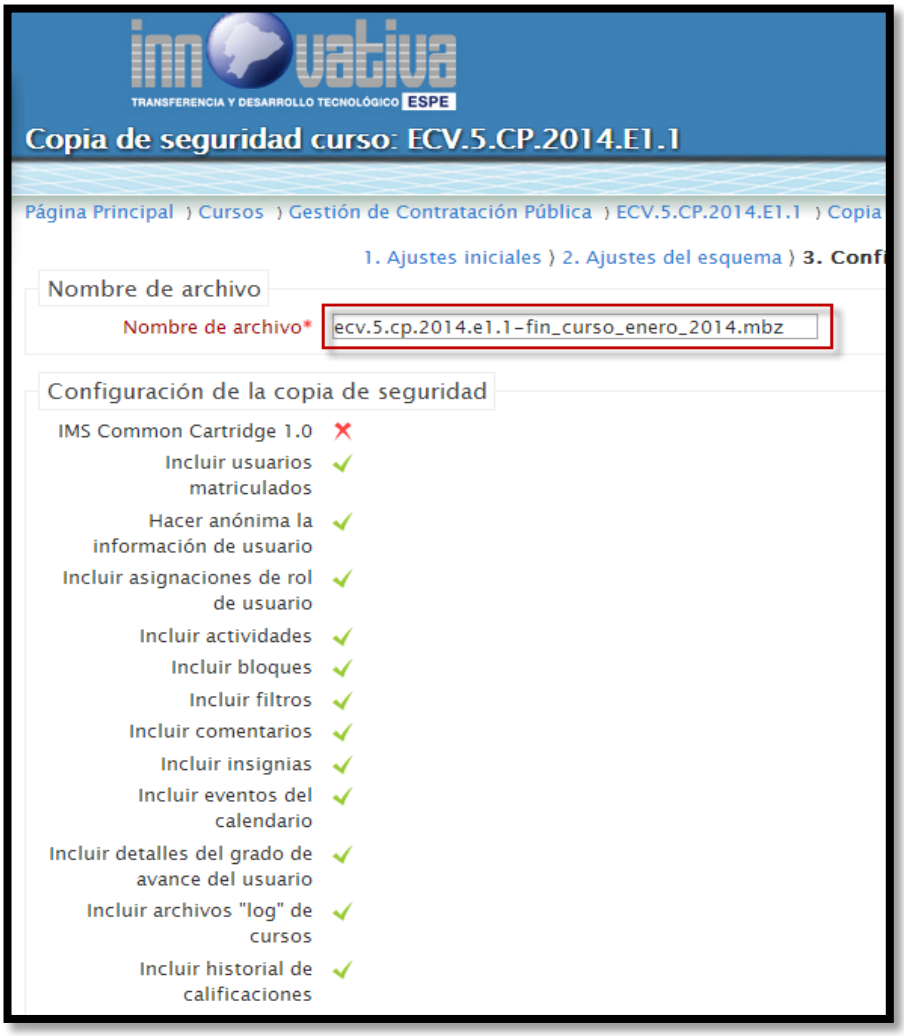


Figura 6: pantalla para asignar el nombre del respaldo

7. En la pantalla mostrada en la figura 7, presionar el botón **Ejecutar copia de seguridad**

Figura 7: pantalla para ejecutar la copia de seguridad

8. En la pantalla mostrada en la figura 8, se confirma que la copia de seguridad ha sido descargada con éxito, hacer clic en el botón **Continuar.**

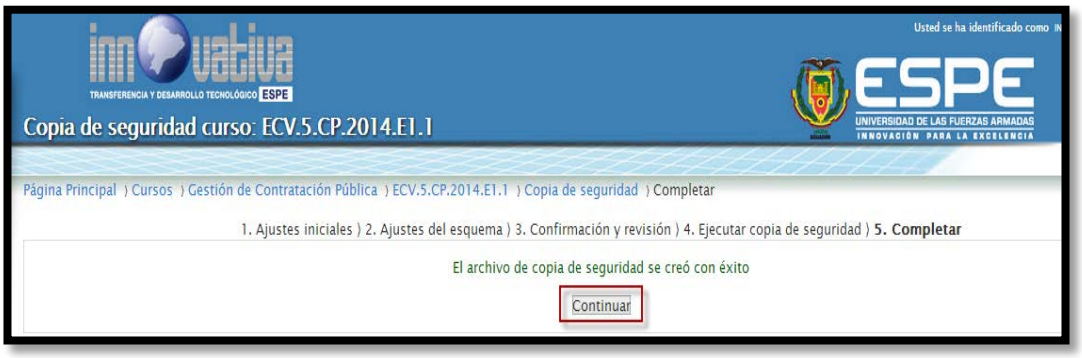


Figura 8: pantalla que confirma la realización de la copia

9. En la pantalla que se muestra en la figura 9, se procede a descargar la copia generada, para luego almacenarla en el disco duro externo.

Figura 9: pantalla para descargar la copia al disco duro

Anexo 9

Proceso para identificar los bienes informáticos afectados

Responsable: Especialista en Sistemas

Nº	Actividad
1	Realizar un análisis de los daños ocasionados en los equipos de computación como: servidores, computadores y equipos de la red y el software afectado.
2	Determinar de acuerdo a las condiciones del equipo de cómputo si la falla detectada requiere de la compra de partes o materiales o de su reemplazo.
3	Priorizar la necesidad de los equipos
4	Evaluar el funcionamiento de las aplicaciones y las bases de datos
5	Realizar un reporte de los equipos afectados por parte del Departamento de Tics en el formato correspondiente (anexo)

Anexo 10

Proceso para restitución o reparación de bienes informáticos afectados

Nº	Actividad	Responsable
1	Reportar el mal funcionamiento de los equipos	Usuario
2	Identificar los daños en cada estación de trabajo y equipo eléctrico o electrónico	Especialista en sistemas
3	Realizar un reporte de los equipos afectados por parte Departamento de Tics en el formato correspondiente (anexo)	Especialista en sistemas
4	Determinar de acuerdo a las condiciones del equipo de cómputo si la falla detectada requiere de la compra de partes o materiales o de su reemplazo.	Especialista en sistemas
5	Proceso administrativo de adquisiciones	Área Requirente
6	En caso de no requerir partes o materiales corrige fallas y verificar el funcionamiento óptimo del equipo	Especialista en sistemas
7	Recibir de Bodega las partes y/o materiales requeridos	Especialista en sistemas
8	Reparar el equipo de cómputo	
9	Verificar su funcionamiento adecuado.	Especialista en sistemas
10	Entregar al usuario y hacer firmar acta de satisfacción	Especialista en sistemas

Anexo 11

Proceso para detectar Falla en la conexión de red

Nº	Actividad	Responsable
1	Verificar el lugar físico donde se encuentra el dispositivo con fallas	Especialista en sistemas
2	Revisar a nivel de capa física las conexiones (Tarjeta de Red, patch cord, caja de pared)	Especialista en sistemas
3	Si la falla no se solventa con el paso 2, revisar las conexiones en el rack de comunicaciones.	Especialista en sistemas
4	Si la falla no se solventa con el paso 3, revisar las conexiones en nivel de capa de enlace, ejecutar comando como ping y tracert para verificar las conexiones.	Especialista en sistemas
5	Si la falla no se solventa con el paso 4, revisar las conexiones en las capas superiores del modelo OSI, es decir verificar aplicaciones que puedan producir el inconveniente	Especialista en sistemas
6	Registrar la solución que se ha dado	Especialista en sistemas

Anexo 12

Proceso para control de virus informático

Nº	Actividad	Responsable
1	Reportar al Departamento de sistemas el mal funcionamiento del equipo	Usuario
2	Rastrear el origen de la infección (archivo infectado, correo electrónico, etc.)	Especialista en sistemas
3	Eliminar el agente causante de la infección.	Especialista en sistemas
4	Remover el virus del sistema.	Especialista en sistemas
5	Probar el sistema.	Especialista en sistemas
6	En caso no solucionarse el problema formatear el equipo	Especialista en sistemas
7	Personalizar la estación para el usuario	Especialista en sistemas

Anexo 13

Proceso para restaurar Servidores

Respaldar y restaurar Servidores virtuales

En el caso de los servidores Innovativa, estos se encuentran virtualizados, a continuación se detalla el procedimiento para respaldar y restaurar servidores virtuales en VMWare.

1. Ejecutar la aplicación cliente VMWare vSphere Client, e ingresar el **User name y Password**, luego presionar el botón **Login,** como se observa en la figura 1.

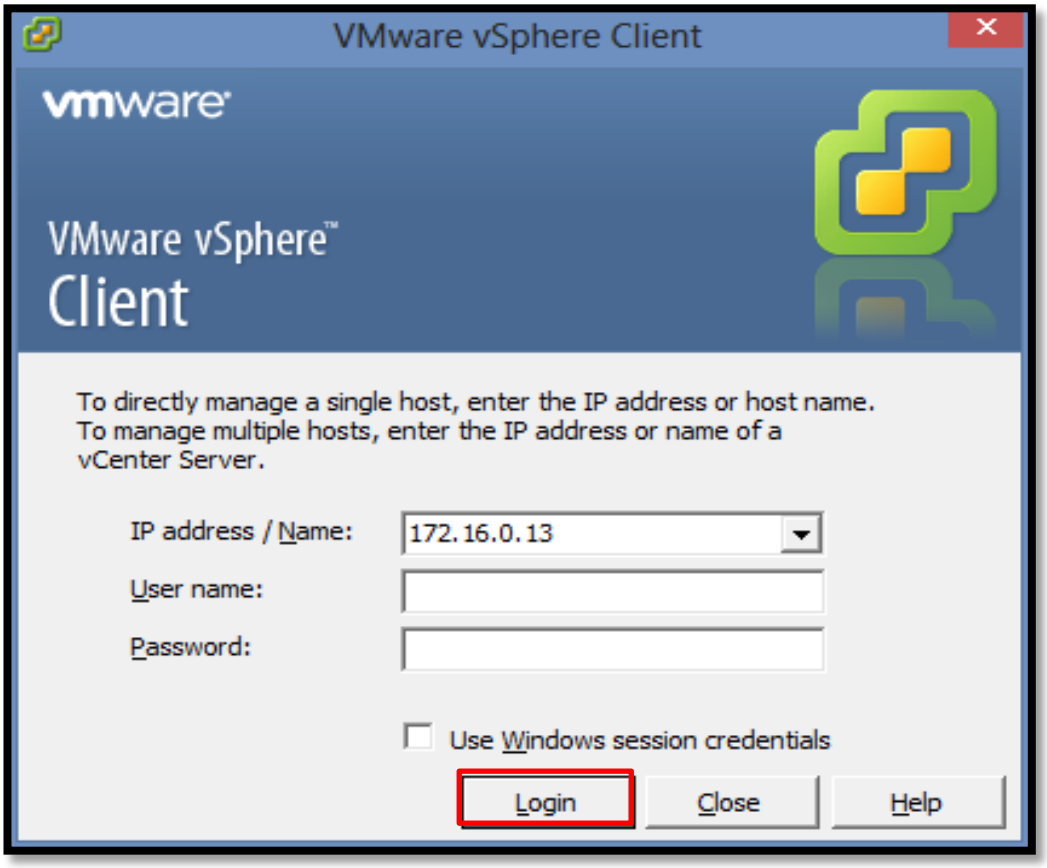


Figura 1: pantalla de ingreso

2. En la figura 2 se podrá visualizar el panel de control de la aplicación, en la parte izquierda podemos ver los diferentes servidores que se encuentran virtualizados. En la parte derecha nos aparece las diferentes funciones de la aplicación, ingresamos a la pestaña **Summary**.

