PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA:

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

INFORME DE ESTUDIO DE CASO

PLAN INFORMÁTICO DE CONTINGENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE TIC DE LA PUCESE.

PREVIO AL GRADO ACADÉMICO DE INGENIERIA DE SISTEMAS Y COMPUTACIÓN

AUTOR:

LADINES GARCÉS KATHERINE STEFANIA.

ASESOR:

ING. SUSANA PATIÑO ROSADO

ESMERALDAS, 2017

Disertación Aprobada luego de haber dado cumplimiento de los requisitos exigidos por el reglamento de Grado de la Pontificia Universidad Católica del Ecuador Sede en Esmeraldas, previa la obtención del Título de Ingeniería de Sistemas y Computación.

Ing. Susana Patiño Rosado

ASESORA DE TESIS

Ing. Klever Vera

LECTOR 1

Ing. Xavier Quiñónez Ku

LECTOR 2

Ing. Xavier Quiñónez Ku

DIRECTOR DE ESCUELA

FECHA: …….

AUTORÍA

Yo, KATHERINE STEFANIA LADINES GARCÉS, declaro que la presente investigación enmarcada en el actual trabajo de estudio de caso es absolutamente original, autentica y personal.

En virtud que el contenido de esta investigación es de exclusiva responsabilidad legal y académica de la autora y de la PUCESE.

KATHERINE STEFANIA LADINES GARCÉS

CI: 0803482413

AGRADECIMIENTO

A mis padres, Elena y Luis, por su apoyo incondicional, sus buenos consejos y los valores enseñados que han sido mi fortaleza para luchar por mis sueños.

A mis hermanos, Jefferson, Charly, Lupita, por ser la inspiración para culminar este proyecto, han sido una bendición para mi vida desde que Dios permitió que llegaran a este mundo, con su alegría e inocencia impulsan cada día para ser su ejemplo.

A mi asesora, Ing. Susana Patiño, por el tiempo y la dedicación que brindó durante el desarrollo de mi estudio de caso, quien con sus conocimientos supo guiarme para realizar un buen trabajo.

A mis docentes, que compartieron sus experiencias y enseñanzas durante mi tiempo de aprendizaje universitario, gracias a ellos tengo una visión de ingeniera preparada para el ambiente profesional.

DEDICATORIA.

A Dios, por ser la luz durante todo este camino, porque su bondad permitió que culminara este proyecto y simplemente de su mano su mano nade es imposible.

A mi abuelita que está en el cielo, porque su ausencia me ayudó a valorar más la vida y saber apreciar las bendiciones que Dios pone en mi camino.

INDICE

INDICE DE FIGURAS

INIDICE DE TABLAS

1. RESUMEN.

La propuesta del plan de contingencia para el departamento de TIC’s de la PUCESE, se plantea como una problemática, por las razones de que ningún territorio está libre de enfrentar una situación o escenario de riesgo que puede ser catastrófico para el lugar que lo experimente. Las probabilidades de presentarse una contingencia son altas debido a los antecedentes que se tienen actualmente en la ciudad de Esmeraldas y uno de los principales motivos son los movimientos telúricos presentados hasta el momento en la ciudad. Es por ello que entre los principales objetivos esta identificar los escenarios de riesgos y vulnerabilidades que pueden afectar el área de TIC’s; para lo cual se realizó un análisis aplicando varias técnicas de investigación.

Durante el desarrollo del estudio se plantean tácticas que permitirán la elaboración de un plan de contingencia con el personal que labora actualmente, pues están en la capacidad de ejecutar la debida planificación para superar un escenario de contingencia. Así también cabe mencionar que es indispensable la organización de equipos para efectuar el plan, se plantean los escenarios más críticos que se pudieron analizar para el departamento de TIC’s de la PUCESE, proponiendo estrategias que permitan la continuidad de las operaciones de manera que se evite interrumpir la jornada laboral en caso de presentarse un escenario de riesgo.

La propuesta del plan de contingencia finaliza realizando un análisis de los pasos que debe seguir el departamento de TIC’s de la PUCESE para aplicar el plan, consiguientemente las pruebas de verificación que se deben realizar y las respectivas recomendaciones para que el plan sea factible.

2. ABSTRACT.

The proposal of the contingency plan for the TIC department of the PUCESE, is considered as a problem, for the reasons that no territory is free to face a situation or scenario of risk that can be catastrophic for the place that experiences it. The chances of a contingency occur are high because of the antecedents that are currently in the city of Esmeraldas and one of the main reasons are the earthquakes presented so far in the city. That is why among the main objectives is to identify the scenarios of risks and vulnerabilities that can affect the area of TIC; For which an analysis was carried out applying several research techniques.

During the development of the study, tactics are proposed that will allow the elaboration of a contingency plan with the staff that is currently working, as it is able to execute the proper planning to overcome a contingency scenario. It is also worth mentioning that it is indispensable to organize teams to carry out the plan, the most critical scenarios that could be analyzed for the TIC department of PUCESE are proposed, proposing strategies that allow the continuity of operations so as to avoid interrupting the working day in the event of a risk scenario.

The proposal of the contingency plan finalizes the accomplishment of an analysis of the steps that must be followed by the department of the TIC of the PUCESE to apply the plan, the tests of verification that must be realized and the respective recommendations for the feasible plan.

3. JUSTIFICACIÓN.

Cualquier sistema de información está expuesto a riesgos, es decir tanto el software como el hardware son vulnerables a diversos factores de riesgo que pueden ser humanos, físicos o naturales. En caso de presentarse cualquier incidente, la urgencia para la determinación de la gravedad del problema ocurrido va a depender de la capacidad, habilidad y la estrategia a seguir para señalar con precisión una posible solución ante el evento sucedido.

Ante la ocurrencia de un escenario de riesgo, lo primero que se tiene en cuenta es saber cuánto tiempo llevara recuperar la normalidad de las labores, a esto también se lo conoce como (tiempo de recuperación de la información); lo cual significa una fuerte inversión en recursos humanos y técnicos para lograr recuperar todo lo afectado. Cabe mencionar que la protección de la información es vital ante la posible pérdida, destrucción, robo y otras amenazas que se presentan en una institución, por ello se debe tener el conocimiento y preparación de un plan de contingencia informático.

Las personas que intervienen directamente con este caso de estudio son los integrantes del departamento de TIC de la PUCESE, los cuales cumplen distintos roles, cuyas actividades van desde coordinación de proyectos realizados a beneficios de la universidad, hasta dar asistencia técnica a docentes o personas que lo soliciten dentro de la institución.

El planteamiento del estudio tiene un alto impacto en la mejora de los servicios que brinda el departamento de TIC de la PUCESE, pues al aplicar un plan de contingencia se tendrá de manera planificada las posibles respuestas a riesgos que pueden llegar a incidir en esta área. Permitiendo que se pueda tener una respuesta ágil y eficiente ante los inconvenientes que se puedan presentar, optimizando recursos, garantizando que se mantenga la seguridad de los procesos, de la información que se maneja en la institución y la integridad del personal que labora en el departamento.

4. OBJETIVOS.

4.1. OBJETIVO GENERAL.

- Determinar un plan de Contingencia de TI mediante la especificación de los procedimientos de los escenarios críticos que afectarían a los servicios tecnológicos principales de la PUCESE.

4.2. OBJETIVOS ESPECÍFICOS.

- Efectuar un previo diagnóstico que permita identificar servicios críticos de TI mediante una investigación de campo en el departamento de TIC de la PUCESE
- Prever las consecuencias de riesgos tecnológicos de las actividades operativas y analizar estrategias que permitan la continuidad de la actividad con el menor tiempo y trastorno posible.
- Realizar las observaciones correspondientes para mitigar los riesgos que se presentan, de acuerdo a la información recopilada.

- Proponer una metodología para definir las etapas y actividades que contiene un Plan de Contingencia de TIC.

5. CASO.

5.1. DEPARTAMENTO INFORMÁTICO.

El departamento de informática en una organización juega un papel muy importante, debido a que significa todo el sustento técnico/tecnológico dentro de la entidad o empresa donde se aplique, el departamento informático puede dirigir las siguientes funciones: la gerencia de redes, dar soporte a los usuarios, crear, administrar y dar seguimiento a las bases de datos, procurando siempre cuidar la integridad de equipos e información, realizando aplicaciones y reportes que aporten insumos para la toma de decisiones, controlar usuarios y perfiles, etc.

Entre las características que debe tener un departamento informático se resaltan que debe ser proactivo y propositivo, no debe dar excusas de lo que no se puede hacer sino proponer y tomar iniciativa sobre lo que se debe hacer, esto debido a que un analista informático tiene la capacidad de identificar más fácilmente procesos que pueden ser automatizados.

El departamento informático debe tratar a las demás áreas como clientes con los cuales tiene que cumplir con el objetivo de reducir los problemas que se presentan diariamente en la operación de los colaboradores de las distintas áreas; teniendo sentido de la responsabilidad para la confidencialidad de la información, haciendo uso adecuado de los recursos de la empresa, organización o institución correspondiente.

Vigo (2001) menciona que el departamento de informática debe ser un área líder en la optimización de procesos y calidad, pues es uno de los principales objetivos de este departamento, manteniéndose informados sobre los últimos avances tecnológicos y diseñar aplicabilidad en busca de la reducción de procesos y disminución de costos, así también dar seguimiento a los problemas de un sistema como una debilidad propia, debido a que dicha falla trae pérdidas económicas a la organización en general.

Se considera que una de las tareas que tiene el departamento y considerada como una de las más importantes es que debe analizar el impacto económico que tendría cada acción que se puede implementar teniendo presente que se deben cumplir con las normas de calidad. En síntesis para que funcione correctamente una organización, sus áreas deben complementarse al trabajar coordinados en busca de los mismos objetivos y evidentemente sobre una misma dirección, lo cual implicaría que el trabajo del departamento informático debe ir en función de quitar obstáculos (en automatización), no de resolver incidentes (casos solicitados); de esta forma concluye (Vigo, 2001).

5.2. SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN.

Para comprender el concepto de lo que lo que son los Servicios de TI es mejor empezar definiendo varios conceptos que están relacionados con el tema y lograr una mayor comprensión. A continuación se explican los siguientes, tomando como referencia conceptos de (Vigo, 2001):

Servicio.- Es una manera de proveer valor a los clientes facilitándole resultados que quieren obtener evitando asumir costos y riesgos específicos.

Proceso.- Un conjunto de actividades coordinadas que combinan e implementan recursos y habilidades con el fin de lograr un resultado, que directa o indirectamente, aportan valor para el usuario o cliente.

En todo servicio se respaldan los procesos, es por eso la relación de estos conceptos importantes antes de establecer el tema de lo que es un servicio de TI y como se realiza su gestión.

Entonces un servicio de tecnología de información se lo define como el conjunto de actividades que buscan responder a una o más necesidades de un cliente por medio de un cambio de condición en los bienes informáticos potenciando el valor de estos y reduciendo el riesgo inherente del sistema. Según lo establecido por Gilberto Moncada Vigo (2001) un servicio TI se basa en el uso de las tecnologías de la información y soportar los procesos de negocios del cliente, también cabe mencionar que los servicios TI se componen de una combinación de personas que utilizan sus habilidades para otorgar valor al cliente aplicando una disciplina basada en procesos, enfocándose al alineamiento

que proporcione cumplir con las necesidades de la empresa, poniendo énfasis en los beneficios que se pueden percibir para la institución.

5.3. DEPARTAMENTO DE TIC'S DE LA PUCESE.

Al incrementarse la demanda del servicio de educación superior en estos últimos años en el país, y por ende, la PUCESE ha tenido que ampliar su oferta académica a la sociedad, esto conlleva al crecimiento en los servicios tecnológicos necesarios para poder responder a dicha demanda.

Desde esta óptica, la PUCESE debe garantizar disponibilidad, confiabilidad y continuidad de los servicios informáticos para el diario ejercicio del área administrativa y académica de la comunidad universitaria.

