

ESCUELA DE INGENIERÍA EN SISTEMAS

Tema:

Desarrollo de un plan de contingencias basado en un estándar de seguridad, orientado a un servidor de aplicaciones

Disertación de grado previo a la obtención del título de

Ingeniero de Sistemas y Computación

Línea de investigación:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus Aplicaciones.

Autor:

JONATHAN LLERENA MIRANDA

Directora:

ING. MSC. TERESA MILENA FREIRE AILLÓN

Ambato-Ecuador

Marzo 2018

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

Desarrollo de un plan de contingencias basado en un estándar de seguridad, orientado a un servidor de aplicaciones

Línea de Investigación:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus Aplicaciones

Pontificia Universidad Católica del Ecuador
BIBLIOTECA

Autor:

JONATHAN LLERENA MIRANDA

Teresa Milena Freire Aillón, Ing. Msc. f._____
CALIFICADOR

Darío Javier Robayo Jácome, Ing. Msc f._____
CALIFICADOR

José Marcelo Balseca Manzano, Ing. Msc. f._____
CALIFICADOR

Elva Aidee Llerena Barreno, Ing. Msc. f._____
DIRECTOR DE UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villaroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato-Ecuador

Marzo 2018

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Jonathan Llerena Miranda portador de la cédula de ciudadanía No. 180359290-4 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Ingeniero de Sistemas y Computación son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

Jonathan Llerena Miranda
CI. 180359290-4

Pontificia Universidad Católica del Ecuador
BIBLIOTECA

AGRADECIMIENTO

Agradezco a todos mis maestros, que fueron los pilares que fundamentaron mi educación no sólo académica, sino también personal y profesional predicando con el ejemplo de profesionalismo y desempeño. A la Ingeniera Teresa Freire y el Ingeniero Galo López por haber fomentado el espíritu de investigación y amor con respeto y colaboración a la profesión, por ser unos profesionales y ante todo por ser la ayuda necesaria para poder culminar éste trabajo con éxito, a mis amigos que me han apoyado siempre con su aliento y palabras, a mis compañeros, y más que todo a Dios por darme la voluntad y fuerza de lucha para culminar todo el esfuerzo con éxito.

Jonathan Llerena Miranda

DEDICATORIA

Quiero dedicar el presente trabajo a mi familia, a mis padres que gracias a su esfuerzo y trabajo me permitieron llegar hasta ésta instancia. A mi hermana Daniela por ser mi guía espiritual, personal y moral durante toda mi vida, darme su apoyo incondicional en toda ocasión, su sabio consejo en el momento más oportuno, y darme el amor y la comprensión necesaria. Mis hermanos de corazón Andrés, Pablo y Paúl por acompañarme en todos mis años dándome aliento y más ganas de seguir adelante aquí y desde el cielo. A mi amigo Daniel por ayudarme para tener el tiempo de culminar este trabajo.

Jonathan Llerena Miranda

RESUMEN

El presente trabajo de investigación tiene como objetivo el mantener los procesos de forma gestionada para la entrega de servicios de valor agregado, mediante eficiencia y tecnología adecuada para poder hacerlo. Al implementar un plan de contingencias para el Departamento de Informática en la Pontificia Universidad Católica del Ecuador Sede Ambato (PUCESA), se minimiza el surgimiento de cualquier riesgo e impacto en la organización, ya que todos los recursos de información que aquí se usan son vitales y sin ellos serían inoperables ciertos ámbitos de la Institución.

La norma ISO/IEC 27001 es la que proporciona seguridad para dichos procesos y procedimientos estableciendo documentación que sirve para llevar un control adecuado. El presente plan está apoyado en la metodología explicativa realizada por Oficina Nacional de Gobierno Electrónica e Informática (ONGEI), misma que comprende 8 fases hasta la implementación del proyecto, la cual garantiza la entrega del plan y que permitirá que los procesos internos del Departamento sean más estructurados y eficientes para su control.

Palabras clave: plan de contingencias, procesos, valor agregado, informática, riesgos, información, norma ISO, seguridad.

ABSTRACT

The objective of this research project is to assure that processes are carried out in a manageable way in the delivery of value-added services in the IT Department of the Ambato site of the Pontificia Universidad Católica del Ecuador, through efficiency and the use of technology appropriate to the task. In implementing a contingency plan, the IT Department minimizes both the incidence of risks, and their potential impact should they emerge. This is because each information resource used in the university is vital, and without them, certain departments of the university would be non-operational. The ISO 27001 standard provides security to the above-mentioned processes and procedures, through stipulation of documentation allowing for suitable monitoring processes to be carried out. The proposal made in this project is informed by the explanatory method produced by the National Office of Electronic and IT-based Government, which comprises eight stages leading up to the implementation of the project. This method guarantees the submission of the plan, and assures that the internal processes of the IT Department are more structured and efficient.