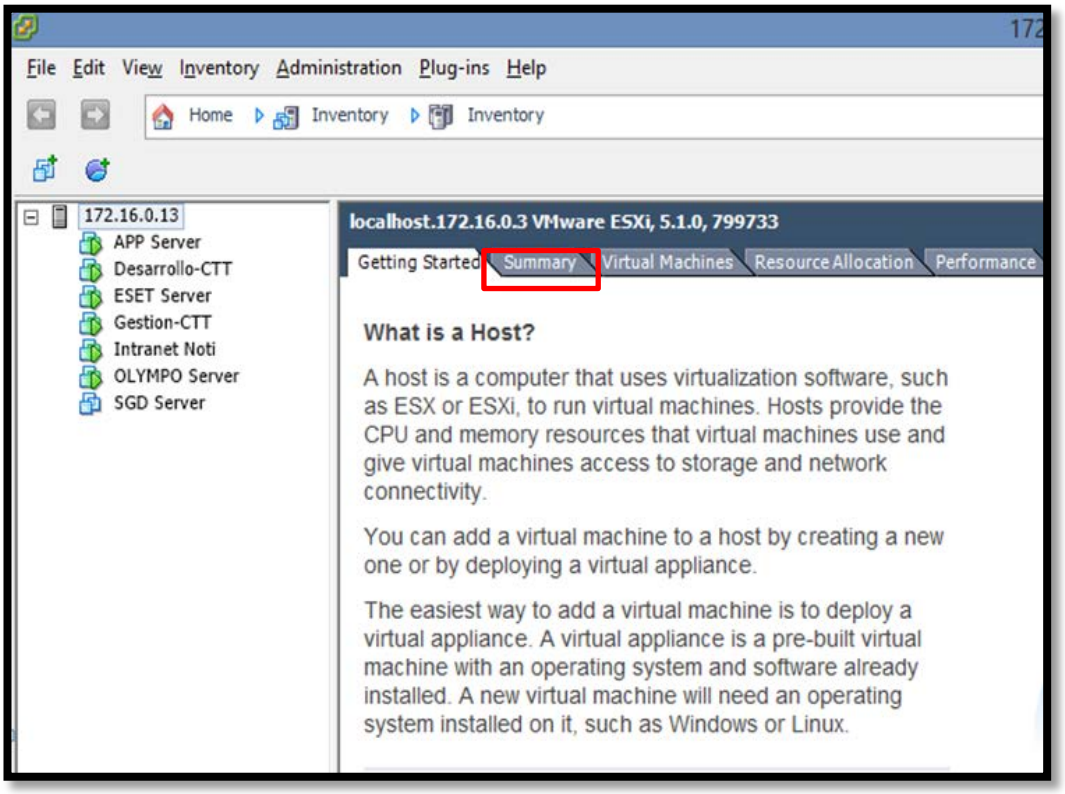


Figura 2: pantalla de funciones de la aplicación

3. En la figura 3 se puede observar la sección **Storage** que nos presenta los almacenamientos de datos que tenemos para utilizar con los servidores virtuales, seleccionamos uno de ellos y con clic derecho seleccionamos **Browse Datastore**.

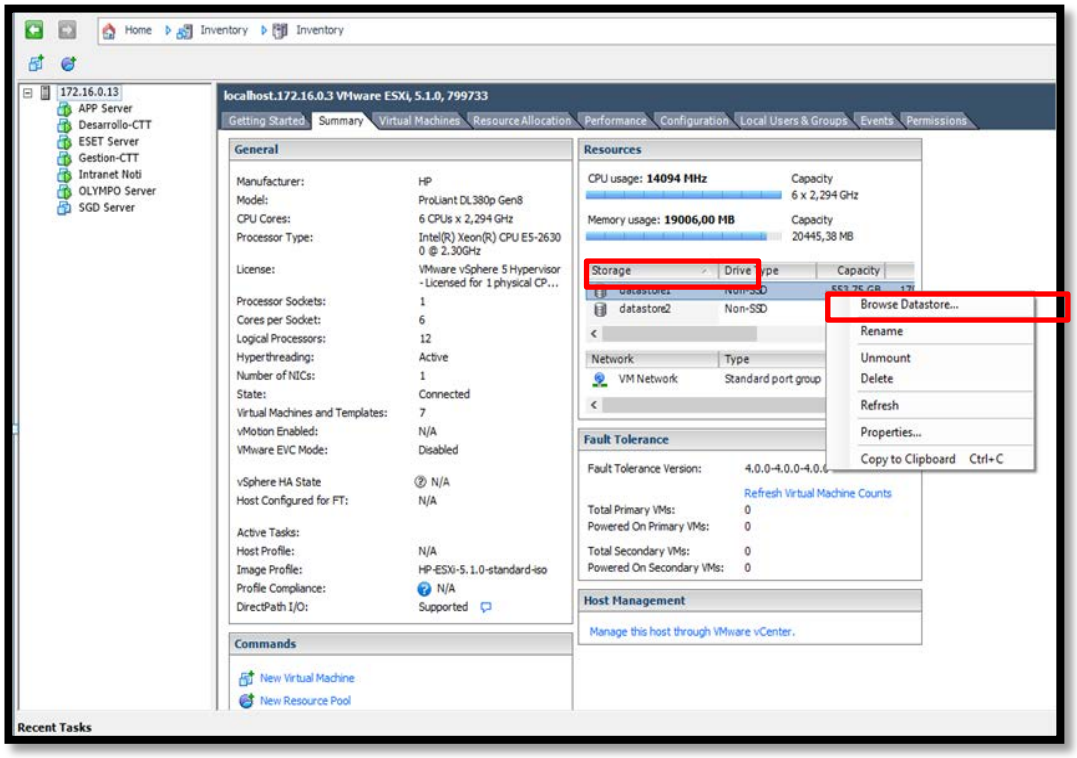


Figura 3: pantalla de respaldo de servidores virtuales

4. Aparecerá el contenido del **Datastore**, aquí se pueden visualizar los datos que contiene cada uno de los servidores virtuales.

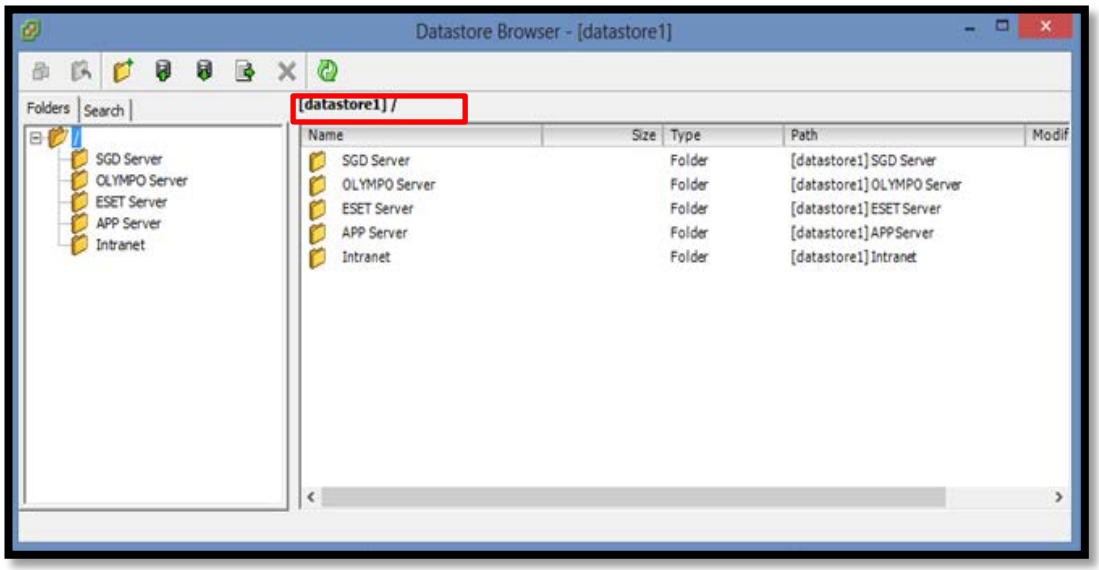


Figura 4: pantalla con los datos de los servidores virtuales

5. En el caso de requerir respaldar uno de los servidores virtuales, se deberá seleccionar la carpeta de este servidor y presionar la opción **Download a file from this datastore to your local machine**, con esta opción se procede a respaldar los datos del servidor virtual como muestra la figura 5.

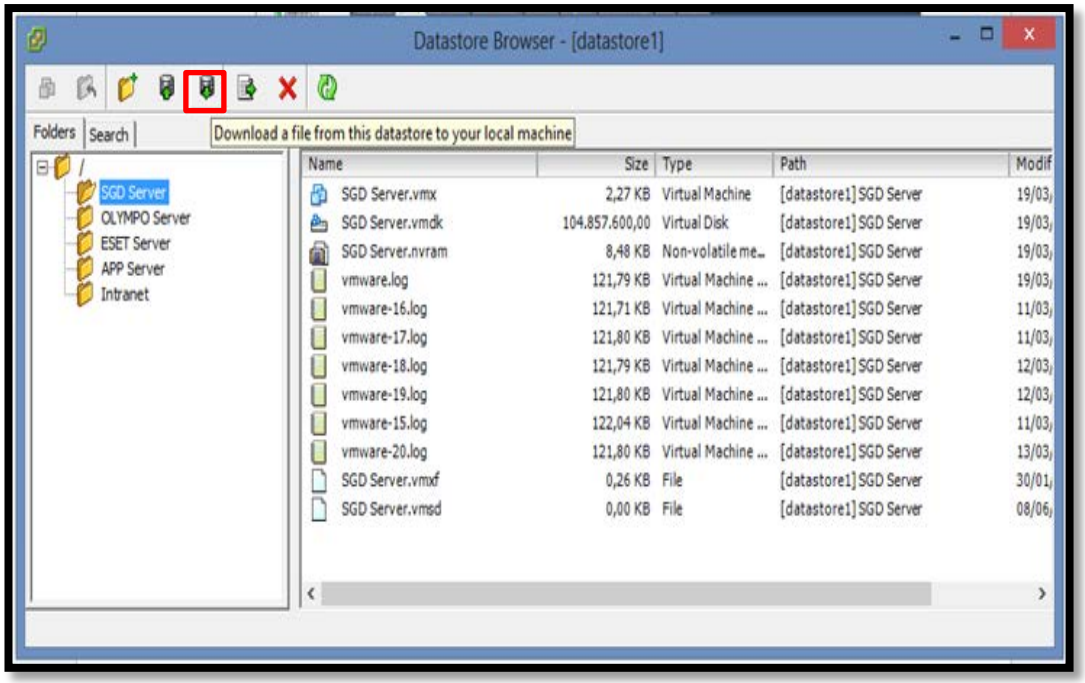


Figura 5: pantalla para descargar los datos

6. Seleccionar la carpeta donde se guardará el respaldo del servidor virtual y presionar el botón **Aceptar** como muestra la figura 6.

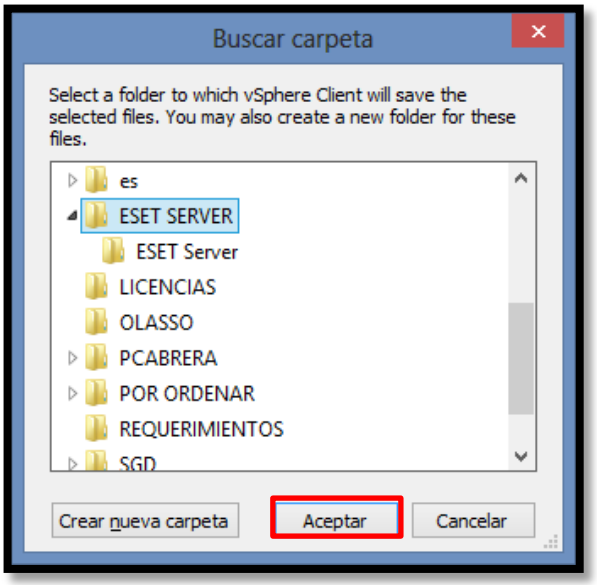


Figura 6: pantalla seleccionar el path donde se graba el respaldo

7. Para el caso de restauración de servidores, se debe repetir el paso 6 pero seleccionamos la opción **Upload files to this datastore,** como indica la figura 7.