La PUCESE cuenta con un departamento de TIC's que se encuentra organizado de la siguiente manera:

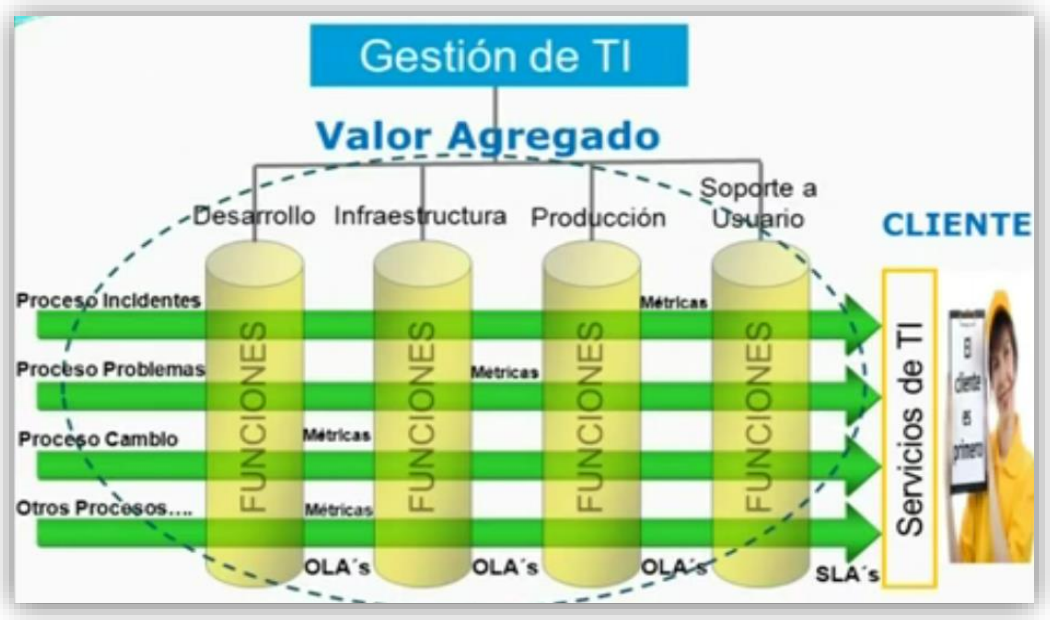
Figura 1. Organización del Departamento de TIC's

5.4. GESTIÓN DE SERVICIO TI.

La Gestión de Servicio TI es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final. Y teniendo estos conceptos básicos bien claros se puede liderar con objetividad una organización TI dentro de cualquier organización. Purificación Aguilera López (2005) argumenta que dentro de esta área el concepto de ***buenas prácticas*** se refieren a las formas óptimas de ejecutar un proceso, los

mismos que pueden servir de modelo para otras organizaciones considerándose como marco de trabajo de buenas prácticas en el área de informática que están destinadas a facilitar y mejorar la entrega de servicios de tecnologías de la información.

Figura 2. Gestión de TIC Aplicado al Departamento Informático



Fuente: Tomado De La Investigación De (Sartenejas, 2009)

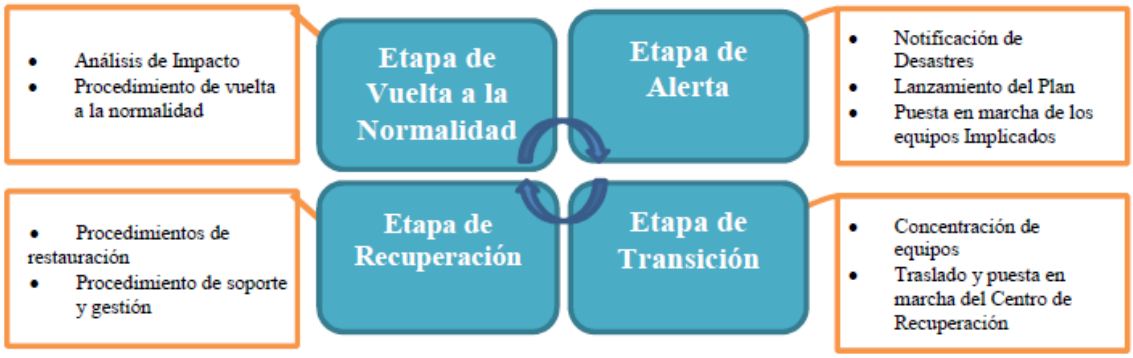
5.5. PLAN DE CONTINGENCIA.

Un plan de contingencia se considera como la estrategia planificada constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocios por una paralización total o parcial de la capacidad operativa de la empresa, (Vigo, 2001). Es decir se podría definir a un plan de contingencias como una estrategia planificada que permite orientar una solución alternativa para restituir rápidamente los servicios de la organización ante la presencia de alguna eventualidad que paraliza las actividades de una entidad laboral que se puede dar parcial o totalmente. Sin embargo, el plan de contingencia funciona más bien como una herramienta que ayudará a que los procesos críticos de una empresa u organización tengan continuidad de funcionamiento aún cuando se presente una falla en los sistemas computarizados.

Las razones de proponer un plan de contingencia no pretende un reconocimiento de la ineficiencia en la gestión de las actividades realizadas en una empresa, sino más bien significa todo lo contrario, pues aporta un importante avance a la hora de superar todas aquellas posibles situaciones de peligro y que pueden provocar importantes pérdidas, no sólo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo, (Vigo, 2001)

El plan de contingencia está compuesto de varias etapas que se deben seguir paso a paso para su correcto desarrollo, las cuales se observan a continuación:

Figura 3. Etapas del Plan de Contingencia



Fuente: Tomado de la investigación de (Alvarez, 2014)

5.6. ELEMENTOS ESENCIALES PARA EL PLAN DE CONTINGENCIA INFORMÁTICO.

El consenso: Son los planes, que deben ser propuestos, elaborados con el apoyo de los todos los departamentos, para que sean presentados y aprobados por la Autoridad de la Institución, las prioridades deben ser pactadas con anterioridad por las partes implicadas.

Los recursos: los recuersos se refieren a los lugares alternativos de trabajo, Ordenador con "hardware" y"software" apropiados, Terminales, Copias de seguridad actualizadas, etc. A su vez hace referencia a las pruebas y seguros detallándolos de la siguiente manera:

- **Pruebas**

  Validez de las copias de seguridad.

Formación y reciclaje del personal.

- **Seguros**

  Asegurar los equipos informáticos

Lo mencionado anteriormente fue expuesto por (Lopez, 2005).

5.7. ANÁLISIS Y EVALUACIÓN DE RIESGOS.

Son procedimientos que definen cómo una institución continuará o recuperará sus funciones críticas en caso de una interrupción no planeada, también que los sistemas de TI son vulnerables a diversas interrupciones de las cuales describe las siguientes en la investigación de (Granda, 2011):

a) Leves: Caídas de energía de corta duración, fallas en disco duro, etc.
b) Severa: Destrucción de equipos, incendios etc.

Asegura que se dé una interrupción mínima a los procesos de atención al usuario en caso de una interrupción significativa de los servicios que normalmente soportan esos procesos. Así también menciona los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte, hora y actividad.

Existen distintos tipos de contingencias de los cuales los siguientes:

Riesgos Naturales: tales como mal tiempo, terremotos, erupción volcánica, etc.

Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión, transporte, ataque de virus, etc.

Riesgos Sociales: como actos terroristas y desordenes.

Las causas más representativas que originarían cada uno de los escenarios propuestos en el Plan de Contingencias y Seguridad de la Información se presentan en la tabla 1 y la tabla 2, que se observan más adelante.

Tabla 1. Posibles Tipos y Escenarios de Riesgos

CAUSAS	ESCENARIOS
○ Fallas Corte de Cable UTP. ○ Fallas Tarjeta de RED. ○ Fallas IP asignado. ○ Fallas Punto de Switch. ○ Fallas Punto Pacht Panel. ○ Fallas Punto de Red.	I. No hay comunicación entre CLIENTE – SERVIDOR
○ Fallas de Componentes de Hardware del Servidor. ○ Falla del UPS(Sin suministro eléctrico) ○ Ataque de Virus Informático. ○ Sobrepasar el límite de almacenamiento en Disco. ○ Computador de Escritorio funciona como servidor.	II. Falla de un Servidor
○ Accidente ○ Renuncia Intempestiva	III. Ausencia parcial o permanente del personal de Tecnología de la Información.
○ Corte General de Fluido Eléctrico	IV. Interrupción del Fluido Eléctrico durante la ejecución de los procesos.
○ Falla de equipos de comunicación: Switch, antenas, fibra óptica. ○ Fallas en el software de acceso a internet. ○ Perdida de comunicación con proveedores de Internet.	V. Pérdida de servicio de Internet.

FUENTE: Tabla Tomada De La Investigación De (SANTA, s.f.)

Tabla 2. Actividades a Efectuar un Plan de Contingencia

	EMERGENCIA	RESTAURACION	RECUPERACION
OBJETIVO	Limitar el daño	Continuar Procesos Vitales	Recuperar proceso total
ACTUACION	Inmediata	A corto plazo	A medio plazo
CONTENIDO	Evacuación Valoración de daños Arranque de acciones	Alternativas para los procesos vitales	Estrategias para la recuperación de todos los recursos
RESPONSABILIDAD PRINCIPAL	Institución	Usuarios	Unidad de Sistemas

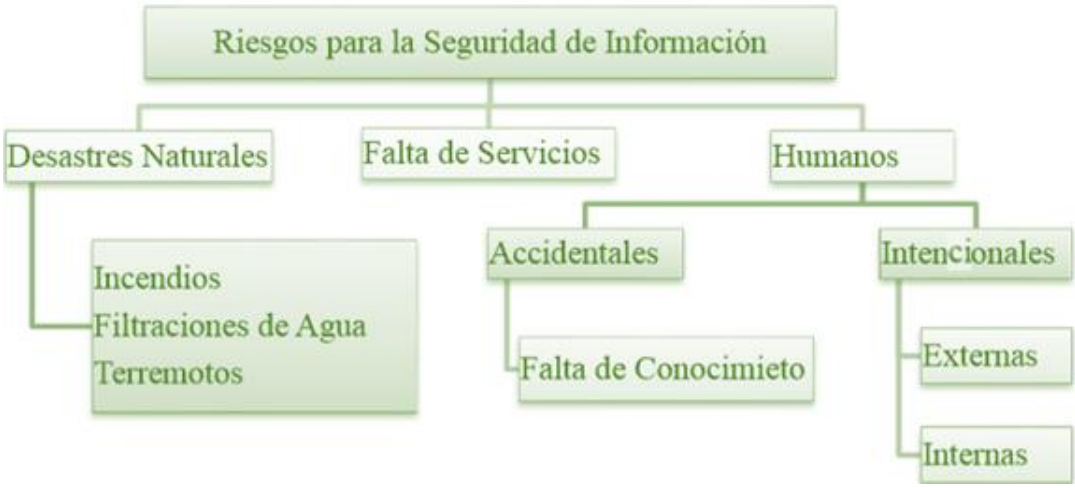
Fuente: Tabla Tomada de la Investigación de (SANTA, s.f.)

5.8. IDENTIFICACIÓN DE EVENTOS QUE PUEDEN CAUSAR INTERRUPCIONES EN LOS PROCESOS.

Vigo (2001) menciona en su investigación que para la identificación de los eventos de contingencia se debe tener la información adecuada de los riesgos críticos, como identificarlos, saber las causas y el impacto que generarían para la institución si llega a materializarse el evento.

Como todas las entidades laborales están expuestas a daños producto de desastres naturales o interrupciones en los sistemas, estas actividades producen pérdidas. En el siguiente diagrama se observa los posibles escenarios de contingencia que pondrían en riesgo la seguridad de la información.

Figura 4. Riesgos para la Seguridad de la Información



Fuente: Diagrama Tomado De La Investigación De (Luna, 2015)

La figura anterior muestra los eventos planteados como un riesgo para la información, están clasificados en tres categorías que plantean específicamente los eventos que pueden ocurrir a cualquier entidad ya sea laboral, educativa o familiar. Así también es necesario resaltar que la categoría de desastres naturales a pesar de tener pocas probabilidades de realizarse es la que tendría un alto impacto en caso de efectuarse, más aun si en Esmeraldas actualmente se están dando varios movimientos telúricos se debe estar preparado para superar la contingencia que se pueda presentar.

5.8.1. EVALUACIÓN DE RIESGOS.

Como lo menciona Martínez(2015) dentro de la evaluación de riesgos se debe identificar, cuantificar y priorizar los riesgos dentro de la organización, estos resultados deben proporcionar la suficiente información para realizar una adecuada gestión de riesgo mediante la implementación de controles de protección. Para la evaluación de riesgos y consecuencias producto de la materialización de una o varias amenazas, se debe realizar el siguiente proceso:

Figura 5. Procesos para la Evaluación de Riesgos

Fuente: Referencia en la investigación de (Luna, 2015)

En el proceso de identificación de riesgos es importante conocer los puntos críticos dentro de la organización, para brindarle la debida atención a cada proceso, no toda la información ni todo proceso van a tener la misma importancia para la organización.

5.8.1.1. VALORACIÓN DE ACTIVOS.

Álvarez (2014) expresa que una vez identificados los activos de mayor relevancia, se procede a la definición de una escala de valoración para cada uno de los activos críticos, puede ser de forma cuantitativa o cualitativa.

Tabla 3. Valoración de Activos

VALORACION DE ACTIVOS				
Valor	**Denominación**	**Disponibilidad**	**Integridad**	**Confidencialidad**
4	Critico	La información, instalaciones y recursos siempre debe estar disponibles. Su pérdida es considerada como Catastrófica para la Institución.	Toda información, instalación o recurso donde la integridad es importante y debe garantizarse Su pérdida seria Catastrófica.	A barca toda información, Instalación o recursos calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
3	Alto	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
2	Medio	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Todo recurso, información o instalación en el cual la integridad es de importancia media y debe garantizarse.	Información, Instalación o recurso calificado como de uso semi restringido. Solo puede ser utilizado por personal interno.
1	Bajo	Este nivel barca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda formación, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes

Fuente: Tomada de la Investigación de (Luna, 2015)

Los criterios que se toman en cuenta para la asignación de activos son los siguientes, así lo menciona en su texto Luna (2015):

- El valor económico que representa.
- Cuando se considere que el activo tiene pérdida de confidencialidad, integridad, disponibilidad.
- El impacto que puede generar para la institución por daños o en su caso suspensión de los servicios.

5.8.1.2. PROBABILIDAD DEL RIESGO.

Martínez (2015) argumenta que un activo aumenta su valor de riesgo cuando necesita más protección, y esto depende de la posibilidad de ocurrencia de una amenaza. Se

determinará en base a estadísticas recogidas, además se tomará en consideración lo siguiente:

- La importancia del activo para la organización.
- La facilidad de explotación de una vulnerabilidad del activo.
- La susceptibilidad técnica de la vulnerabilidad a la explotación.