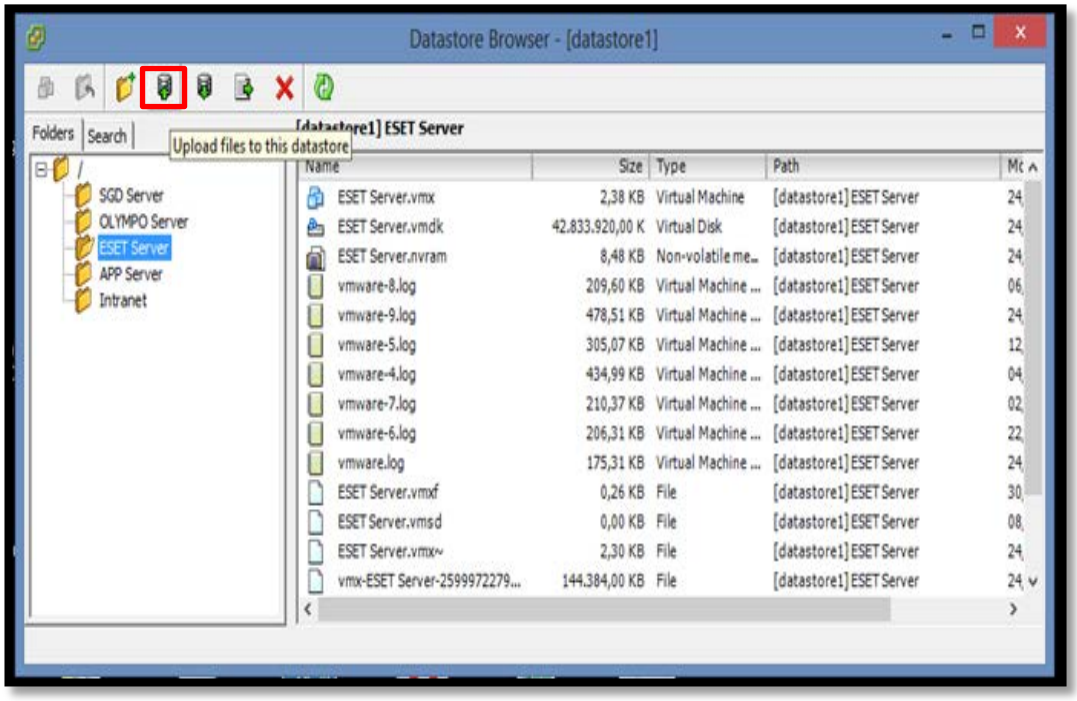


Figura 7: pantalla para restaurar los datos de un servidor

8. La figura 8 indica que para restaurar un servidor virtual, vamos al menú **File**, opción **New** y **Virtual Machine**.

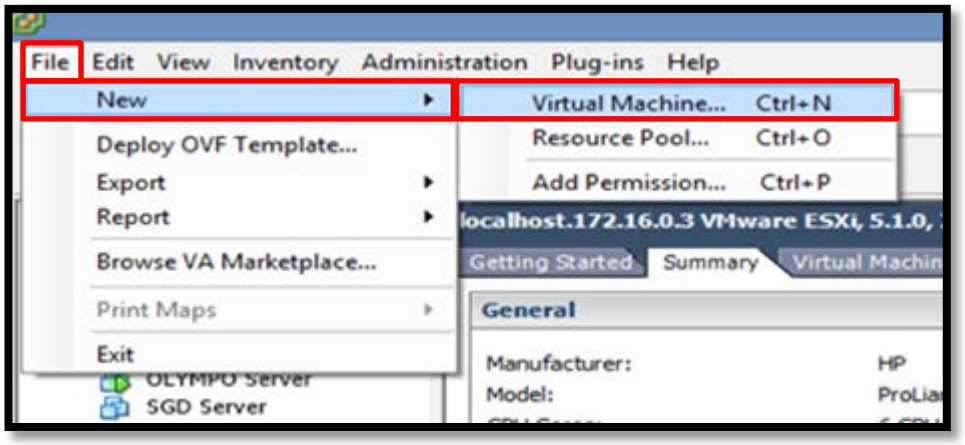


Figura 8: pantalla crear nueva máquina virtual

9. Seleccionar la opción **Custom** y presionar **Next** como muestra la figura 9.

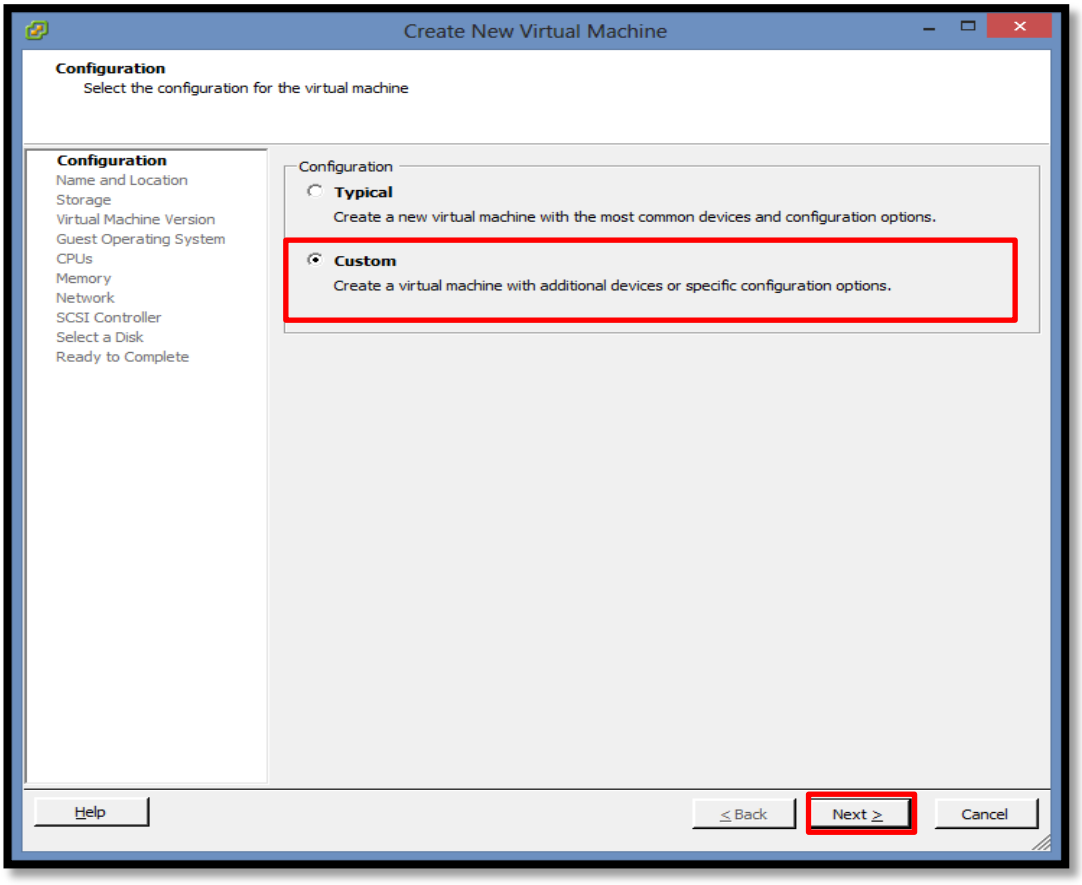


Figura 9: pantalla para seleccionar el tipo de configuración

10. Ingresar el nombre de nuestro servidor virtual y hacer clic en el botón **Next** como se ve en la figura 10.

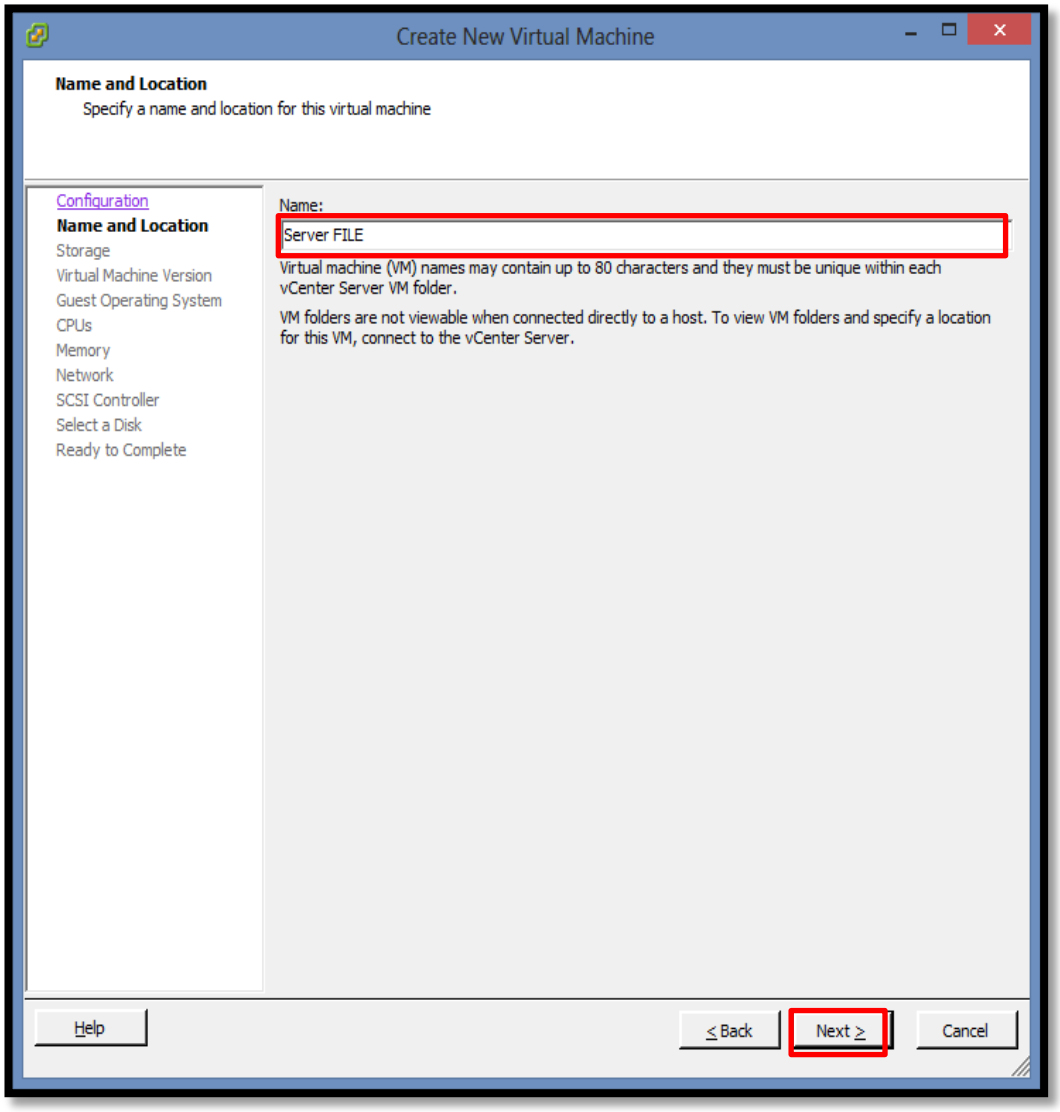


Figura 10: pantalla para dar el nombre al nuevo servidor virutal

11. La figura 11 indica como seleccionar el **Datastore** en donde se almacenarán los datos del servidor virtual a restaurar, presionar el botón **Next**.

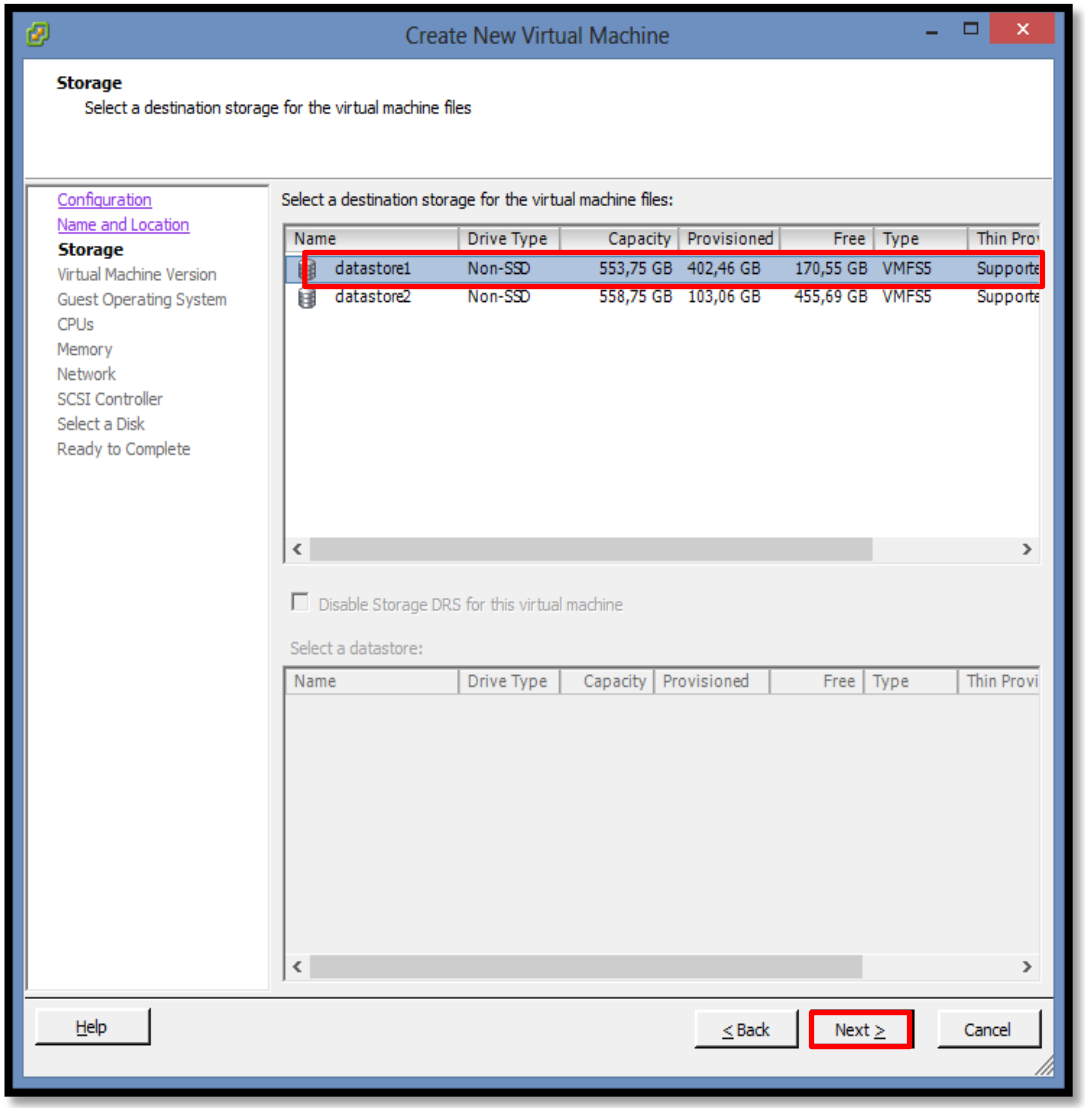


Figura 11: pantalla para seleccionar el datastore

12. Escoger el tipo de Máquina Virtual, en este caso seleccionar **Virtual Machine Version: 8** y hacer clic en el botón **Next,** como indica la figura 12.

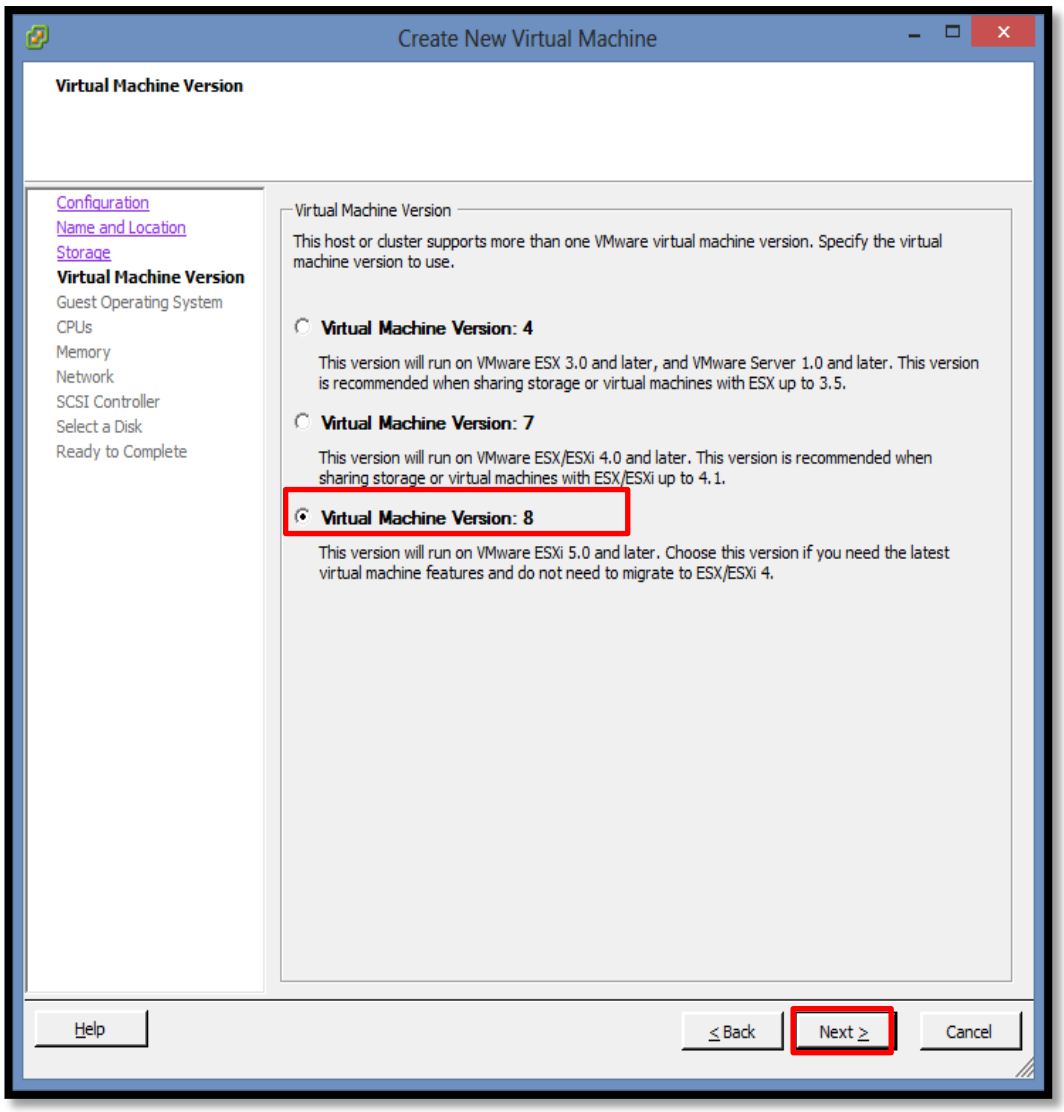


Figura 12: pantalla para seleccionar la versión dela máquina virtual

13. Seleccionar el sistema operativo para el servidor virtual y hacer clic en **Next**, como se puede observar en la figura 13.

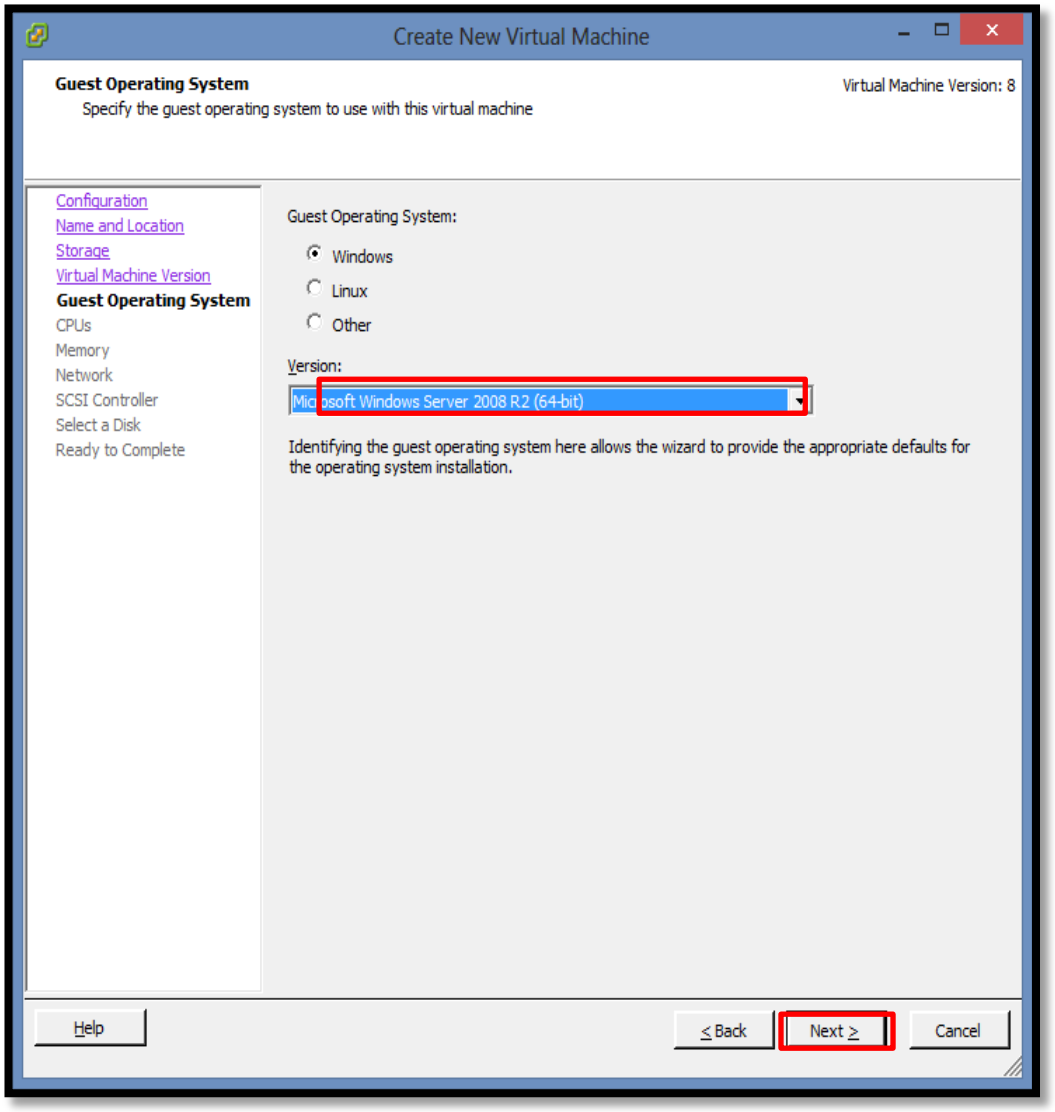


Figura 13: pantalla para seleccionar el sistema operativo

14. Seleccionar la configuración que se necesita en cuanto a procesadores para el servidor virtual, y presionar el botón **Next,** como se indica en la figura 14.