Tabla 4. Criterio para Análisis de Probabilidad de Ocurrencia del Evento

Denominación	Valor	Control existente (eficiencia)
BAJA	0	Documentado se aplica totalmente.
	1	Documentado y se aplica parcialmente.
MEDIA	2	Documentado pero no se aplica.
	3	Documentado pero da cumplimento total al estándar.
	4	Documentado y da cumplimiento parcial al estándar.
ALTA	5	Documentado pero no da cumplimiento al estándar.
	6	No se evidencia el control.

5.8.1.3. IMPACTO DEL RIESGO.

"Un eventualidad en la seguridad de la información puede afectar a más de un activo dentro de la organización, estos impactos pueden ser inmediatos en el futuro, y provocando pérdidas financieras. El impacto inmediato puede ser directo o indirecto." (Luna, 2015, pág. 59)

- **Directo:** Según lo explica Miranda (2013), este impacto ocurre cuando se necesita el reemplazo del activo perdido, configuración, instalación o copia de soporte, el costo de las operaciones suspendidas debido al incidente hasta volver a las actividades normales.
- **Indirecto**: Se da cuando la afectación genera pérdida, así lo menciona Miranda (2013) por los daños en los equipos o cuando se utilizaron recursos que pudieron usarse en otra parte y los costos por interrupción de las actividades.

Luna (2015), señala que existen diferentes criterios para realizar la valoración de los impactos causados por los diferentes riesgos, depende únicamente de cada organización el definir las consideraciones necesarias para llevar a cabo esta actividad, y se detalla a continuación:

- El grado de afectación o el costo que implicaría para la organización si produce algún daño o la interrupción de un proceso crítico.
- De acuerdo a la importancia de los activos de la institución.
- Las brechas de seguridad que existen tanto a nivel de lógico como físico.
- Las operaciones que se realizan tanto al interior como al exterior.
- El valor financiero para la organización si sufre alguna emergencia.

Tabla 5. Evaluación de Impacto

IMPACTO	VALOR	DESCRIPCIÓN
BAJO	1	Cuando no influye en las labores, y así también los sistemas principales trabajan de manera continua.
MEDIO	2	Cuando las averías son parciales y se dan en los sistemas, sin embargo no influyen en la continuidad de las operaciones.
ALTO	3	Cuando las operaciones, funciones, los usuarios y los sistemas informáticos se ven afectadas impidiendo la continuidad de su funcionamiento.
CRITICO	4	Además la información crítica se perdió, daños severos en los equipos, provocando impedir la continuidad de las labores.

5.8.1.4. DETERMINACIÓN DEL RIESGO.

Los riesgos que tengan alto nivel en probabilidad de ocurrencia y gran impacto dentro de la organización son los que se van a considerar al momento de la elaboración del plan de contingencia. En la figura se puede observar el nivel de riesgo.

Tabla 6. Niveles de Riesgo

PROBABILIDAD						
	5	A	A	C	C	C
	4	M	M	A	A	A
	3	M	M	M	A	A
	2	B	M	M	A	A
	1	B	B	M	A	A
		1	2	3	4	5
	IMPACTO					

Designación de colores:

- El rojo equivale a los riesgos altos y críticos (A y C)
- El amarillo equivale a los riesgos medios (M)
- El verde equivale a los riesgos bajos (B)

5.8.2. Tipos de Análisis de Riesgos.

"Dependiendo del nivel de riesgo en que se encuentre un activo y el grado de vulnerabilidad que este tenga, la estimación para distinguir que clase de riesgo es, y se establece que puede ser cualitativo o cuantitativo." (Luna, 2015, págs. (42, 43))

- **Cualitativo:** Cuando se usan adjetivos basados en las cualidades, mientras demuestren en ese momento que el objeto o sistema analizado puede tener una probabilidad de ocurrencia ya sea alta, media o baja; la utilización de este tipo de riesgo es más sencilla e intuitiva para la investigación, pues hace referencia a una estimación de pérdida.
- **Cuantitativo:** Al hablar de manera cuantitativa se refiere a dar valores numéricos tanto para las consecuencias o para la probabilidad de que dicho suceso ocurra, basándose en un análisis de datos con incidentes anteriores que se produjeron en su momento.

Para un análisis de riesgo siempre deben estar al tanto de las actividades, el personal que dirige y el personal operativo, pues en caso de una emergencia se deben saber cómo mitigar los sucesos de alto riesgo, por esta razón de manera preventiva llevar una documentación es la opción más factible para el buen resultado de un proceso.

Para realizar la asignación de un valor a los riesgos encontrados en la seguridad se debe considerar lo siguiente, así lo aporta en su artículo (Luna, 2015):

Objetivos estratégicos de la organización, políticas.

- Las funciones y estructura de la organización.
- Políticas de seguridad de la información que tiene la institución.

- Enfoque general de la organización hacia la gestión de los riesgos.
- Los activos de información.
- La ubicación y sus características.

6. METODOLOGÍA.

Después de una evaluación sobre el tipo de método al cual se enfoca esta investigación, cabe mencionar que dependiendo de las características planteadas para desarrollar este estudio, se deduce que el método utilizado para esta investigación es el método descriptivo el mismo que se utiliza cuando se describen fenómenos inesperados, tal como se viven en la actualidad, los eventos provocados por la naturaleza. Estos pueden ser longitudinales o transversales, cualitativos o cuantitativos. De manera que se aplicó el método descriptivo, el cual implica observar y describir el comportamiento de un sujeto sin influir sobre él de ninguna manera.

Se aprecia también que este método es empleado para evaluar los hábitos de los usuarios, y saber cómo se puede actuar frente a posibles situaciones en los distintos departamentos en caso de que llegase a ocurrir un evento inesperado (Salkind, 1999).

Se procedió a realizar una síntesis de los datos obtenidos en el estudio para una mayor comprensión mediante el método analítico – sintético, en vista de que se aplicaron pruebas estadísticas para saber cuáles fueron los intereses de una explícita población. Según Salkind (1999) este tipo de investigación estudia a cierto grupo de personas en una población, es decir como para obtener una muestra, con la cual se puede hacer una idea de cómo se encuentra la situación actual de la población en conjunto.

Después del preámbulo necesario para saber cuál fue el tipo de método aplicado para esta investigación, es ineludible mencionar que permitió obtener un estudio para saber cuál es la situación actual del Departamento de TIC frente a un plan de contingencia.

Las fuentes conceptuales sobre el estudio indicado, se realizó a través de: libros digitales, artículos, artículos científicos, blogs científico - universitarios, entre otros. Se redactó el marco teórico del Estudio de Caso con las referencias de autores citados en las diferentes fuentes de consultas los mismos que fueron citadas bajo las normas APA 6ta edición.

Para tener una constancia la toma de los datos utilizados para este estudio se realizó a través de encuestas, las mismas que fueron digitalizadas por medio de aplicaciones herramientas informáticas, tales como: hoja de cálculo de Microsoft Excel, Formularios de Google. Y para el análisis de los datos obtenidos se utilizó el programa estadístico SPSS (Statistical Package for the Social Sciences).

Según Salkind (1999) el SPSS es una potente aplicación de análisis estadísticos de datos, dotada de una intuitiva interfaz gráfica que resulta muy fácil de manejar. Así también explica que la variedad de análisis incluidos es amplia, si bien lleva un cierto retraso respecto a otras aplicaciones en el mercado, en cualquier caso están incluidas las técnicas más habituales.

6.1. POBLACIÓN.

Para el desarrollo de este estudio en el primer periodo académico del 2015, en el que parte la presente investigación, se encuentran 8 trabajadores que conforman el equipo de trabajo en el Departamento de TIC de la PUCESE, los cuales se involucran con esta investigación puesto que las funciones que desempeñan están relacionadas directamente con el tema planteado.

La población que fue considerada para este caso la conformaron las siguientes personas:

Tabla 7. Población para Encuestas

Población	Descripción
1	Jefe del Departamento de TIC's
2	Área de Redes y Comunicación
3	Área de Soporte Técnico
2	Área de Desarrollo de Software

Según los datos adquiridos, la presente investigación no necesita una muestra, ni tampoco una técnica de muestreo: esto se debe a que la población para este estudio solo son 8 personas, razones que indican que no supera el valor estimado para realizar la técnica antes mencionada.

6.2. ANÁLISIS E INTERPRETACIÓN DE LOS DATOS.

Para el análisis de los datos obtenidos mediante las encuestas realizadas a la población perteneciente a esta esta investigación se aplicó el Alfa de Crombach para su respectivo estudio; el Alfa de Crombach es un coeficiente que sirve para medir la fiabilidad de una escala de medida y cuya denominación Alfa fue realizada por Crombach en 1951, tal como lo expresa en su escrito Salkind (1999).

Entre las ventajas de esta medida se encuentra la posibilidad de evaluar cuánto mejoraría (o empeoraría) la fiabilidad de la prueba si se excluyera un determinado ítem.

Como herramienta estadística para aplicar el Alfa de Combrach por medio de SPSS se permitió el análisis estadístico de las encuestas, SPSS es fácil de utilizar e incluye un amplio rango de procedimientos y técnicas para ayudarle a aumentar los ingresos, superar a la competencia, dirigir investigaciones y tomar mejores decisiones que presentan las funciones principales necesarias para realizar el proceso analítico de principio a fin, para mayor comprensión se representa la siguiente tabla con las escalas de correlación y su interpretación.

Tabla 8. Escalas de Coeficientes de Correlación.

Coeficiente	Interpretación
r = 1	Correlación perfecta
0.80 < r < 1	Muy alta
0.60 < r < 0.80	Alta
0.40 < r < 0.60	Moderada
0.20 < r < 0.40	Baja
0 < r < 0.20	Muy baja
r = 0	Nula

Fuente: Tabla Tomada De La Investigación De (Salkind, 1999)

Dentro del análisis estadístico se realizaron Correlaciones Bivariadas, que funcionan como una técnica estadística destinada a averiguar si dos variables tienen relación entre sí, si la relación es fuerte-moderada o débil y que dirección tiene la relación.

6.3. ANÁLISIS DE LA POBLACIÓN.

Para la población designada como primera parte de la investigación se realizaron encuestas a los integrantes del Departamento de TIC's de la PUCESE la misma que tiene 8 preguntas cuyas respuestas fueron utilizadas para recopilar la información necesitada, la encuesta se la puede observar en la sección de Anexos.

El análisis de fiabilidad, del Alfa de Cronbach que se obtuvo en el programa SPSS como se ve en la Tabla N° 9, determinó que el instrumento es aceptable porque dio un resultado >.7, con 8 elementos o variables, que son el número de preguntas que se utilizó en la encuesta.

Tabla 9. Estadísticas de Fiabilidad Depto de TIC's

Alfa de Cronbach	N° de Elementos
,742	8

Para el análisis de frecuencia estadística y correlación bivariada se utilizaron las siguientes variables:

- **Identificación de problemas:** Existe una modalidad para identificar los problemas relacionados con la tecnología de la información.

  Informal: Se identifican problemas de manera informal.
  Documentación Monitoreada: Se identifican problemas mediante un proceso de documentación monitoreado.
  Documentación Automatizada: Se identifican problemas mediante un proceso de documentación automatizado.
  No existe: No existe identificación de problemas.

- **Clasificación de Problemas:** ¿La clasificación de los problemas dentro del departamento de TIC se realiza de acuerdo a los incidentes?

Informal: Se identifican problemas de manera informal.

Documentación Monitoreada: Se identifican problemas mediante un proceso de documentación monitoreado.

Documentación Automatizada: Se identifican problemas mediante un proceso de documentación automatizado.

No existe: No existe identificación de problemas.

- **Registro de Problemas:** ¿Existe una base de datos para registrar los problemas del departamento de TIC
- **Análisis de Problemas:** Se realiza un análisis y seguimiento a los problemas presentados en el departamento de TIC.
- **Plan Solución de Problemas:** Existe un plan para dar solución a los problemas presentados en el departamento de TIC
- **Registro de Cierres:** Se tiene algún registro de cierre sobre problemas solucionados en el departamento de TIC.
- **Plan de Mejora:** Existe un plan de mejora relacionado con las problemáticas en el departamento de TIC.
- **Avance del Dpto. TIC:** Considera que el Departamento de TIC tendría un gran avance si se planifica un Plan de Contingencia.

Con lo referido anteriormente el análisis de frecuencia estadística de la variable que se obtuvo del SPSS, señala claramente en la Tabla N° 10, que la gran mayoría de los integrantes del equipo de trabajo en el Dpto. de las TIC identifican los problemas de manera informal.

Tabla 10. Frecuencias Estadísticas Identificación de Problemas

		Frecuencia	Porcentaje
Válido	Informal	7	87,5
	Documentación Monitoreada	1	12,5
	Total	8	100,0

En la frecuencia estadística que se obtuvo del SPSS de la variable Clasificación de Problemas reveló que, que la clasificación de los problemas dentro del departamento de las TIC ocurre de manera informal, como se ve reflejado en la Tabla N° 11. Esto se debe

a que en las encuestas solo hubo una persona que reflejo en su respuesta una clasificación de problemas mediante una documentación automatizada.

Tabla 11. Frecuencias Estadísticas Calificación de Problemas.

		Frecuencia	Porcentaje
Válido	Manera Informal	7	87,5
	Documentación Automatizada	1	12,5
	Total	8	100,0

El análisis de la frecuencia estadística de la variable Registro de Problemas que se obtuvo del SPSS, como se ve en la Tabla N° 12, describe que si se tiene una base de datos para registrar los problemas en el departamento de las TIC, excepto por una persona encuestada que marco la opción No.

Tabla 12. Frecuencias Estadísticas Registro de Problemas.

		Frecuencia	Porcentaje
Válido	Si	7	87,5
	No	1	12,5
	Total	8	100,0

Por consiguiente el análisis de la frecuencia estadística de la variable Análisis de Problemas que se obtuvo del SPSS, como se ve en la Tabla N° 13, la cual describe que si se realiza un seguimiento a los problemas que se presentan en el departamento de las TIC.

Tabla 13. Frecuencias Estadísticas Análisis de Problemas

		Frecuencia	Porcentaje
Válido	Casi Siempre	5	62,5
	A veces	3	37,5
	Total	8	100,0

Con la variable de Plan de Solución de Problemas el análisis de la frecuencia estadística de la variable se obtuvo como se ve en la Tabla N°14 que los resultados en el SPSS, describen que no se tiene un plan preparado para la solución de los problemas que se presentan a diario en el Dpto. de TIC, por defecto se estipula que las decisiones son dadas

por iniciativas en base a conocimientos que posee el equipo de trabajo que se encuentra en el departamento.

Tabla 14. Frecuencias Estadísticas Plan de Solución a los Problemas

		Frecuencia	Porcentaje
Válido	Si	3	37,5
	No	5	62,5
	Total	8	100,0

Por consiguiente el análisis de la frecuencia estadística de la variable Registro de Cierre del SPSS, como se ve en la Tabla N° 15, la cual describe que si se realiza el cierre o solución de los problemas que se presentan a diario en el Dpto. de TIC.

Tabla 15. Análisis de Frecuencias Registro de Cierre

		Frecuencia	Porcentaje
Válido	Si	7	87,5
	No	1	12,5
	Total	8	100,0

Como siguiente variable está el Plan de Mejora en donde el análisis de la frecuencia estadística del SPSS, como se ve en la Tabla N° 16, obteniendo como resultado que la mayoría de los integrantes del Dpto. de las TIC coinciden con que no se tiene un plan de mejora que ayude a dar una solución óptima a los inconvenientes que se presentan a diario.

Tabla 16. Análisis de Frecuencias Plan de Mejora

		Frecuencia	Porcentaje
Válido	Si	3	37,5
	No	5	62,5
	Total	8	100,0

Como ultima variable para el análisis de la frecuencia estadística del SPSS se tiene el Avance del Dpto. TIC’s, como se ve en la Tabla N° 17, obteniendo como resultado que la mayoría de los integrantes del Dpto. de las TIC opinan que si sería propicio la posibilidad de tener un plan de contingencia aplicado en el departamento de TIC.

Tabla 17. Análisis de Frecuencia Avance del Dpto. TIC's.

		Frecuencia	Porcentaje
Válido	Si	5	62,5
	No	3	37,5
	Total	8	100,0

En el resultado de la correlación bivariada de Pearson que se obtuvo del SPSS, estableció que existe una relación positiva moderada entre las variables Plan Solución de Problemas y Avance Dpto. de TIC, debido a que el valor resultante está dentro del rango de 0.4 a 0.6, como se ve en la Tabla N° 18, es decir que existió una correlación bivariada significativa entre las variables que fueron utilizadas en la encuesta.

Tabla 18. Correlaciones Bivariadas de Pearson

	Plan Solución de Problemas	Avance Dpto. de TIC
Plan solución de problemas	1	,600
Avance Dpto. de TIC	,600	1

7. PROPUESTA DE INTERVENCIÓN.

7.1. ANÁLISIS DE RIESGO.

Para el estudio de este caso se aplicó la técnica de investigación, la cual es:

Entrevista:

Se realizó la entrevista dirigida al Jefe del Departamento de TIC´s, con el propósito de adquirir información relacionada con el análisis de los servicios considerados como críticos ante la posible eventualidad de que un riesgo se pueda presentar, pues como personal administrativo en este departamento, debe estar al tanto de la información necesaria y específica que se necesita obtener para el desarrollo del estudio de caso.

La entrevista está dividida en dos partes:

La primera parte cuenta con 4 preguntas específicas para lograr identificar claramente cuáles serían los servicios tecnológicos críticos que pueden presentar un evento.

La segunda parte de la entrevista está compuesta por una lista de chequeo, la cual sirve como una lista de control de los posibles varios riesgos que se pueden presentar en los servicios tecnológicos brindados por el departamento de TIC´s. Por consiguiente este listado permitió analizar cuáles son los riesgos que presentan más vulnerabilidad para el departamento de TIC´s y considerar las amenazas de alto impacto.

7.1.1. IDENTIFICAR LOS SERVICIOS Y ACTIVOS CRÍTICOS DE TI.

Entrevista realizada al Jefe del Departamento de TIC's de la PUCESE.

Pregunta 1: ¿Qué servicio tecnológicos son críticos?

Respuesta: Los servicios que son considerados críticos para el departamento de TIC´s, pues depende del punto de vista que se lo plantee. Si se habla de la continuidad de los servicios ante una eventualidad inesperada los servicios considerados críticos serian; Moodle, Financiero, Académico, Talento Humano.

Pregunta 2: ¿Qué servicios son necesarios y deben ser levantados inmediatamente después de una catástrofe?

Respuesta: Moodle

Pregunta 3: ¿Cuánto tiempo pueden permanecer inactivos estos servicios?

Respuesta: De ninguna manera. Simplemente no deberían estar inactivos, se trabaja por la continuidad de los servicios.

Pregunta 4: ¿Quién es responsable de cada servicio?

Respuesta: En el departamento los servicios están distribuidos de la siguiente manera:

Área de Redes - Financiero

Área de Base de datos - Académico

Moodle - Complementario, todos participan en el desarrollo

Desarrollador – Páginas Web y varios servicios, excepto administrativos.

Análisis.

Para el Jefe del departamento de TIC´s, uno de los servicios más importantes considerado como crítico ante un evento inesperado es el Moodle, debido a que este servicio necesita disponibilidad continua tanto para estudiantes como para docentes. Por estas razones no debería considerarse la inactividad de este servicio en ningún horario.

7.1.2. IDENTIFICAR AMENAZAS Y VULNERABILIDADES.

Entrevista realizada al Jefe del Departamento de TIC's de la PUCESE.

Tabla 19. Identificación de Amenazas y Vulnerabilidades

CONTROLES	DOCUMENTACION	SI	NO	N/A	OBSERVACION
Inventario	Existe un inventario de los activos y es revisado periódicamente.	X			Pero no es revisado periódicamente
	Existen políticas de seguridad para salvaguardar los equipos.		X		No hay documentos que así lo detallen, pero los guardias de la universidad y personal que labora saben que es prohibido extraer material del departamento. Excepto que esté autorizado.
	Existe una política que impida sacar los servidores del data center.	X			Pero no está documentado. El personal de seguridad de la universidad no dejara que alguien llegue muy lejos en caso de querer extraerse algún objeto
Plan De Mantenimiento	Existen políticas que determinen el mantenimiento de los equipo.	X			No documentada. Pero 1 vez al año realizan las revisiones de los servidores
	Existe un plan de mantenimiento de los servidores.		X		Está en plan de Desarrollo
	Existen listados de los sistemas instalados en los servidores de forma independiente.	X			Los listados están solo para un 50 % de los servidores. Se utilizan formatos de fichas para las listas.

	Existe la documentación de los procedimientos para levantar el s.o. Del servidor.	X			En un 50 % debido a que se manejan también de forma virtual estos procesos.
	Se tiene un procedimiento que se realiza para ejecutar un mantenimiento en los servidores.		X		Por lo cual se está trabajando para efectuarlo, como un sistema de monitoreo.
Sistema Suministro De Energía	Existe una adecuada conexión de los equipos a toma tierra.		X		
	Los servidores cuentan con sistemas de alimentación ininterrumpida.	X			
Plan De Contingencia	Existe un procedimiento para salvaguardar los servidores ante una catástrofe.		X		Pero se tiene respaldos de datos en la nube, y una parte en Quito también.
Control De Acceso	Existe una política de acceso a los servidores.		X		Es conocimiento de los trabajadores
	Se encuentran desactivadas las cuentas de usuario en el servidor que no se están utilizando.	X			Tienen opciones que después de 10 minutos de inactividad se bloquee automáticamente.
	Existen aplicaciones que no son necesarias en los servidores.	X			Debido que no se ha realizado una depuración.
	Los servidores no tienen la configuración por defecto.	X	X		50% si y el otro 50% no. Hace referencia a la respuesta anterior.
	Existe un procedimiento para instalar los últimos parches de seguridad y actualización.	X			Se realizan en su mayoría de manera automática. Pero esta en potencial de mejora este procedimiento.
	Se dispone de una copia de seguridad completa de cada servidor tras una configuración correcta.	X			
	Están activados los registros de actividad (logs) de los servidores y son revisados periódicamente.	X			Pero no son revisados periódicamente

	Los servidores tienen instaladas herramientas que permitan comprobar la integridad en los ficheros del sistema.	X			
	Los mensajes de inicio de sesión están modificados, para evitar que se muestre información sobre la configuración y recursos del sistema.	X			
Respaldo De La Base De Datos	Existen políticas relacionada con los respaldos de la base de datos.	X			Pero no está de manera formal o documentada
	Existe un procedimiento de respaldo de la base de datos.	X			Pero no de manera formal o documentada
	Se encuentra inventariado y etiquetado los respaldos de seguridad.	X			
	El lugar donde se almacenan los respaldos, es seguro.	X			
	Existe un plan para comprobar la eficiencia de los respaldos.		X		
	Existe un registro de incidencias dela restauración del daño de los respaldos.		X		
Cuentas De Usuario	Existen políticas y procesos relacionados con la solicitud, creación, configuración, seguimiento y cancelación de cuentas de usuarios de los servidores.		X		
	Existe documentación que justifique la creación de cuentas de usuario con privilegio administrativo con la autorización de la dirección de sistemas.		X		
	Existe en las políticas las revisiones periódicas sobre la administración de las cuentas.		X		

	Existe un proceso para detectar actividades no autorizadas, como conexiones a horas extrañas o desde equipos que no se habían contemplado inicialmente.		X		
	Existen procedimientos para detectar cuentas inactivas en un periodo determinado.		X		
Identificación Y Autenticación De Usuarios					
	Existe un tiempo de caducidad para la contraseña.	X			En los servidores si
	Existe un registro historial de contraseñas, para impedir que puedan volver a ser utilizadas.		X		
	Existen políticas que determinen la composición de una contraseña.		X		De manera formal no. Pero se aplica la modalidad de clave segura que contiene: letras, números, mayúsculas, minúsculas y caracteres especiales.
	Existe algún mecanismo de bloqueo de cuentas tras varios intentos fallidos de autenticación.	X			Dependiendo del sistema.
	Existe un procedimiento a efectuar, en caso de que la contraseña sea adquirida por terceros.		X		
	Existe un proceso que impida utilizar la misma contraseña en varios sistemas.		X		
	Existe una política que exija el cifrado del fichero que contiene las contraseñas.	X			En una Base de Datos.
	Existe un registro de las sesiones iniciadas por usuarios así como también los intentos fallidos.		X		Pero depende del Servidor, para servidores de respaldos sí
	Existen mecanismos que eviten a un usuario acceder a datos o recursos con derechos distintos de los autorizados.	X			

Autorización Y Control De Acceso Lógico	Existe una política de control de acceso de servicios en los servidores.		X		Nada formal o documentado
	Existen grupos definidos de usuarios que permitan un mejor acceso a los datos y aplicaciones.		X		En desarrollo
	Existe un mecanismo para restringir los derechos y privilegios administrativos de los usuarios.		X		En desarrollo
	Existe un control para registrar los intentos de acceso fraudulentos a los datos, ficheros y aplicaciones del sistema informático.		X		En desarrollo
	Existe algún procedimiento que ayude a descubrir la autoría de los intentos fraudulentos.		X		En desarrollo
Monitorización De Servidores Y Dispositivos De La Red	Existen políticas de seguridad que faciliten la detección de intentos de ataques contra los servicios críticos.		X		
	Existen "logs" que permita registrar las sesiones iniciadas por los usuarios en los servidores.	X			
	Existe un sistema de monitoreo que permita enviar alarmas cuando existan incidentes.		X		
	Existe la revisión de "logs", cada que tempo, que medidas toman.		X		
	Existe una política en la cual se informe sobre "logs" a los empleados.		X		

Fuente: Propia de la Investigación.

7.1.3. EVALUACIÓN DEL RIESGO.

La evaluación de los riesgos se realiza mediante el análisis de las vulnerabilidades en los servicios críticos, para la definición de la probabilidad de ocurrencia se hace referencia a la tabla anterior; entre los criterios de evaluación a considerar están, la importancia que tiene el activo para el departamento, la disposición de aplicación de una vulnerabilidad del activo y que tan susceptible este la vulnerabilidad.

Tabla 20. Evaluación de Riesgos.