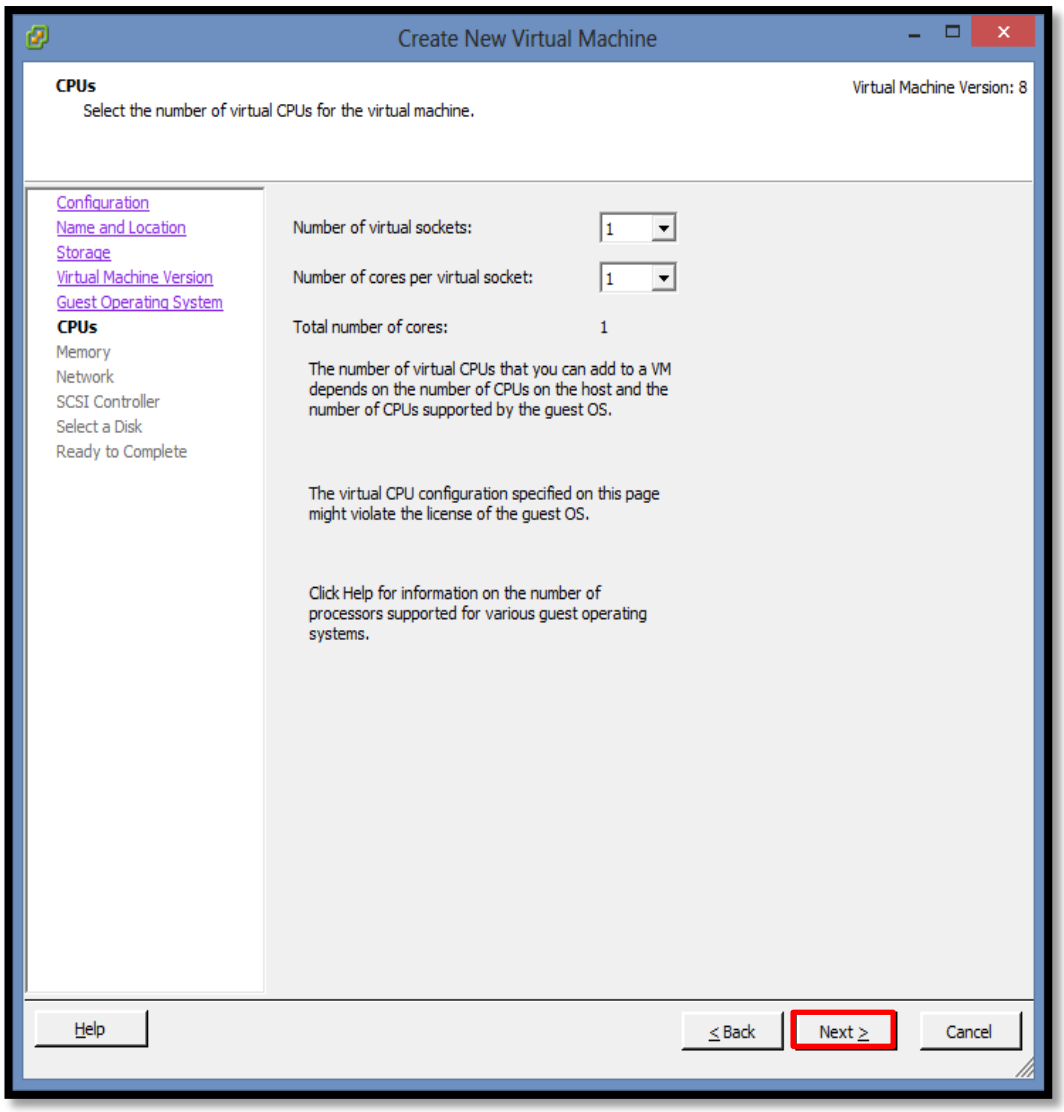


Figura 14: pantalla para configurar procesadores

15. La figura 15 muestra como seleccionar la memoria RAM y presionar **Next**.

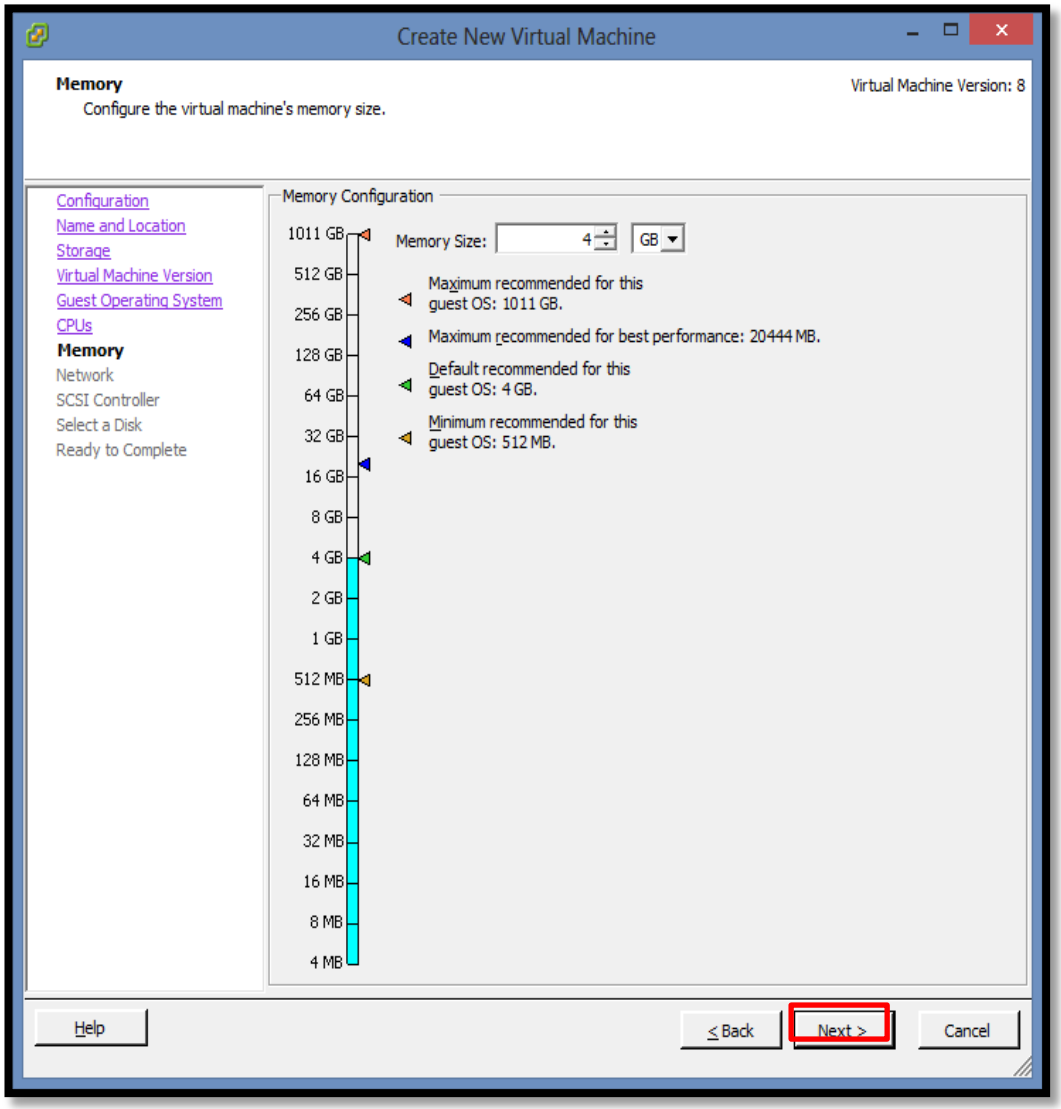


Figura 15: pantalla seleccionar la memoria ram asignada

16. Configurar la interfaz de red y presionar **Next,** como se indica en la figura 16.

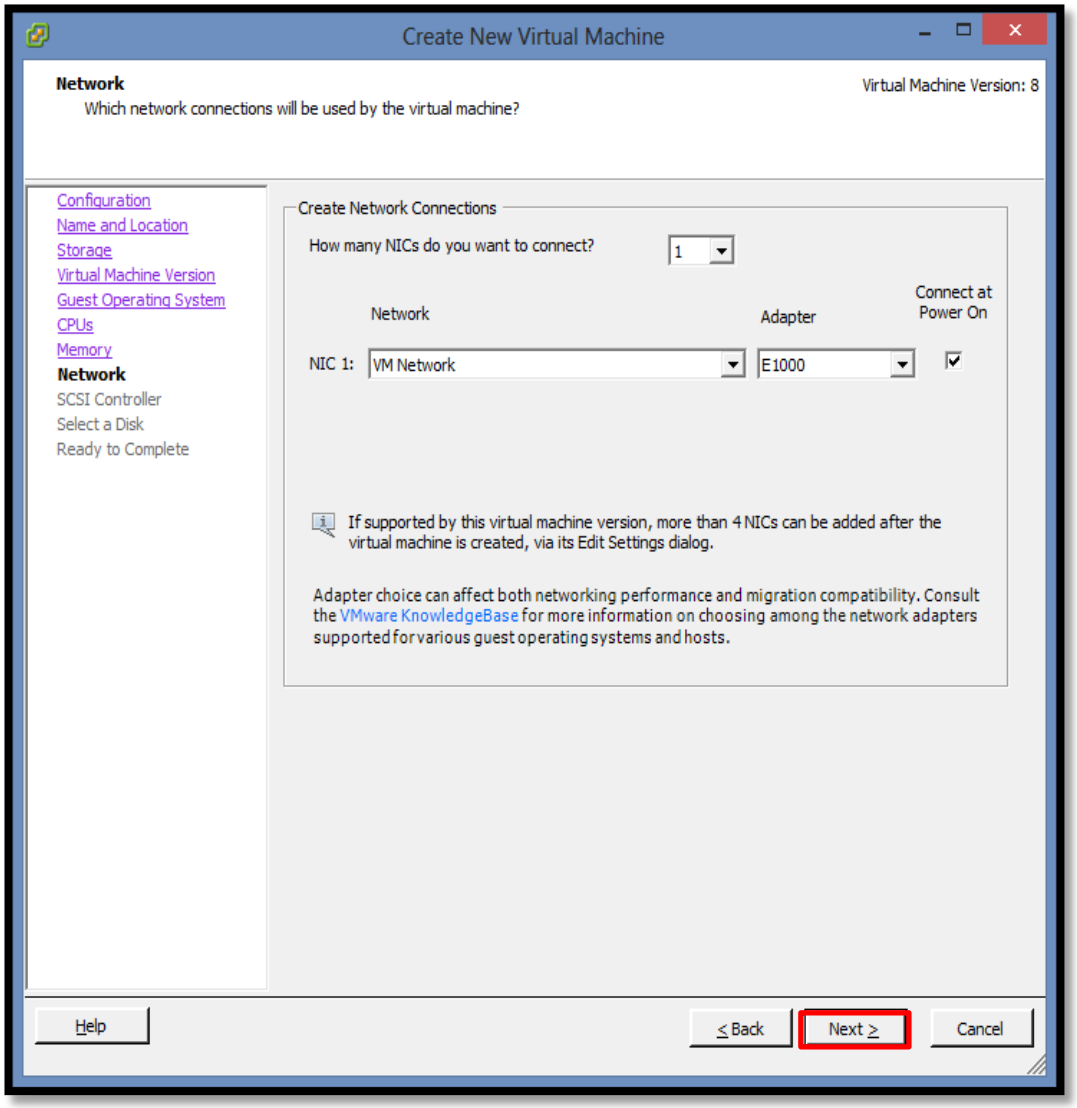


Figura 16: pantalla para configurar la interfaz de red

17. Como muestra la figura 17 seleccionar el tipo de conexión SCSI y presionar **Next**.

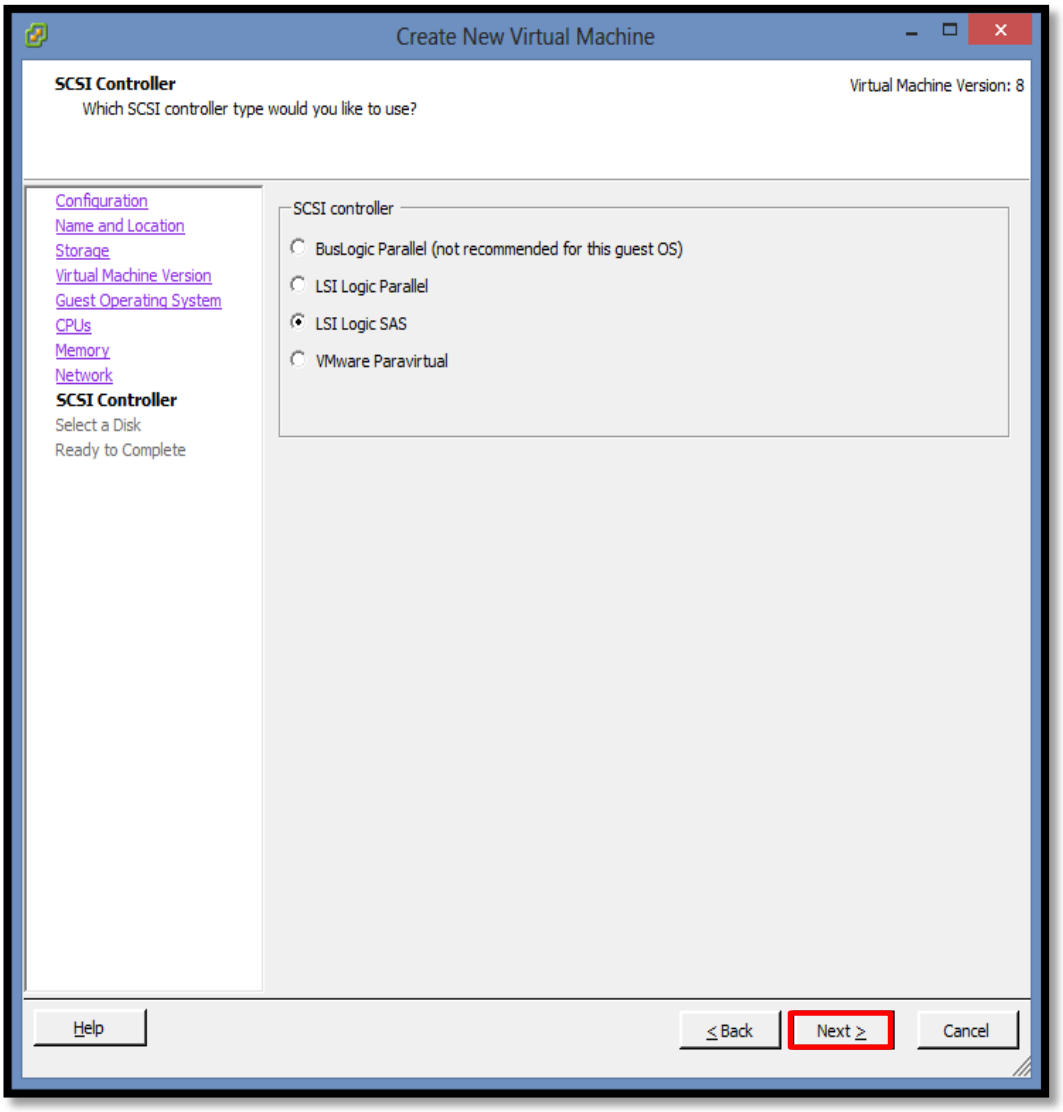


Figura 17: pantalla configurar la conexión SCSI

18. Escoger la opción **Use an existing virtual disk** y presionar **Next ,** como muestra la figura 18.

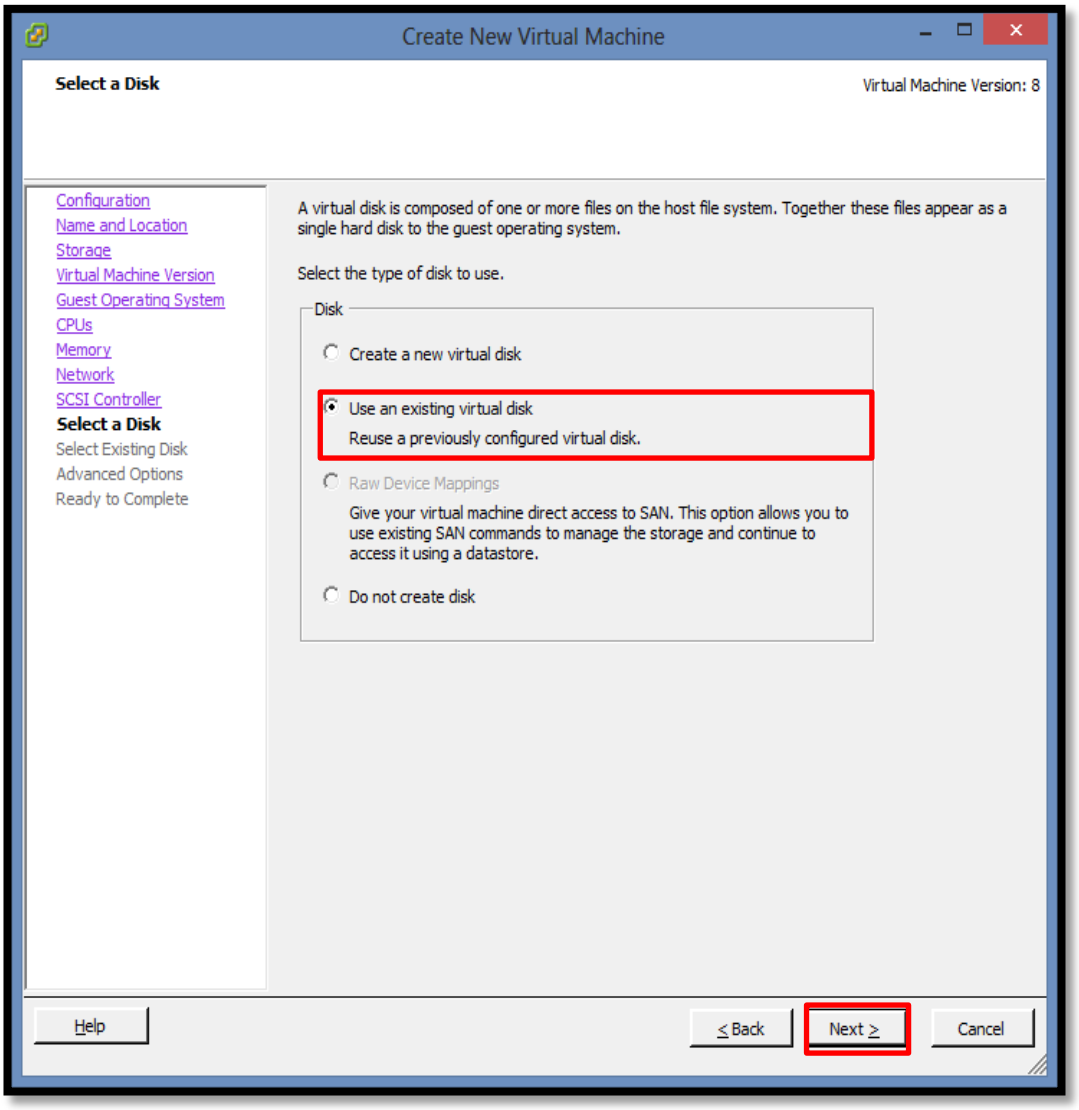


Figura 18: pantalla para escoger o crear un disco virtual