SERVICIO/PROCESO CRITICO	ACTIVO	EVENTO	TIPIFICACIÓN DEL RIESGO	RIESGO DEL ACTIVO
SISTEMA DE MOODLE	SERVIDOR MOODLE	Robo	R1	Medio
		Errores de Mantenimiento y actualización de equipos	R2	Medio
		Falla de sistema de suministro de energía	R3	Alto
		Catástrofe (Incendio/ Terremoto/Maremoto)	R4	Alto
	SISTEMA WEB MOODLE	Acceso no autorizado y Manipulación de la configuración	R5	Medio
		Errores de Mantenimiento y actualización de programas	R6	Bajo
		Falta de Manual técnico	R7	Medio
		Falta procedimiento para detectar contraseñas inactivas	R8	Medio
		Caída del sistema por agotamiento de recursos informáticos	R9	Medio
	BASE DE DATOS MOODLE (MySQL)	Errores de Mantenimiento y actualización de datos	R10	Medio
		Falla de respaldo de la base de datos	R11	Bajo

		Falta de plan para eficiencia de los respaldos	R12	Alto
		Caída del sistema por agotamiento de recursos informáticos	R13	Medio
		Falta de Licencia legal	R14	Bajo
	SISTEMA OPERATIVO CENTOS 6 - 32 BITS	Acceso no autorizado y Manipulación de la configuración	R15	Bajo
		Instalación no autorizada de software	R16	Bajo
		Errores de Mantenimiento y actualización de programas	R17	Medio
		Falta de Manual técnico	R18	Alto
		Caída del sistema por agotamiento de recursos informáticos	R19	Medio
SISTEMA FINANCIERO	SERVIDOR FINANCIERO	Acceso no autorizado y Manipulación de la configuración	R20	Medio
		Falla de sistema de suministro de energía	R21	Alto
		Robo	R22	Medio
	BASE DE DATOS PUCESE-SERVER – Pucsedb	Falta procedimiento para detectar contraseñas inactivas	R23	Medio
		Falta de plan para eficiencia de los respaldos	R24	Alto
		Modificación o alteración de la información(red de datos)	R25	Alto
	SISTEMA OPERATIVO WINDOWS	Acceso no autorizado y Manipulación de la configuración	R26	Medio
		Instalación no autorizada de software	R27	Bajo
		Falta de Manual técnico	R28	Alto

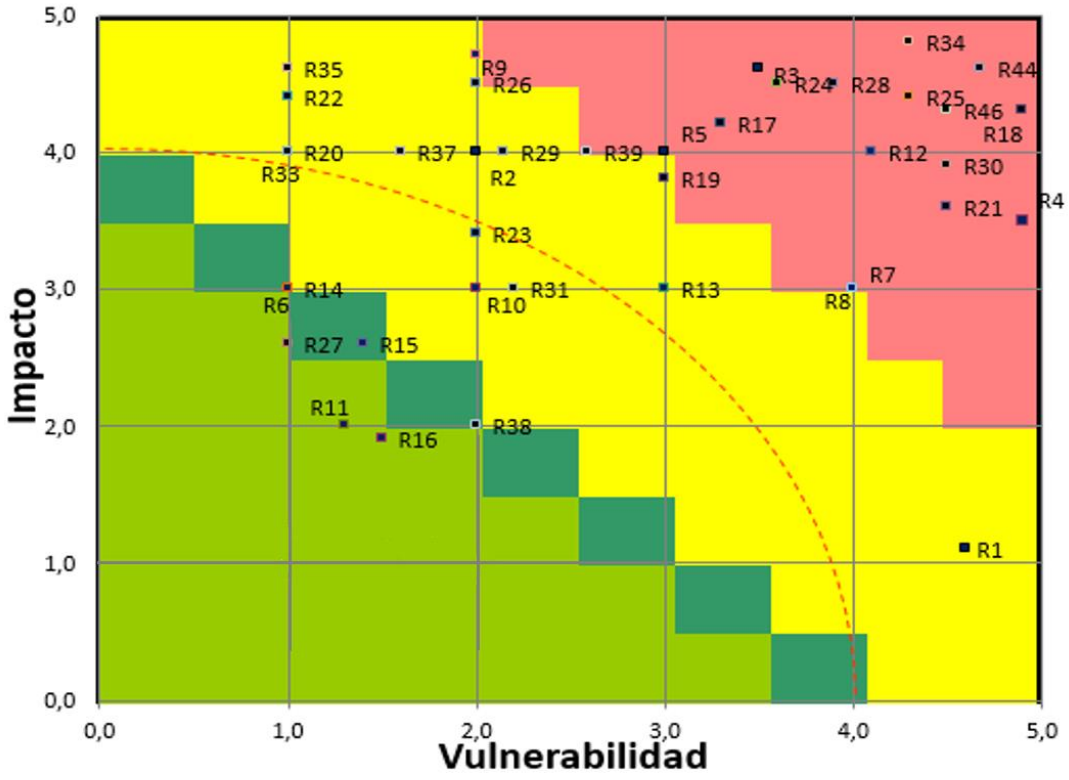
SISTEMA ACADÉMICO	SERVIDOR DE BDD SQL SERVER 2008	Errores en la configuración y Errores del administrador	R29	Medio
		Políticas sobre el uso de los servicios de red	R30	Alto
		Equipo de Usuario desatendido	R31	Medio
		Robo	R32	Bajo
	BASE DE DATOS ACADÉMICO	Falla de respaldo en la base de datos	R33	Medio
		Registro de sesiones de ingresos de usuarios o intentos fallidos	R34	Alto
		Acceso no autorizado y Manipulación de la configuración	R35	Medio
	SISTEMA OPERATIVO WINDOWS	Robo	R36	Medio
		Caída del sistema por agotamiento de recursos informáticos	R37	Medio
		Falta de Licencia legal	R38	Bajo
SISTEMA DE TALENTO HUMANO	BASE DE DATOS SQL – SERVER	Falla de respaldo en la base de datos	R39	Medio
		Falta de Licencia legal	R40	Bajo
	SERVIDOR SQL SERVER 2008	Falta de controles contra código malicioso	R41	Medio
		Robo	R42	Bajo
		Acceso no autorizado y Manipulación de la configuración	R43	Medio
		Falla de sistema de suministro de energía	R44	Alto
	SISTEMA OPERATIVO WINDOWS	Instalación no autorizada de software	R45	Bajo
		Falta de Manual técnico	R46	Alto
		Acceso no autorizado y Manipulación de la configuración	R47	Medio
		Falta de Licencia legal	R48	Bajo

7.1.4. MATRIZ DE RIESGO.

La matriz de riesgo que se observa en la siguiente gráfica muestra el impacto que tiene cada riesgo, de acuerdo a los resultados del cuadro anterior. En la gráfica de la matriz se consideran para el eje de la "x" los valores de la vulnerabilidad que presente el evento; para el eje de la "y" los valores del impacto que puede causar el evento en caso de plasmarse a la realidad.

Los eventos que resalten su ubicación después de la curva que se observa con líneas entre cortadas, son los que tuvieron valoraciones altas en la evaluación hecha previamente.

Figura 6. Gráfica de Matriz de Riesgos



7.2. ANÁLISIS DE RESULTADOS.

En esta etapa de la investigación ya se tiene conocimiento de los procesos tecnológicos que tienen un nivel crítico, alto, también los que pueden afectar y provocar que se necesite el plan de contingencia de TIC's.

De acuerdo a los resultados los siguientes eventos que tienen un valor alto son:

Tabla 21. Análisis de Resultados

Amenazas	Recomendación
Falla de sistema de suministro de energía (R3, R21, R44)	Se debería tener un sistema ininterrumpido de energía eléctrica con el propósito de proveer en todo momento un suministro eléctrico.
Modificación o alteración de la información. (Red de datos) (R25)	Se debería controlar los derechos y privilegios de acceso, asumiendo la responsabilidad de garantizar la integridad de la información**.**
Falta de Manual técnico (R18, R28, R46)	Se debería tener un documento que tenga información de las especificaciones técnicas para posteriormente de un incidente poner en marcha la aplicación.
Políticas sobre el uso de los servicios de red (R30)	Se deberían crear políticas para controlar el uso de los servicios de red. De manera que se pueda recibir las notificaciones detalladas, en especial cuando ocurran accesos no autorizados. (fecha, hora, lugar)
Falta de plan para eficiencia de los respaldos (R12, R24)	Se debería tener un plan para eficiencia de los respaldos, de manera que la verificación de funcionalidad de los respaldos sea controlada.
Registro de sesiones de ingresos de usuarios o intentos fallidos (R34)	Se debería tener una política que describa un control para saber en qué horario ingresan los usuarios y el número de veces que tuvieron intentos fallidos
Catástrofe/Terremoto/Tsunami (R4)	Considerar la posibilidad de tener un sitio alterno para los servicios de ti y los demás servicios

7.3. DESARROLLO DEL PLAN DE CONTINGENCIA DE TIC´S.

Para el desarrollo del plan de contingencia de TIC'S, se debe tener:

- Equipos organizados para efectuar el desarrollo del Plan.
- Asignar las tareas que cada uno de los equipos deba realizar.
- Cada equipo debe tener claro las dependencias orgánicas entre ellos.
- Los procedimientos de alerta ante eventos que puedan dar inicio al Plan.
- Instrucciones de acción ante eventos inesperados.
- Para vuelta a la normalidad, tener una estrategia.

7.4. ORGANIZACIÓN DEL EQUIPO.

Esta etapa del plan de contingencia depende de cada institución, sin embargo es de mayor seguridad tener una previa planificación de cómo distribuir al personal que labora diariamente. Es recomendable que dentro del personal designado se encuentren personas de inspectoría en la institución, en conjunto con el personal del área informática; debiendo crear claras funciones, responsabilidades y objetivos, para actuar inmediatamente cuando se presente un escenario de riesgo. A continuación se detallan especificaciones para organizar el equipo.

7.4.1. ROLES Y RESPONSABILIDADES.

Los equipos designados para activar y aplicar el plan de contingencia de TIC's, son el personal clave al momento de ocurrir una emergencia, cada uno tendrá su función específica para efectuar el plan. El número de personas que conformen el equipo varía dependiendo de cómo se solicite y acorde a la estrategia que tengan, a continuación se ejemplifican los equipos que pueden formar el Plan como lo menciona.

Una persona puede pertenecer a más de un equipo, siempre y cuando no interfieran sus actividades para integrarse en ambos. El personal o cantidad de miembros que tenga cada equipo va a depender del tamaño de la organización y la táctica que se esté aplicando para

la recuperación de los servicios. A continuación se describen la distribución de equipos, según lo sugiere (Alvarez, 2014):

- **Equipo Director o Comité de Crisis.**

Este comité es designado para dirigir durante una contingencia y recuperación de los servicios. El principal propósito de este equipo o persona, es reducir de manera preventiva las posibles eventualidades de riesgo que se puedan presentar; también toman las decisiones claves, manteniendo siempre informados a la directiva principal de la institución sobre cualquier situación. Y como una de las decisiones más importantes de este equipo está el activar el Plan de Contingencia de TIC's, para iniciar rápidamente el proceso de notificación a los compañeros de trabajo.

- **Equipo de Recuperación.**

Como función restablecen todos los sistemas necesarios (voz, datos, comunicaciones, etc.). Este equipo debe estar en capacidad de establecer la estructura para la recuperación de todo lo que incluya el departamento, es decir servidores, ordenadores, comunicación de voz y datos, entre otros elementos necesarios para la infraestructura de un servicio tecnológico.

- **Equipo Logístico.**

Su tarea está basada en toda la logística necesaria para la recuperación. Es decir que este equipo debe tener conocimiento de cómo realizar el transporte de material o personal (en caso necesario), debe adquirir los suministros de oficina, tener los contactos con proveedores, realizar trámites administrativos para el departamento y lo más importante es que debe trabajar en conjunto con los demás equipos para que las necesidades logísticas sean cubiertas en su totalidad.

- **Equipo de las Unidades del Departamento.**

Realizan las pruebas que verifiquen la recuperación de los sistemas críticos. Es decir que en este equipos estará el personal apto para realizar las pruebas de funcionalidad para verificar las aplicaciones críticas, la operatividad de los sistemas, así también la puesta en marcha de los mismos.

- **Equipo de Relaciones Públicas.**

Encargado de las comunicaciones a las personas involucradas y si amerita el caso a medios de comunicación. Toda institución, departamento u organización dependen de un sector que es considerado como el más importante para su desarrollo y son los clientes (o en su caso los usuarios); es así que este equipo debe ser el que estricta y cautelosamente debe mantenerlos informados. Si es necesario también deberá contactarse con los medios de comunicación. Este equipo es creado con el principal objetivo de que la información se emita de una sola fuente y evitar confusiones.

Una vez descrito el papel que debe desempeñar cada equipo, a continuación se observa la siguiente tabla donde se muestran los responsables en cada caso de manera formal, en relación con el departamento de TIC's. (Alvarez, 2014)

7.4.2. ASIGNACIÓN DE ROLES.

Tabla 22. Roles

Rol	**Responsable**
Equipo Director o Comité de Crisis	Jefe del Departamento de TIC's Comisión Administrativa Financiera: • Pro rector (Coordinador) • Jefe del Departamento Financiero • Jefa de RRHH
Equipo de Recuperación	Jefe de Seguridad y Salud Ocupacional Jefe del Departamento de TIC's
Equipo Logístico	Jefe del Departamento de TIC's Jefe de Adquisiciones
Equipo de las Unidades de Departamento o Negocio	Jefe del Área de Redes y Comunicación Jefe del Área de Soporte Técnico Jefe del Área de Desarrollo de Software
Equipo de Relaciones Publicas	Jefe de los Distintos Departamento de la PUCESE

7.4.3. FICHAS PARA LA ORGANIZACIÓN DE LOS EQUIPOS.

Los equipos son los encargados de poner en marcha todo el proceso para el levantamiento de los servicios críticos afectados por la contingencia, es por estas razones que uno de los pasos también importantes en este proceso es la realización de Fichas que contengan los datos necesarios para contactarse con cada uno de los miembros que conforman los equipos.

Como se observa a continuación las fichas deben tener la siguiente información:

Tabla 23. Formato de Fichas para la Organización de Equipos

INTEGRANTES DEL EQUIPO (nombre del equipo)	
RESPONSABLE DEL EQUIPO	
Nombre:	
Cargo:	
Función:	
Teléfono Celular:	
Teléfono Casa:	
Dirección Casa:	
MIEMBROS DEL EQUIPO	
Nombre:	
Cargo:	
Función:	
Teléfono Celular:	
Teléfono Casa:	
Dirección Casa:	
BACKUPS DEL EQUIPO	
Nombre:	
Función:	

Reemplaza a:	
Teléfono Celular:	
Teléfono Casa:	
Dirección Casa:	

Fuente: Tomada de la investigación de (Alvarez, 2014).

7.5. DESARROLLO DE PROCEDIMIENTOS.

Una vez establecidos los equipos y se han designado las funciones que debe desempeñar cada uno, se tiene que desarrollar los procedimientos que van a seguir, y su actuación en cada una de las etapas de activación del Plan de Contingencia de TIC's.

7.5.1. ETAPA DE ALERTA.

Esta etapa está divida en tres partes que son: Notificación – Evaluación - Ejecución del Plan. Aquí se definen los procedimientos ante la ocurrencia de un suceso que genera una perdida ya sea parcial o total de uno o varios servicios críticos.

7.5.1.1. Notificación.

Como parte del plan de alerta se debe tener un programa de concientización, para informar al personal de cómo debe actuar ante casos donde se encuentren con una contingencia o un incidente que sea considerado catastrófico y por consiguiente saber a quién debe comunicar lo ocurrido.

Tabla 24. Etapa de Alerta: Notificación

	Incidente	Acción
1	Algún empleado detecta un evento de contingencia o incidente en el departamento. (Fuego, inundación, Virus, Robo, etc.).	Se informa rápida y detalladamente al responsable del personal de turno o de seguridad

2	El responsable de turno o el de seguridad ya tiene conocimiento de lo ocurrido.	Aviso a la persona del comité de Crisis	Aviso a emergencia (si procede)

7.5.1.2. Evaluación.

Ahora que el personal de comité de crisis fue informado del evento, pues procede a recopilar información para realizar la evaluación de la situación. También tendrán la obligación de informar a los responsables de los distintos equipos lo ocurrido, para estar a la espera de que se tome la decisión de ejecutar el plan o a su vez tomar otro tipo de solución más rápida al inconveniente.

Tabla 25. Etapa de Alerta: Evaluación

	Incidente	**Acción**
3	Algún miembro del comité de crisis es enterado del evento ocurrido.	En un lugar determinado por el comité de crisis tendrán la respectiva reunión para evaluar lo ocurrido, y así tomar la decisión de activar o no el plan de contingencia.
		Los responsables de cada equipo deberán estar informados de la situación, es decir los mencionados continuación: -Responsable de seguridad. -Comité de Dirección de la institución. -Relaciones públicas. -Equipo de recuperación. -Responsable de los equipos.

7.5.1.3. Ejecución del Plan.

Cuando el comité decide poner en marcha el plan de contingencia, se da inicio al árbol de llamadas a cada responsable y miembros del equipo, para informar la situación y

empezar con las actividades que le corresponden a cada uno. El árbol de llamada queda planteado de la siguiente manera:

Figura 7. Árbol para Ejecución del Plan

Fuente: Tomada de la investigación de (Alvarez, 2014)

Tabla 26. Etapa de Alerta: Ejecución del Plan

	Evento	**Acción**
4	El Comité de Crisis decidió activar el plan de contingencia	Dar inicio al árbol de llamadas Informar a la Dirección de todo.
5	Pasos para la etapa de transición	

7.5.2. *ETAPA DE TRANSICIÓN.*

Esta es la etapa previa para recuperación de los sistemas o infraestructura tecnológica. Lo más recomendable es que en esta etapa el coordinador de cada equipo debe estar al tanto de todo lo que está disponible para comenzar con la recuperación en el tiempo más corto posible. Esta etapa está dividida en dos partes:

- **Procedimiento de concentración y traslado de personas y equipos.**

  La solución decidida como estrategia de respaldo puede variar. Una vez que se ha dado a los equipos el respectivo aviso y se ha puesto en marcha el plan de contingencia, si se dio el incidente en horas de trabajo se procede a la reunión en el

lugar donde se designó, pero si no se encuentran en horas laborables el lugar sería elegido por la Dirección del Comité de Crisis.

También se debe tener en cuenta que se debe tener una importante labor de coordinación para el traslado de todos los materiales necesarios para poner en marcha el centro de recuperación (como por ejemplo, cintas de backup, material utilizados en las oficinas, documentación en caso de tenerla, etc.)

- **Procedimiento de puesta en marcha del centro de recuperación.**

Como se tienen los equipos ya en el centro de recuperación, contando con todos los elementos necesarios y actualmente disponibles, se empieza con el establecimiento de la infraestructura ya sea esta de hardware, software, de comunicación, etc.

Tabla 27. Etapa de Transición

	Evento	Acción
6	Concentración y traslado de personas y equipos	
7	Puesta en marcha del centro de recuperación	

Los procedimientos anteriormente detallados son la base para la etapa de recuperación de los sistemas. En caso de que uno de los procedimientos anteriores, falle, no será posible comenzar la recuperación y por consecuencia el plan de contingencia fallará.

7.5.3. ETAPA DE RECUPERACIÓN.

Cuando ya se tiene la bases listas para empezar el proceso de recuperación, se procede a cargar los datos y a la restauración de los servicios críticos. Esta etapa y la anterior se caracterizan por ser las más difíciles ya que requieren gran esfuerzo e intervención de todos los miembros de los equipos para cumplir con los plazos fijados. Está dividida en dos partes:

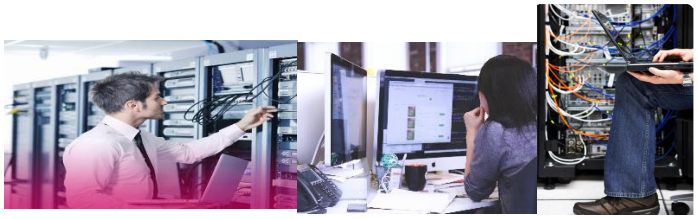
- **Procedimientos de Restauración.**

  En esta parte se realizan las actividades para restaurar los sistemas críticos.

- **Procedimientos de Gestión y Soporte.**

  En esta parte cuando se tienen los sistemas restaurados, se comienza a comprobar el funcionamiento de cada uno, se realiza el mantenimiento para protegerlos, para estar seguros que se podrán reanudar las actividades con las máximas garantías de éxito. Por último se realizan las pruebas y verificación del correcto funcionamiento de todo, eso le corresponde al Equipo de Unidad del Negocio.

Tabla 28. Etapa de Recuperación

	Evento	Acción
7	Procedimientos de Restauración	
8	Procedimientos de Gestión y Soporte	

7.5.4. ETAPA DE VUELTA A LA NORMALIDAD

Ahora con la correcta ejecución de los procesos críticos y que se haya solucionado la contingencia, se comienza con el proceso para plantear las estrategias y acciones para recuperar el funcionamiento con normalidad total. Esta etapa está dividida en los siguientes procedimientos:

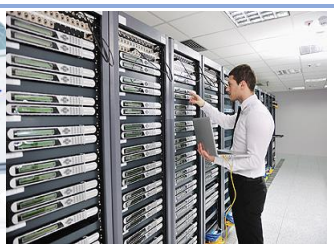
- **Análisis de impacto.**

  En este proceso se realiza el análisis de los equipos e instalaciones, lo cual me permita diagnosticar las que estén dañadas y así definir una estrategia de vuelta a la normalidad.

- **Procedimiento de vuelta a la normalidad.**

  Ya definido el impacto, se deben establecer los mecanismos que me permitirán recuperar la normalidad total de las funciones. Esto incluye la adquisición de nuevos equipos, mobiliario, material múltiple, etc.

Tabla 29. Etapa de Vuelta a la Normalidad

	Evento	Acción
9	Análisis de impacto	 
10	Procedimiento de vuelta a la normalidad.	 

7.5.5. GENERACIÓN DE INFORMES Y EVALUACIÓN.

Después de solucionado el incidente y ya ejecutada la etapa de vuelta a la normalidad, todos los equipos tendrán que presentar un informe con todas la acciones que se vieron en la obligación de realizar, y deben detallar si se realizó el cumplimiento de los objetivos según el Plan de Contingencia de TIC's.

También puntualizar los tiempos empleados para cada procedimiento, las dificultades que se presentaron, etc. Todo esto con la finalidad de obtener la información necesaria para valorar si el Plan de Contingencia funciono según lo planificado, o si existieron fallos durante el desarrollo para tomarlos en cuenta para un mejoramiento del mismo.

Tabla 30. Generación de Informes y Evaluación

	Evento	Acción
11	Informes y evaluación	 

7.6. SELECCIÓN DE ESTRATEGIAS.

Las estrategias que se tienen al momento de presentarse una contingencia deben estar ya planteadas por el Equipo de Dirección (Equipo de Comité de Crisis) al momento de realizar el Plan de Contingencia. Las estrategias dependerán de los recursos que se dispongan, cabe mencionar que la selección de estrategias permitirán mitigar el impacto

que genere la posible interrupción de los servicios, a continuación se detallan posibles estrategias:

Tabla 31. Selección de Estrategias.

Estrategia	Sugerencia para Estrategia	Ciudad
a) Departamento de Computo Alterno – Oficinas.	Colegio Fiscal "Sagrado Corazón"	Esmeraldas
b) Departamento Alterno de Operaciones Técnicas.	Gobierno Autónomo Descentralizado De La Provincia De Esmeraldas (GADPE).	Esmeraldas
c) Matriz de la institución	Pontificia Universidad Católica del Ecuador (PUCE)	Quito
d) Proveedor(es) de equipos – Autorizados por el Comité de Crisis	Proveedores Propios de la Institución	Esmeraldas, Quito, Guayaquil

7.7. ESCENARIOS CRÍTICOS.

7.7.1. PRIMER ESCENARIO.

El primer escenario es considerado de incidencia menor dentro del Departamento de TIC's:

1. Escenario de incidencia menor que impide el funcionamiento de varias operaciones que brinda el departamento:
    a. Desconfiguración parcial ya sea física o lógica de algún servidor (correo, impresión, sistemas utilizados por la institución, archivos electrónicos, servidores).
    b. Desperfecto parcial en la parte física o lógica de alguno de los equipos de virtualización.
    c. Daño parcial en la parte física o lógica en los componentes de la red.
    d. Fallas en alguno de los equipos de comunicaciones alternas.

e. Caída del proveedor de servicios principal.

2. Si existe acceso al Departamento de TIC.

7.7.1.1. ESTRATEGIAS DE RECUPERACIÓN.

1. En este escenario de incidencia menor a equipos, servidores, dispositivos de comunicación, componentes de red, etc., se ubica un reemplazo para dichos equipos con fallas. Si el caso es más grave y tome más tiempo solucionarlo, se empieza con las actividades del equipo de recuperación, las cuales están detalladas en la etapa 3 del desarrollo del plan de contingencia.
2. El Equipo Dirección (Comité de Crisis) debe ser notificado del incidente y de la solución que se está dando al incidente menor, para que se haga un correcto desarrollo del proceso de recuperación.
3. En caso de ser un fallo con el proveedor principal de comunicaciones, se debería tener listo el contacto que me permita ubicar al proveedor alterno para que tome control inmediato. (Los proveedores alternos deben estar en el listado realizado por el Equipo de Logística, aplicando la etapa 3 del Desarrollo del Plan).
4. Si el daño es de hardware, se contacta a los proveedores para ejecutar garantías si es necesario, o realizar el soporte y mantenimiento.
5. Si el inconveniente es con la red inalámbrica de algún dispositivo, se procede a trabajar con las redes inalámbricas configuradas disponibles.

La recuperación de los servicio para este primer escenario, puede tardar un tiempo estimado de **horas** o puede ser **inmediato**, esto depende de las condiciones y plazos establecidos por el Equipo del Comité de Crisis.

7.7.1.2. RECURSOS.

Tabla 32. Recursos en Primer Escenario

Recursos Técnicos	Recurso Humanos
Departamento de TIC's	• Personal Técnico Informático. • Jefe del Área de Redes y Comunicación

	• Jefe del Área de Desarrollo de Software • Jefe de Adquisiciones

7.7.2. SEGUNDO ESCENARIO.

El Segundo escenario es considerado cuando se presentan incidencias mayores ya sea en los servicios o para el personal del Departamento de TIC's.