19. Hacer clic en el botón **Browse**, Escoger el path dentro de nuestro **Datastore** donde se encuentran los datos del servidor virtual a restaurar, como se indica en la figura 19.

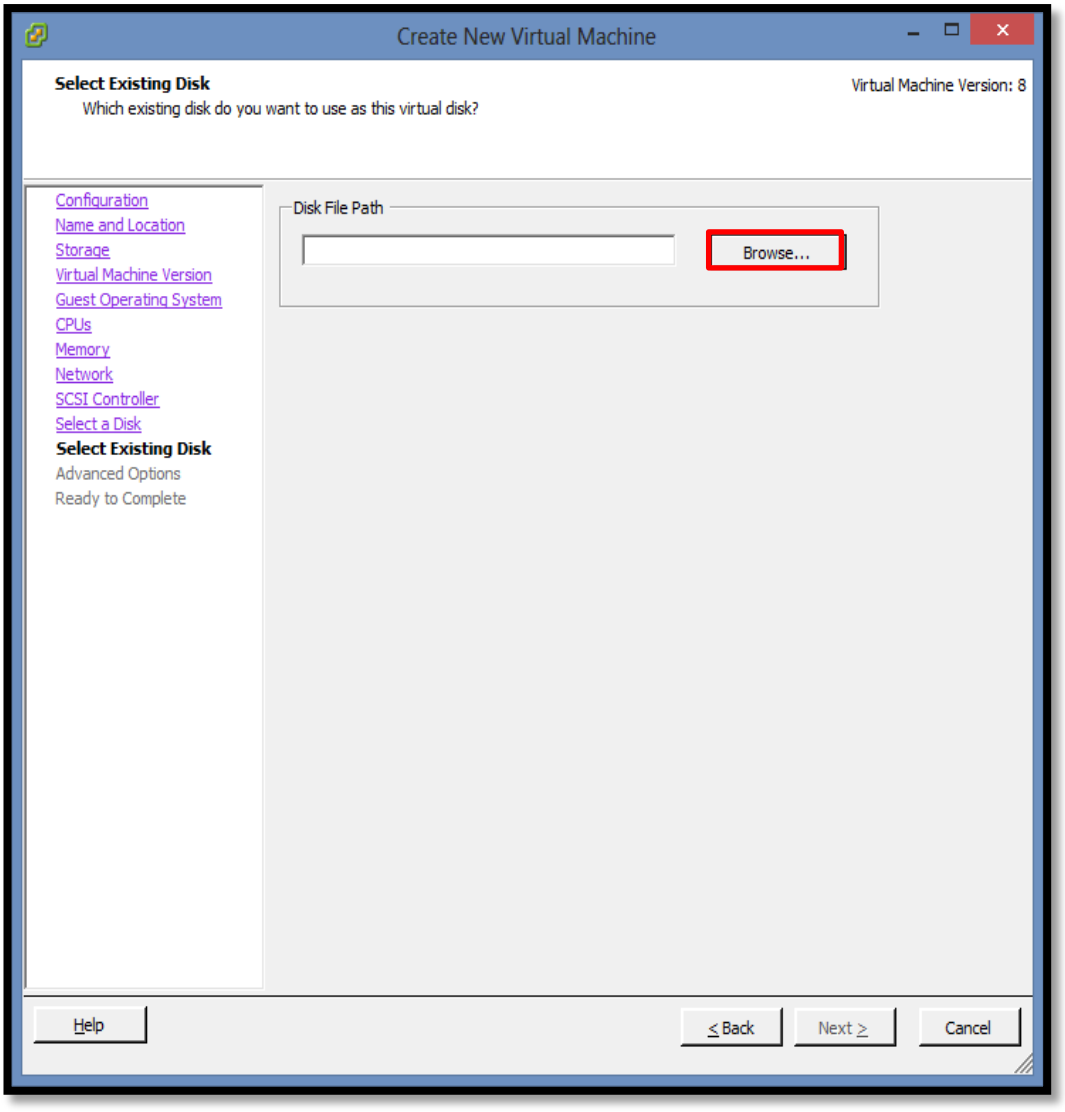


Figura 19: pantalla para seleccionar el path donde se encuentran los datos del servidor

20. Seleccionar el Datasotore en donde se encuentra el respaldo como indica la figura 20.

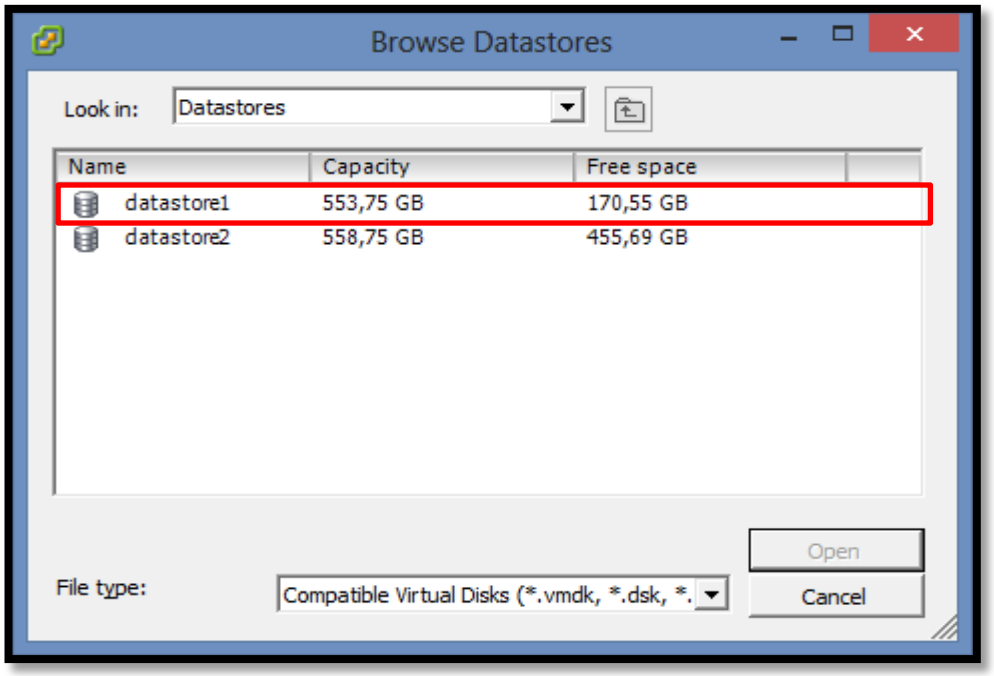


Figura 20: pantalla para seleccionar el datastore

21. La figura 21 muestra como seleccionar la carpeta del servidor.

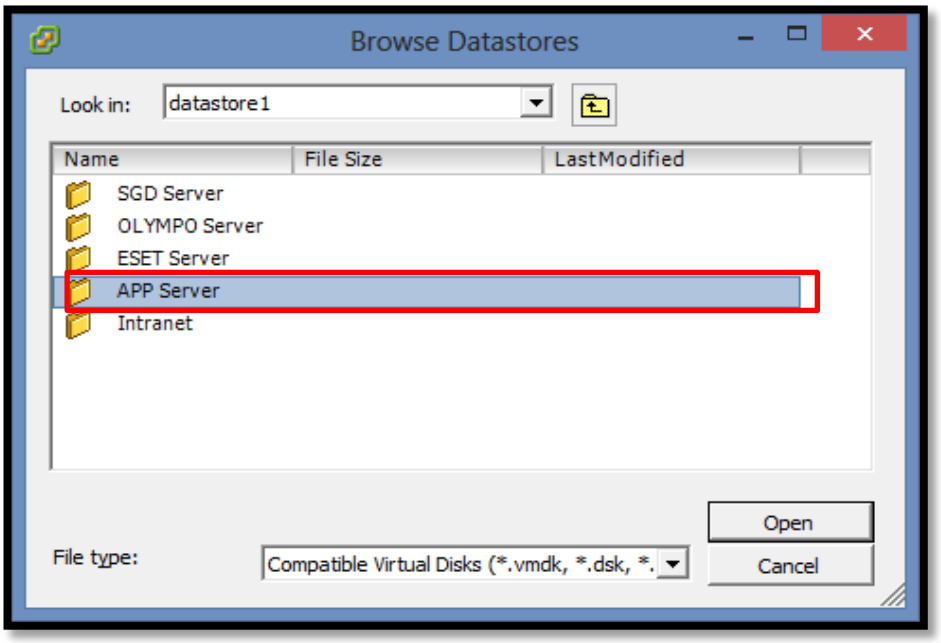


Figura 21: pantalla para seleccionar la carpeta del servidor

22. Una vez seleccionado el path, seleccionar el archivo **vmdk** que contiene el respaldo del servidor .Presionar el botón **Open**, como muestra la figura 22.