1. Incidente para el Departamento de TIC's con un nivel de inoperatividad mayor, que llegue a suspender servicios que este brinda:
    - Avería de nivel físico o lógico en alguno de los servidores (correo, BPM, archivo electrónico, telefonía).
    - Avería de nivel físico o lógico en alguno de los equipos de virtualización.
    - Avería de nivel físico o lógico en alguno de los componentes de la red.
    - Avería de nivel físico o lógico en alguno de los equipos de comunicaciones alternas.
    - Daño físico o lógico en alguno de los UPS, incendios o aire acondicionado.
2. Aún existe acceso al Departamento de TIC's.

7.7.2.1. ESTRATEGIAS DE RECUPERACIÓN.

1. Ya sea en servidores, dispositivos de comunicación, componentes de red y demás; si el daño es **irreparable,** se tendría que acudir al departamento alterno que este seleccionado con anterioridad por el Equipo de Dirección (Comité de Crisis), para que se tome el control de la red y de los recursos en el ambiente de contingencia presentado. Se dan inicio a las actividades de la Etapa de Recuperación inmediatamente.
2. Al ser un daño con el proveedor principal de las comunicaciones, la institución debe aplicar una de las estrategias, contactándose con uno de los proveedores alternos para que el mismo tome control automático de la situación. (El Comité de Crisis debe elegir el Proveedor Alterno y por consiguiente el Equipo de Logística tendrá el Listado para realizar los contactos)

3. Si el daño de comunicación es mayor pero si hay posibilidad de comunicación con el proveedor principal, se contacta urgente para reparación y monitoreo. (Equipo de Logística tiene Listado, debe realizar los contactos)
4. Si el daño es mayor o irreparable en el hardware de los equipos, se contacta de manera urgente a los proveedores para ejecutar el proceso de garantía, o a su vez el contrato de nuevas equipos.
5. Si el caso es necesario se levantarán respaldos de información y se montará en un servidor alterno para restaurar la aplicación.

El **tiempo para dar soluciones** las incidencias mayores, tiene probabilidades bajas de solución inmediata, pero si está estimado en **horas** o máximo **varios días** para resolverlo.

7.7.2.2. RECURSOS.

Tabla 33. Recursos en Segundo Escenario

Recursos Técnicos	Recurso Humanos
• Departamento de TIC's • Departamento de Computo Alterno - Oficinas	• Jefe del Área de Redes y Comunicación • Jefe del Área de Soporte Técnico • Jefe el Área de Desarrollo de software • Jefe de Adquisiciones

Para el Departamento de TIC's se consideran los siguientes servicios ya sea de forma individual o mixta:

A. Para las bases de datos el servicio debe ser íntegro, para cualquier aplicación que se encuentre en ambiente de contingencia.

B. Solo para las personas que estén registradas en la lista de los equipos organizados para activar el plan, se les proveerá el servicio de correo electrónico.

C. Se debe tener el servicio de enlace con el Centro Alterno (Área de Tecnología de la PUCE), en caso de que el departamento actual sea dado de baja y se notifique

oficialmente el paso a ambiente de contingencia. Decisión del Equipo de Dirección (Comité de Crisis).

7.7.3. TERCER ESCENARIO.

El tercer escenario presenta las siguientes situaciones:

1. Se tienen circunstancias de incidentes dentro del Departamento de TIC's.
2. Se tienen incidentes externos que impiden el ingreso a la institución.

7.7.3.1. ESTRATEGIAS DE RECUPERACIÓN.

1. El Equipo de Dirección (Comité de Crisis) consciente del desastre que enfrentan. Debe poner en alerta a los responsables de cada equipo para dar la orden de comenzar las actividades en el sitio alterno designado. Ejecución de la Etapa 1 del plan, detallada anteriormente.
2. Se da inmediato traslado del personal para hacer uso de las oficinas – del Departamento de Cómputo Alterno y procedan con la instalación de los equipos para restablecer las operaciones. Ejecutando las Etapa 2 del plan detalladas anteriormente.
3. El equipo de Logística debe ponerse en contacto con el Proveedor de Equipos Autorizado por el Comité de Crisis, para solicitar las adquisiciones necesarias para equipar el Departamento de Cómputo Alterno. Para el buen resultado de este proceso el Equipo de las Unidades del Departamento debe trabajar en conjunto con el Equipo de Logística, facilitando un listado de lo necesitado.
4. El lugar alterno debería tener los equipos básicos, respaldos de la información, programas, manuales etc., para así restaurar la información de la base de datos, programas en los equipos alternos y realizar el levantamiento de los servicios. Ejecutando la etapa 3 del plan, detallada anteriormente.
5. Se comprueba que la información se encuentre integra y completa, si es posible considerarlo hasta el punto antes del evento. Y se proceder a reanudar las operaciones; por parte del Equipo de Dirección o el Equipo de Relaciones Publicas se procede a informar a los usuarios y autoridades correspondientes la normalidad de los servicios.

En este escenario es clave monitorear la Etapa de Recuperación, pues un error en esta etapa puede impedir el levantamiento de las actividades con normalidad.

7.7.3.2. RECURSOS.

Tabla 34. Recursos en Tercer Escenario

Recursos Técnicos	Recurso Humanos
• Departamento de Computo Alterno • Matriz de la Institución	• Jefe del TIC's • Jefe de Adquisiciones • Jefe del Departamento Financiero • Jefe de Seguridad y Salud Ocupacional • Jefe del Área de Redes y Comunicación • Jefe del Área de Soporte Técnico • Jefe del Área de Desarrollo de Software • Jefe de los Distintos Departamento de la PUCESE

El tiempo considerado para el restablecimiento de los servicios en el sitio alterno está considerado de días hasta un máximo de semanas para culminar con el levantamiento del nuevo Departamento de TIC's.

7.8. PROCESOS PARA EL PLAN DE CONTINGENCIA.

A continuación se detallan los procesos que permitirán realizar el Plan de Contingencia en su totalidad, para efectuarlo se deberá adquirir lo siguiente:

- ✓ Referente al DATA CENTER y a un Generador Eléctrico: debido a que ambos equipos son muy costosos, podrían alquilar o a través de convenio con la PUCE solicitar ciertos servicios, o colocar equipos en el data center de ellos para habilitar un centro de cómputo alterno.
- ✓ Equipos servidores para replicación de los servicios.

- ✓ Materiales básicos para adecuación de las instalaciones.
- ✓ Contratación de servicio alterno de comunicaciones.
- ✓ Equipos para comunicación alterna.

8. PLAN DE VERIFICACIÓN.

Para un plan de contingencia es muy importante que una autoridad independiente, ajena a las labores de la universidad aplique las pruebas de verificación. Para sistemas de menor importancia, la verificación puede realizarse internamente.

Tomando como referencia lo mencionado por Luna (2015), el análisis de las pruebas de verificación puede incluir:

- Asegurar que la documentación sea la adecuada y esté completa.
- Asegurar que los sistemas de comunicación se ciñan a los estándares establecidos y funcionen de manera efectiva.
- Verificar que lo sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.
- Asegurar que se cuente con las debidas medidas de seguridad y que estas se ciñan a las normas establecidas.

8.1. PROCEDIMIENTO PARA LAS PRUEBAS DEL PLAN DE CONTINGENCIA.

Se recomiendan dos niveles de prueba:

- ♦ Pruebas en capacitación.
- ♦ Pruebas de pequeñas unidades.

"Las pruebas de capacitación son necesarias para la preparación adecuada, pues con la debida instrucción los integrantes del departamento de las TIC estarán preparados tanto en conocimiento como en la realidad que pueden llegar a enfrentar ante una situación de riesgo." (Rivas, 1988)

Por consiguiente comenzar la prueba con las personas que integran el departamento de TIC de la institución, las cuales permitan que se pueda simular situaciones pequeñas en conjunto, para finalmente realizar las pruebas con los departamentos que se involucren más con las necesidades que se resuelven diariamente en el departamento de TIC.

8.1.1. PERIODOS DE PRUEBA.

Tabla 35. Ejemplo para Periodos de Prueba

Prueba	Escenario	Tipo de Prueba	Periodo Sugerido de Prueba
A	1	PARCIAL	CADA TRIMESTRE
B	2	PARCIAL	CADA TRIMESTRE
C	3	GLOBAL	DISPONE LA INSTITUCION

9. CONCLUSIONES DEL PLAN DE CONTINGENCIA.

- El presente Plan de contingencia, tiene como principal objetivo proteger las instalaciones de la Red y Sistemas de Información extremando las medidas de seguridad para prevenir y estar capacitados ante una contingencia.
- En el Plan de Contingencia las principales acciones requeridas para la implementación son: Identificación de riesgos, Evaluación de riesgos, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan.
- Para ampliar la habilidad y los medios de sobrevivir y mantener sus operaciones, el Departamento de TIC's de la PUCESE debe tener un Plan de Contingencia como herramienta, en caso de que un suceso fuera de su alcance le pudiera causar una interrupción parcial o total en sus servicios tecnológicos.

10. RECOMENDACIONES DEL PLAN DE CONTINGENCIA.

- ✓ Desarrollar la documentación de los procesos críticos debido a la necesidad que pueda surgir en la ausencia parcial o permanente del personal del área TIC's.
- ✓ Desarrollar los procedimientos de recuperación para el restablecimiento de las actividades en caso de un desastre natural o extremo.
- ✓ Realizar el análisis de riesgo de los servicios críticos para identificar las vulnerabilidades y amenazas que puedan impedir la correcta ejecución de los planes asociados a los escenarios críticos.
- ✓ Gestionar las solicitudes para habilitar Departamentos de Computo Alternos y contactarse con Proveedores Alternos.
- ✓ Realizar capacitaciones y pruebas al personal, para que estén preparados al momento de ocurrir una contingencia.

11. REFERENCIAS BIBLIOGRÁFICAS.

Aboy, D. J. (2013). *Slideplayer.* Obtenido de Slideplayer: http://slideplayer.es/slide/2261921/

Abuin, J. M. (s.f.). *Humanidades.cchs.csic.es.* Obtenido de Humanidades.cchs.csic.es: http://humanidades.cchs.csic.es/cchs/web_UAE/tutoriales/PDF/SPSSIniciacion.pdf

Alvarez, A. F. (Diciembre de 2014). *PUCE DE QUITO.* Obtenido de PUCE DE QUITO: http://www.puce.edu.ec

Amaya, C. G. (14 de Mayo de 2014). *weliversecurity*. Obtenido de weliversecurity: http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Baray, H. L. (s.f.). *eumed.net*. Obtenido de eumed.net: http://www.eumed.net/libros-gratis/2006c/203/

Cardenas, J. (9 de Octubre de 2013). *Networkianos*. Obtenido de Networkianos: http://networkianos.com/que-es-la-correlacion-bivariada-y-como/

Carlos. (10 de FEBRERO de 2011). *LOS BANDERA*. Recuperado el 15 de AGOSTO de 2015, de LOS BANDERA: http://losbanderas.blogspot.com/2011/02/las-caracteristicas-de-un-buen.html

Castillo, J. R. (07 de Marzo de 2014). *Prezi.* Obtenido de Prezi: https://prezi.com/q0elrufmoham/iso-27005-seguridad-de-la-informacion/

Cordones Maria, G. P. (26 de Abril de 2011). *http://bibdigital.epn.edu.ec.* Obtenido de http://bibdigital.epn.edu.ec: http://bibdigital.epn.edu.ec/handle/15000/3790

Díaz, M. (s.f. de s.f de s.f.). *Áudea Seguridad de la Información* . Obtenido de Áudea Seguridad de la Información: http://www.audea.com/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias/

Farias, W. A. (18 de Febrero de 2013). *Gestion de Serivios de la Tectnologia* . Recuperado el 20 de Agosto de 2015, de Gestion de Serivios de la Tectnologia : http://gsticperu.blogspot.com/

Ferrer, J. (2010). *Metodolgia 02*. Obtenido de Metodolgia 02: http://metodologia02.blogspot.com/p/operacionalizacion-de-variables.html

GMR, U. Y. (28 de MARZO de 2016). *YOUTUBE*. Obtenido de YOUTUBE: https://www.youtube.com/watch?v=_NVZhjw4fi8

Granda Juca, A. J. (2011). *REPOSITORIO INSTITUCIONAL UNIVERSIDAD DE CUENCA*. Recuperado el 20 de AGOSTO de 2015, de REPOSITORIO INSTITUCIONAL UNIVERSIDAD DE CUENCA: http://dspace.ucuenca.edu.ec/handle/123456789/2556

Granda, A. (2015). *DSPACE EN CUANCA*. Recuperado el 20 de AGOSTO de 2015, de DSACE EN CUENCA: http://dspace.ucuenca.edu.ec/bitstream/123456789/2556/1/tm4534.pdf

Granda, A. (s.f.). *dspace.ucuenca.edu.ec.* Obtenido de dspace.ucuenca.edu.ec: http://dspace.ucuenca.edu.ec/bitstream/123456789/2556/1/tm4534.pdf

Huguet, M. C. (s.f.). *www.uoc.edu.* Obtenido de www.uoc.edu: http://s3.amazonaws.com/academia.edu.documents/44012077/El_Sistema_informatico_dentro_organizacion.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1484415951&Signature=ej%2FJrZoB5tuCMCDEXyPmlbiujos%3D&response-content-disposition=inline%3B%20filename%3DEl

Ibarra, C. (26 de 10 de 2011). *Metodologadelainvestigacinsiis*. Obtenido de Metodologadelainvestigacinsiis: http://metodologadelainvestigacinsiis.blogspot.com/2011/10/tipos-de-investigacion-exploratoria.html

IBM. (s.f.). *BASE, SPSS STATISTICS*. Obtenido de BASE, SPSS STATISTICS: http://www-03.ibm.com/software/products/es/spss-stats-base

ISACA. (2009). *UCIPFG.* Obtenido de UCIPFG: http://www.ucipfg.com/Repositorio/MATI/MATI-01/Unidad4/lecturas/51855611-Risk-IT-Framework-Espanol.pdf

Juan, G. M. (Madrid de 2004). *books.google.es.* Obtenido de books.google.es: https://books.google.es/books?hl=es&lr=&id=um1V2jADP78C&oi=fnd&pg=PA71&dq=plan+de+contingencia+informatico+para+para+departamento+de+tecnologia+de+informacion&ots=J_DU9101Qu&sig=41eMZelh_Ns3knB6GVqFqRiu6m4#v=onepage&q&f=false

Kessinger, K. (s.f.). *ISACA*. Obtenido de ISACA: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Publica-en-Espa%C3%B1olel-Marco-de-RiesgosdeTIparaAyudaralasOrganizacionesa-Obtener-Beneficios-y-a-Mitigar-los-Riesgos.aspx?utm_referrer=

Lilian, A. (s.f.). *Repositorio.espe.edu.ec.* Obtenido de Repositorio.espe.edu.ec: http://repositorio.espe.edu.ec/bitstream/21000/9100/1/AC-%20MGS-ESPE-048269.pdf

Lopez, P. A. (2005). *books.google.es.* Obtenido de books.google.es: https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=plan+de+contingencia+informatico&ots=PprnUFGCW_&sig=rL80X9HDAouc4Vw49cLQQuM9AOE#v=onepage&q&f=false

Luna, K. M. (enero de 2015). *Universidad Tecnica del Norte.* Obtenido de Universidad Tecnica del Norte: file:///G:/UNIVERSIDAD/avance/04%20RED%20062%20TESIS.pdf

Martínez, J. G. (2004). *books.google.* Obtenido de books.google: https://books.google.com.co/books?hl=es&lr=&id=CSO5BgAAQBAJ&oi=fnd&pg=PA21&dq=Plan+inform%C3%A1tico+de+contingencia&ots=fNuiD1hTOD&sig=cYL-DWC3ZM7fcBAg0kX_rEgrdgk#v=onepage&q=Plan%20inform%C3%A1tico%20de%20contingencia&f=false

Martinéz, J. G. (2015). *Plan de Contingencia - Continuidad del negocio en las organizaciones .* Madrid: Diaz de Santos S.A. .

Miranda, R. U. (31 de Enero de 2013). *Slideshare.* Obtenido de Slideshare: http://es.slideshare.net/RicardoUrbinaM/tesis-r-urbinaabril2012v3presentacionpb

ONUV. (2015). *ONUV*. Recuperado el 20 de AGOSTO de 2015, de ONUV: http://www.unvienna.org/unov/es/management_its.html

Orozco, D. (24 de Noviembre de 2014). *conceptodefinicion.de.* Obtenido de conceptodefinicion.de: http://conceptodefinicion.de/alfa-de-cronbach/

Ramirez, D. (21 de Junio de 2012). *YOUTUBE*. Obtenido de YOUTUBE: https://www.youtube.com/watch?v=tdfeGvQQZqc

Rivas, G. A. (1988). *Auditoria Informatica.* Madrid: Diaz de Santos, S.A. .

Rivas, G. A. (1988). *books.google.es.* Obtenido de books.google.es: https://books.google.es/books?hl=es&lr=&id=gh_jwmkssdYC&oi=fnd&pg=PA1&dq=Departamento+informatico+y+su+seguridad&ots=ueDz-GANy5&sig=EGkI1GsbPhbr2pVLfIPoXyBE2DA#v=onepage&q=Departamento%20informatico%20y%20su%20seguridad&f=false

Roberto, E. e. (29 de MARZO de 2011). *PYMES Y AUTONOMOS*. Recuperado el 20 de AGOSTO de 2015, de PYMES Y AUTONOMOS: http://www.pymesyautonomos.com/tecnologia/el-departamento-de-informatica-es-percibido-como-una-carga-para-la-empresa

Rodriguez y Serrano, F. J. (s.f.). *digitum.um.es.* Obtenido de digitum.um.es: https://digitum.um.es/xmlui/bitstream/10201/27921/2/SPSS_CORRELACIONES.pdf

S.n. (16 de Marzo de 2015). *SGSI(Sistemas de Gestion de Seguridad de Información)*. Obtenido de SGSI(Sistemas de Gestion de Seguridad de Información): http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Salkind, N. J. (1999). *book.google.com.* Obtenido de book.google.com: https://books.google.es/books?hl=es&lr=&id=3uIW0vVD63wC&oi=fnd&pg=PR19&dq=que+el+metodo+descriptivo+de+investigacion&ots=aHNCih2S5K&sig=1j0Okoq9fSGixsTU1kTncDPap7s#v=onepage&q=que%20el%20metodo%20descriptivo%20de%20investigacion&f=false

SANTA, P. D. (s.f.). *municipiobanos.gob.ec.* Obtenido de municipiobanos.gob.ec: http://www.municipiobanos.gob.ec/banos/images/LOTAIP2015/plan%20de%20contingencia%20informatico.pdf

Sartenejas, U. S. (16 de JUNIO de 2009). *PROF.USB.VE.* Recuperado el 20 de AGOSTO de 2015, de PROF.USB.VE: http://prof.usb.ve/cpuig/DTI.pdf

Ureña, M. G. (03 de Febrero de 2015). *SlideShare.* Obtenido de SlideShare: http://es.slideshare.net/besair/gestion-de-riesgos-de-seguridad-de-la-informacion-iso-27005

Vigo, G. M. (Febrero de 2001). *Softeam.* Obtenido de Softeam: http://www.softeam1.com.ar/utn/Documentos%20Seguridad/plan_de_contingencia.pdf

12. ANEXOS.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Encuesta al Departamento de TIC de la PUCESE.

La presente encuesta tiene por objetivo determinar los inconvenientes provocados por la carencia de un Plan de Contingencia en el Departamento de TIC de la PUCESE.

Instrucciones: Lea lentamente cada una de las preguntas, luego encierre o marque con una (X) la opción que considere conveniente.

1. Existe una modalidad para identificar los problemas relacionados con la tecnología de la información.

   a) Se identifican problemas de manera informal.
   b) Se identifican problemas mediante un proceso de documentación monitoreado.
   c) Se identifican problemas mediante un proceso de documentación automatizado.
   d) No existe identificación de problemas.

2. ¿La clasificación de los problemas dentro del departamento de TIC se realizan de acuerdo a los incidentes?

   a) Se realiza una clasificación de manera informal.
   b) Se realiza una clasificación mediante un proceso documentado monitoreado.
   c) Se realiza una clasificación mediante un proceso de documentado automatizado.
   d) No existe clasificación de incidentes.

3. ¿Existe una base de datos para registrar los problemas del departamento de TIC?

   SI ( ) NO ( )

4. Se realiza un análisis y seguimiento a los problemas presentados en el departamento de TIC.

SIEMPRE	( )
CASI SIEMPRE	( )
A VECES	( )
POCAS VECES	( )
NUNCA	( )

5. Existe un plan para dar solución a los problemas presentados en el departamento de TIC.

SI ( ) NO ( )

6. Se tiene algún registro de cierre sobre problemas solucionados en el departamento de TIC.

SI ( ) NO ( )

7. Existe un plan de mejora relacionado con las problemáticas en el departamento de TIC.

SI ( ) NO ( )

8. Considera que el Departamento de TIC tendría un gran avance si se planifica un Plan de Contingencia.

SI ( ) NO ( )

Guía de Entrevista para la dirección del departamento de TIC's.

Objetivo: Obtener datos para realizar el análisis de riesgo a los servicios críticos.

1) ¿Qué servicios tecnológicos son críticos?

2) ¿Qué servicios son necesarios y deben ser levantados inmediatamente después de una catástrofe?

3) ¿Cuánto tiempo pueden permanecer inactivos estos servicios?

4) ¿Quién es responsable de cada servicio?

Guía de Entrevista para los responsables en cada área del departamento de TIC.

Objetivo: Obtener datos para realizar el análisis de riesgo a los servicios críticos.

RIESGO	DOCUMENTACION	SI	NO	N/A	OBSERVACION
Robo	Existe un inventario de los activos y es revisado periódicamente.				
	Existen políticas de seguridad para salvaguardar los equipos.				
	Existe una política que impida sacar los servidores del Data Center.				
Errores de mantenimiento	Existen políticas que determinen el mantenimiento de los equipo.				
	Existe un plan de mantenimiento de los servidores.				
	Existen listados de los sistemas instalados en los servidores de forma independiente.				
	Existe la documentación de los procedimientos para levantar el S.O. del servidor.				
	Se tiene un procedimiento que se realiza para ejecutar un mantenimiento en los servidores.				
Falla de sistema suministro de energía	Existe una adecuada conexión de los equipos a toma tierra.				
	Los servidores cuentan con sistemas de alimentación ininterrumpida.				
Catástrofe	Existe un procedimiento para salvaguardar los servidores ante una catástrofe.				
Acceso no autorizado	Existe una política de acceso a los servidores.				
	Se encuentran desactivadas las cuentas de usuario en el servidor que no se están utilizando.				

	DOCUMENTACION	SI	NO	N/A	OBSERVACION
Acceso no autorizado	Existen aplicaciones que no son necesarias en los servidores.				
	Los servidores no tienen la configuración por defecto.				
	Existe un procedimiento para instalar los últimos parches de seguridad y actualización.				
	Se dispone de una copia de seguridad completa de cada servidor tras una configuración correcta.				
	Están activados los registros de actividad (logs) de los servidores y son revisados periódicamente.				
	Los servidores tienen instaladas herramientas que permitan comprobar la integridad en los ficheros del sistema.				
	Los mensajes de inicio de sesión están modificados, para evitar que se muestre información sobre la configuración y recursos del sistema.				
Falla de respaldo de la base de datos	Existen políticas relacionada con los respaldos de la base de datos.				
	Existe un procedimiento de respaldo de la base de datos.				
	Se encuentra inventariado y etiquetado los respaldos de seguridad.				
	El lugar donde se almacenan los respaldos, es seguro.				
	Existe un plan para comprobar la eficiencia de los respaldos.				
	Existe un registro de incidencias dela restauración del daño de los respaldos.				
Cuentas de usuario	Existen políticas y procesos relacionados con la solicitud, creación, configuración, seguimiento y cancelación de cuentas de usuarios de los servidores.				
	DOCUMENTACION	**SI**	**NO**	**N/A**	**OBSERVACION**

Cuentas de usuario	Existe documentación que justifique la creación de cuentas de usuario con privilegio administrativo con la autorización de la dirección de sistemas.				
	Existe en las políticas las revisiones periódicas sobre la administración de las cuentas.				
	Existe un proceso para detectar actividades no autorizadas, como conexiones a horas extrañas o desde equipos que no se habían contemplado inicialmente.				
	Existen procedimientos para detectar cuentas inactivas en un periodo determinado.				
Identificación y autenticación de usuarios					
	Existe un tiempo de caducidad para la contraseña.				
	Existe un registro historial de contraseñas, para impedir que puedan volver a ser utilizadas.				
	Existen políticas que determinen la composición de una contraseña.				
	Existe algún mecanismo de bloqueo de cuentas tras varios intentos fallidos de autenticación.				
	Existe un procedimiento a efectuar, en caso de que la contraseña sea adquirida por terceros.				
	Existe un proceso que impida utilizar la misma contraseña en varios sistemas.				
	Existe una política que exija el cifrado del fichero que contiene las contraseñas.				
	Existe un registro de las sesiones iniciadas por usuarios así como también los intentos fallidos.				
Autorización y control de acceso lógico	Existen mecanismos que eviten a un usuario acceder a datos o recursos con derechos distintos de los autorizados.				

	DOCUMENTACION	SI	NO	N/A	OBSERVACION
Autorización y control de acceso lógico	Existe una política de control de acceso de servicios en los servidores.				
	Existen grupos definidos de usuarios que permitan un mejor acceso a los datos y aplicaciones.				
	Existe un mecanismo para restringir los derechos y privilegios administrativos de los usuarios.				
	Existe un control para registrar los intentos de acceso fraudulentos a los datos, ficheros y aplicaciones del sistema informático.				
	Existe algún procedimiento que ayude a descubrir la autoría de los intentos fraudulentos.				
Monitorización de servidores y dispositivos de la red	Existen políticas de seguridad que faciliten la detección de intentos de ataques contra los servicios críticos.				
	Existen “logs” que permita registrar las sesiones iniciadas por los usuarios en los servidores.				
	Existe un sistema de monitoreo que permita enviar alarmas cuando existan incidentes.				
	Existe la revisión de “logs”, cada que tempo, que medidas toman.				
	Existe una política en la cual se informe sobre “logs” a los empleados.				