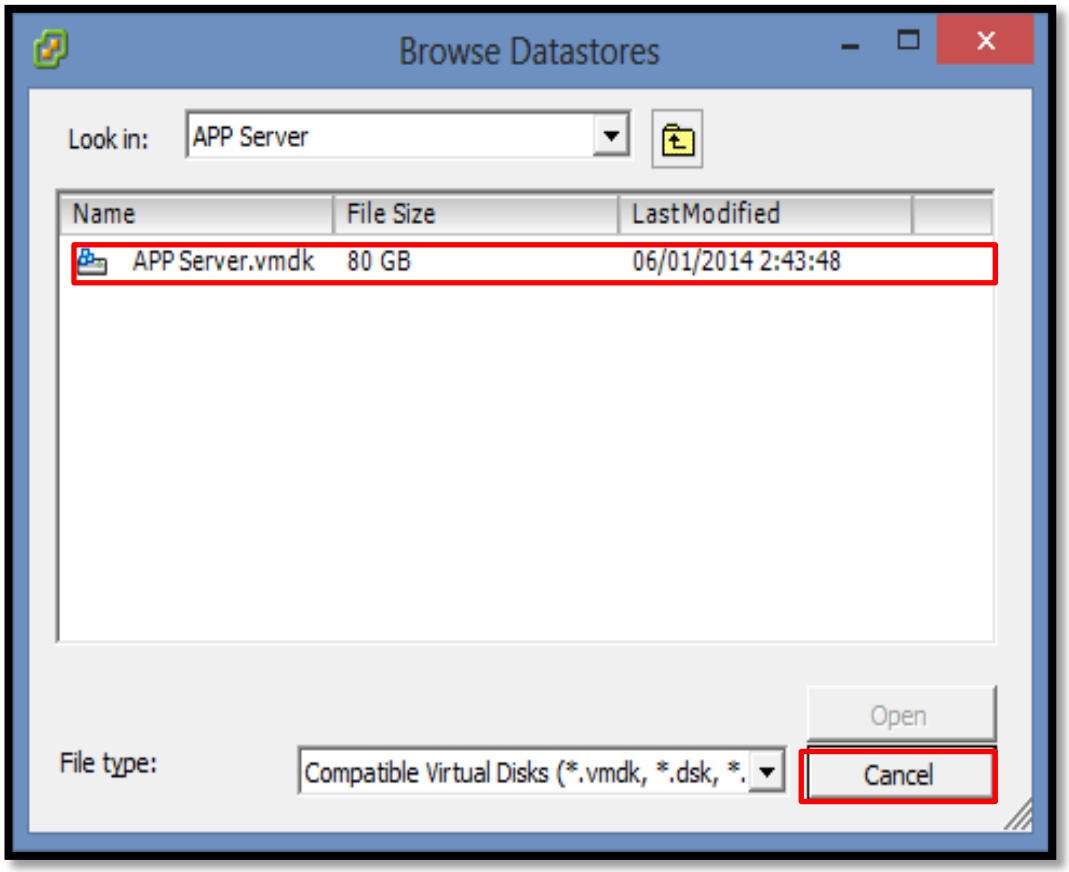


Figura 22: pantalla para seleccionar el archivo wmdk

23. Se muestra el **Disk File Path** que contiene el Datasotore, el path y el archivo vmdk a restaurarse, presionar el botón **Next,** como indica la figura 23.

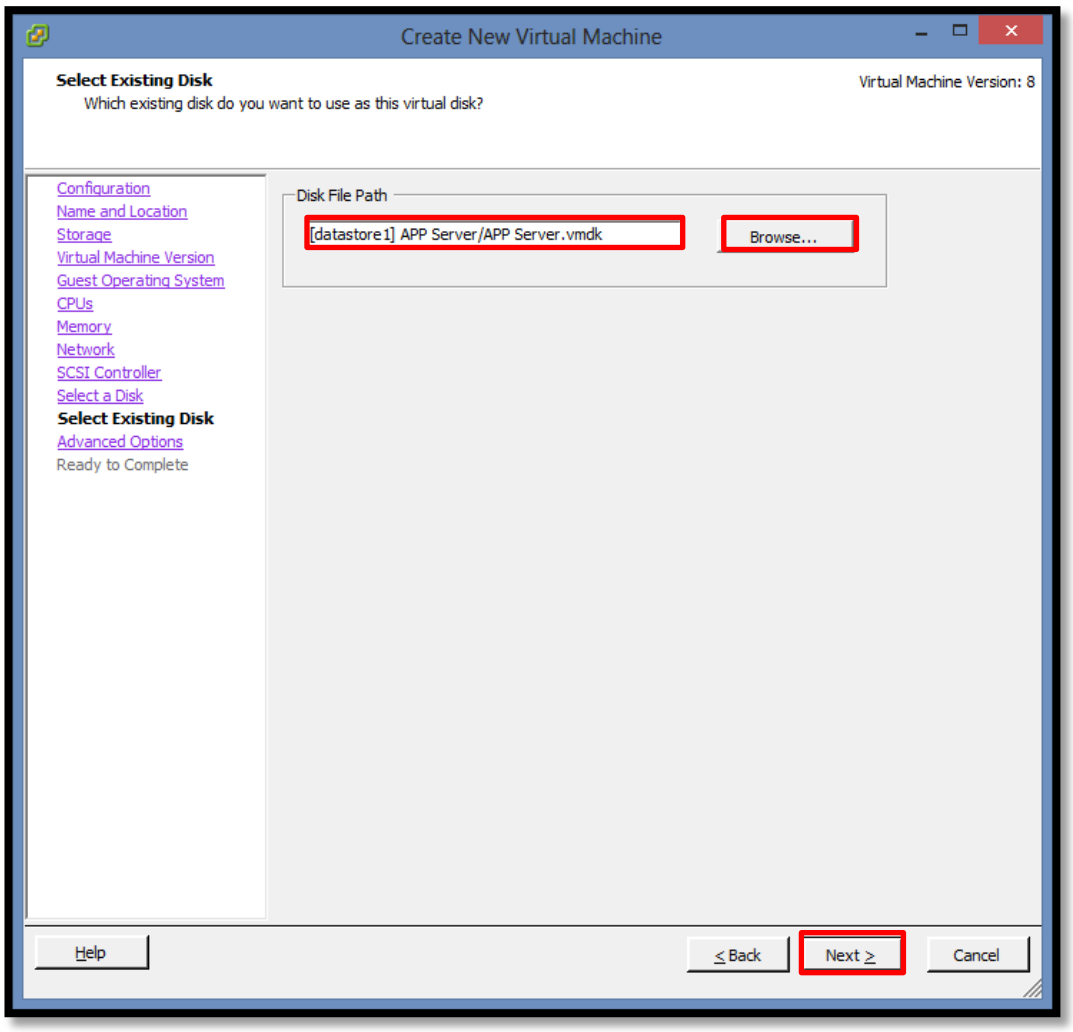


Figura 23: pantalla con el path de donde se subirán los datos

24. Finalmente presionar **Finish** como se observa en la figura 24.

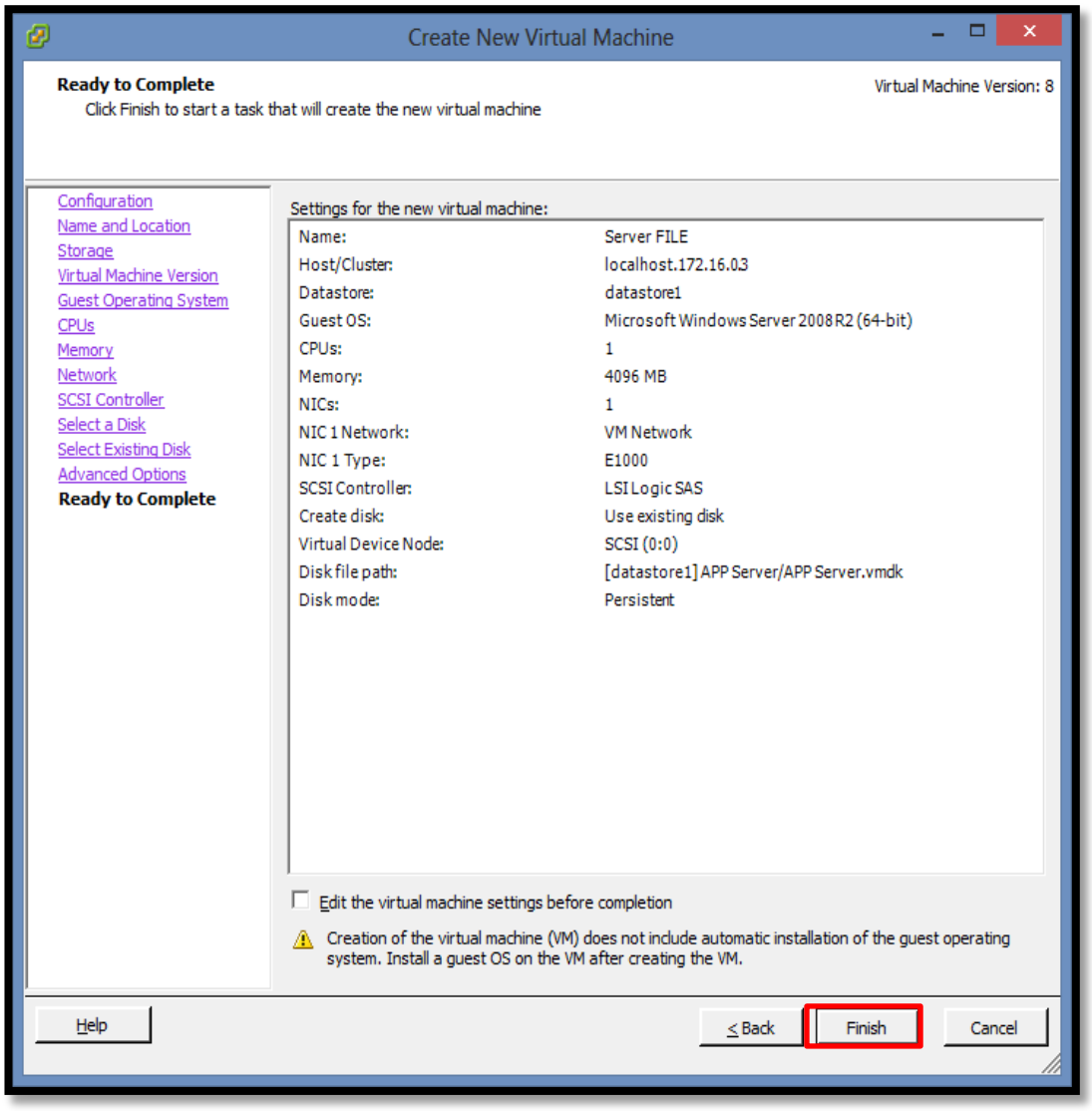


Figura 24: pantalla para finalizar la restauración de los datos

Proceso para restaurar el servidor Moodle

Responsable: Web Master

1. Digitar **https://www.1and1.com/login** en el navegador de internet para poder ingresar a la ventana de administración del servidor, y aparecerá la pantalla que se observa en la figura 1.

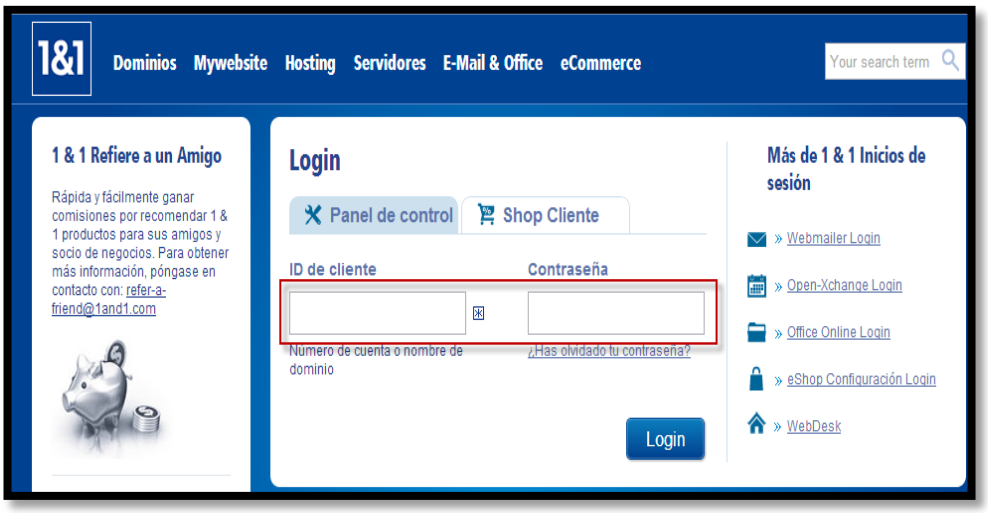


Figura 1: pantalla para ingresar

2. Ingresar el **Id. de Cliente**, la Contraseña, y presionar el botón **Login**, aparecerá la pantalla que se muestra en la figura 2. Seleccionar la opción **Servidores**.

Figura 2: pantalla seleccionar el servidor

3. En la pantalla q se muestra en la figura 3., seleccionar la opción **Herramientas de recuperación**.

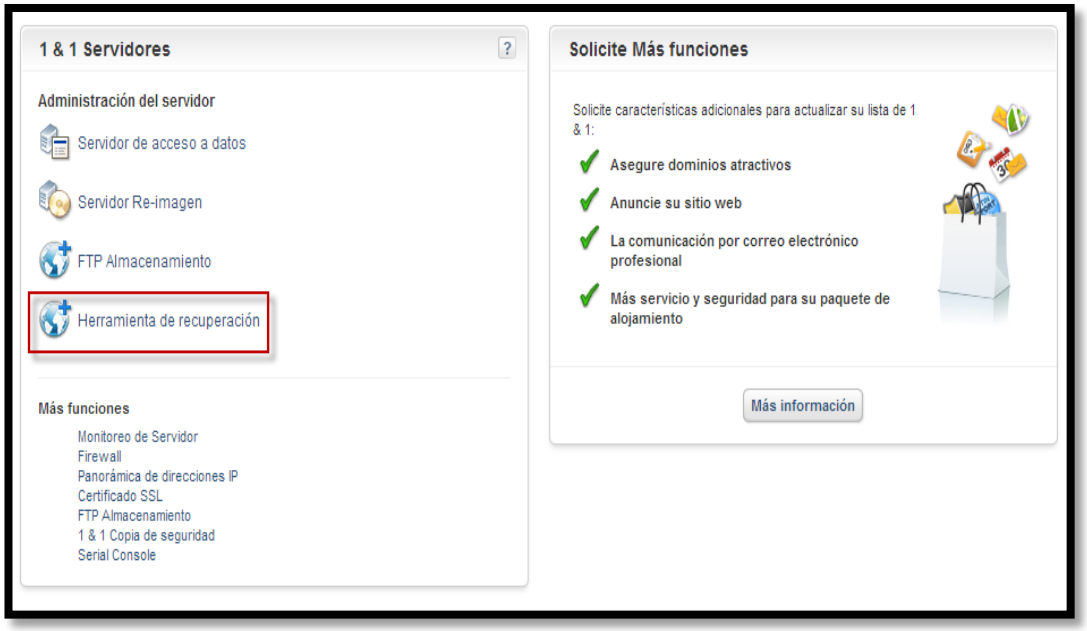


Figura 3: pantalla de administración del servidor

4. Luego en la pantalla q se muestra en la figura 4, seleccionar la opción **Reboot now**, y presionar el botón **Next.**

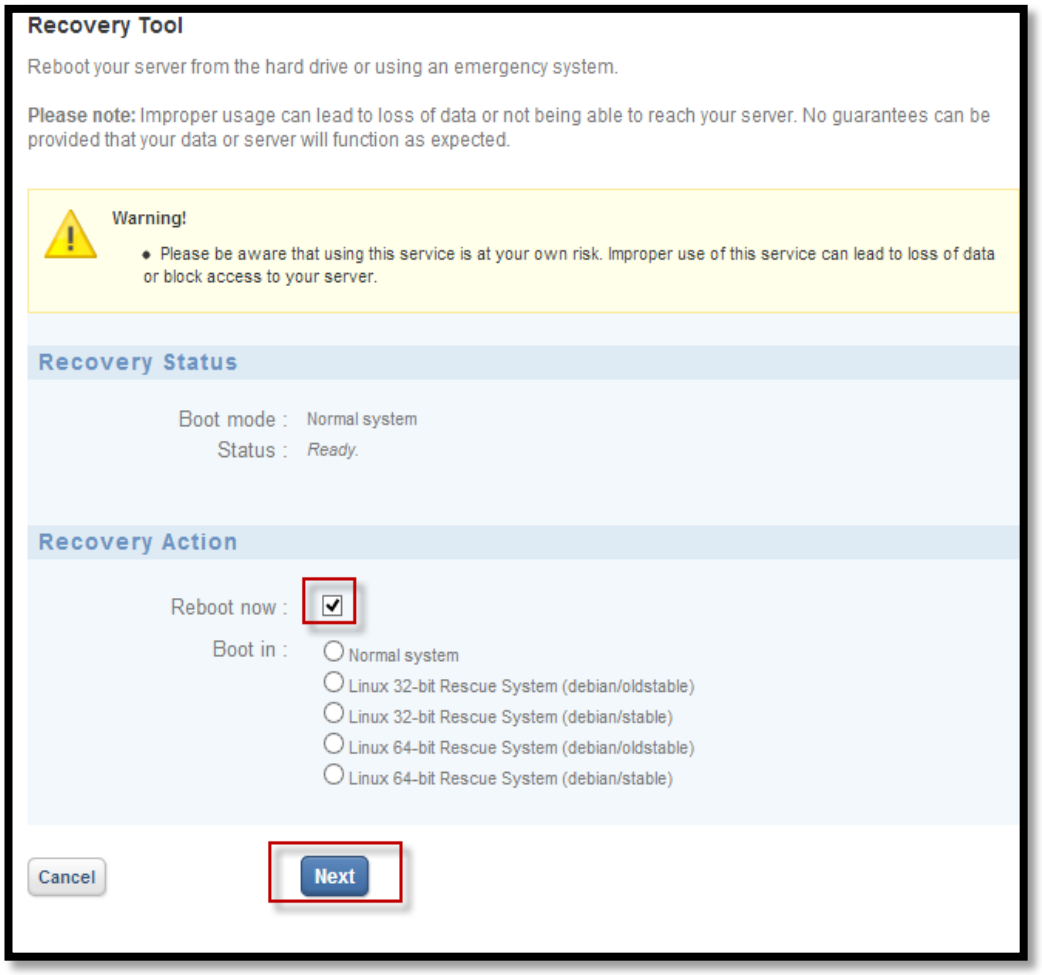


Figura 4: pantalla para reiniciar el servidor

Anexo 14

Formato para la documentación de pruebas

Prueba del Plan de Contingencia				
Riesgo:		**Fecha:**		**Hora:**
Descripción del escenario:				
Nº	**Actividad o control ejecutado**	**Tiempo de ejecución**	**Responsable**	**Observaciones**
Recomendaciones:				
Elaborado por:				

CAPÍTULO V

5. Conclusiones y Recomendaciones

5.1. Conclusiones

- Las Normas ISO 17799, COBIT, NFPA 10 Y NFPA 75 han contribuido para poder definir controles que brinden seguridad tanto al personal como a la infraestructura tecnológica del Área de TI de Innovativa.
- Se han determinado 12 contingencias potenciales a las que actualmente INNOVATIVA se expone y que deben ser controladas.
- No existe documentación de los procesos para recuperación de una contingencia.
- El plan de contingencias para el Área de TI, está enfocado principalmente en prevenir y reducir los daños causados al suscitarse una contingencia. y permitirá reducir de manera razonable la probabilidad y el impacto de los riesgos.

5.2. Recomendaciones

- En lo posible seguir implementado los controles para la seguridad de la infraestructura de TI sugeridos en las Normas ISO 17799, COBIT.
- Documentar los procesos que se deben ejecutar para la recuperación de un desastre.
- Implementar los controles de prevención establecidos en el plan en un periodo máximo de seis meses.

- Una vez implementados los controles establecer un cronograma de pruebas y ejecutarlo.
- Revisar, evaluar y rehacer el plan de contingencias en el periodo de un año.

Bibliografía

Claudio, B. A., & Chicaiza, N. d. (2003). *Propuesta de un manual de contingencia informático para la U. T. C.* Latacunga.

Dirección de Tecnologías de Información y Comunicaciones. (2007). *Manual para elaborar un Plan de Continuidad del la Gestión en tecnologías de Información y Comunicaciones.* Costa Rica.

Empresa Municipal Administradora de Peaje de Lima. (2011). *Plan de Contingencia Informático de la Empresa Municipal Administradora de Peaje de Lima.* Lima.

Goode, W., & Hatt, P. (1977). *"Estudio de casos", en Métodos de Investigación Social.* México.

Hernandez, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación* (Quinta edición ed.). México D.F.: MacGrawHill.

Huamán Valencia, H. G. (2005). *Manual de Técnicas de Investigación Conceptos y Aplicaciones.* Lima, Perú: IPLADESS S.A.C.

Instituto del Mar del Perú. (2012). *Plan de Contingencias Informático 2012-2015.* Callao.

Instituto Nacional de Estadística e Informática. (2001). *Guía práctica para el desarrollo de planes de contingencia de Sistemas de Información.* Lima.

ISO/IEC 17799. (2005).

IT Governance Institute. (2007). *Cobit 4.1.* Estados Unidos.

Llumiquinga Marcillo, C. V., & Vallejo, P. F. (2005). *DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DESARROLLO DEL PLAN DE CONTINGENCIA PARA EL ÁREA DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE.*

Mackernan, J. (1989). *"El estudio de casos" en Investigación.* Madrid.

Maza Anton, G. L. (2009). *Plan de Contingencia Informático y Serguridad de la Información aplicado en al Universidad Nacional de Piura.* Piura.

Monroy Cornejo, S. (2009). El Estudio De Caso: ¿Método o Técnica de Investigación? *Metodología de la Ciencia*.

Municipalidad de la Punta. (2010). *Plan de Contingencia Informático.* Perú.

Paz, C. (2010). *Ingeniería en Sistemas*. Obtenido de Ingeniería en Sistemas ITSC: http://pazsystemengineering.blogspot.com/2010/05/plan-de-contingencia-informatico.html

Ramirez, M. Y., Londoño, E. A., & Gómez, J. A. (2012). *Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la empresa "T"*. Bogotá.

Stake, R. (1999). *Investigación con estudio de casos.*

Villaón Huerta, A. (2004). *Códigos de buenas prácticasde seguridad UNE-ISO/IEC 17799.* Obtenido de http://www.shutdown.es/ISO17799.pdf

Yory, J. (2006). *http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf.*