Keywords: contingency plan, processes, value-added, IT, risks, information, ISO standard, security

ÍNDICE DE CONTENIDOS

PRELIMINARES

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD……iii
AGRADECIMIENTO…… iv
DEDICATORIA…… v
RESUMEN…… vi
ABSTRACT…….. vii
CAPÍTULO I. 2
FUNDAMENTOS TEÓRICOS..... 2
1.1. Antecedentes 2
1.2. Problema..... 3
1.2.1. Descripción del problema..... 3
1.2.2. Preguntas básicas 4
1.3. Justificación..... 4
1.4. Objetivos 5
1.4.1. Objetivo General. 5
1.4.2. Objetivos Específicos. 6
1.5. Fundamentos Teóricos 6
1.5.1. Plan de Contingencias 6
1.5.1.1. Características 7
1.5.1.2. Alcance 8
1.5.1.3. Tipos 8
1.5.1.4. Plan de Contingencia Informático 9
1.5.2. Estándares de Seguridad..... 12
1.5.2.1. ISO 27001..... 15
1.5.3. Servidor..... 16
1.5.3.1. Servidor de Aplicaciones..... 18
CAPÍTULO II. 21
METODOLOGÍA 21
2.1. Metodología de Investigación 21
2.2. Técnicas de Recolección de Información..... 21
2.2.1. Encuestas 22

2.2.2. Entrevistas 22
2.2.3. Observación 22
2.3. Población 23
2.4. Metodología de Desarrollo 23
2.4.1. Fase 1. Planificación 23
2.4.2. Fase 2. Identificación de Riesgos 25
2.4.3. Fase 3. Identificación de Soluciones 27
2.4.4. Fase 4. Estrategias 30
2.4.5. Fase 5. Documentación del Proceso 33
2.4.6. Fase 6. Realización de Pruebas y Validación 33
2.4.7. Fase 7. Implementación 41
2.4.8. Fase 8. Mantenimiento 41
CAPÍTULO III. 42
DESARROLLO 42
3.1. Resultados 42
CAPÍTULO IV 88
RESULTADOS 88
4.1. Análisis de Resultados 88
4.2. Validación de Resultados 89
CONCLUSIONES 90
RECOMENDACIONES 91
BIBLIOGRAFÍA 92
ANEXO 1. ENCUESTA 94

ÍNDICE DE GRÁFICOS

GRÁFICOS

Gráfico 3.1. Organigrama…… 45
Gráfico 3.2. Target para VEGA de ACADEMICS…….. 57
Gráfico 3.3. Resultado de escaneo de ACADEMICS…….. 58
Gráfico 3.4. Target para ZENMAP de SACI..... 60
Gráfico 3.5. Resultados del escaneo SACI..... 61
Gráfico 3.6. Target para VEGA de MOODLE..... 63
Gráfico 3.7. Resultados del escaneo MOODLE..... 63

TABLAS

Tabla 2.1. Población del Departamento de Informático PUCESA..... 24
Tabla 3.1. Inventario de Hardware y Software..... 46
Tabla 3.2. Tabulación de Encuestas……..... 70
Tabla 3.3. Priorización de Criticidad……..... 70
Tabla 3.4. Cuadro de Evaluación de Riesgos……..... 72
Tabla 3.5. Tablas de Estimación de Probabilidad e Impacto……74
Tabla 3.6. Tabla de Probabilidad vs. Impacto…….75
Tabla 3.7. Plan de Tratamiento de Riesgos. 78

INTRODUCCIÓN

Dentro de la Pontificia Universidad Católica del Ecuador Sede Ambato se encuentra el Departamento de Informática, el mismo que maneja la información utilizada por personal docente, administrativo y estudiantes y está enfocado en 4 sistemas que son el sistema Académico, Contable, Administrativo y la Plataforma Virtual EVAE. Los servidores de aplicaciones manejan información crítica, y es constantemente accedido por usuarios, lo cual provoca que sea de dependencia importante y se encuentre en riesgo de sufrir algún percance, lo mismo que hace vital el uso de un plan de contingencia que permita minimizar la incidencia de catástrofes de gran alcance, y en caso de sucederlos, minimizar su impacto y luego una posible recuperación de todo lo que se maneja. Un plan de contingencias informático no está enfocado únicamente a los riesgos de la información sino también a infraestructura, y busca evitarlos antes que corregirlos. Es necesario hacer énfasis en la importancia de mantener lo más segura posible a la empresa, institución u organización para no afectar de forma sustancial a los usuarios de la información.

CAPÍTULO I.

FUNDAMENTOS TEÓRICOS

1.1. Antecedentes

Hoy en día, la necesidad de mantener la entrega de servicios eficientes en referencia a tecnologías de la información (TI) es un concepto muy abarcador y grande en esencia de cumplimiento de objetivos que estén encaminados al cumplimiento de metas de la organización, y por tanto; esto hace que los aspectos en cuanto a materia tecnológica se refieren, vayan tomando un valor incremental y un rol indispensable para las empresas el desarrollo de un plan de contingencias que ataque a las deficiencias de una organización siempre será un aspecto muy importante, debido a que por demandas de calidad altas son requeridas para e momento de brindar un servicio u ofrecer un producto realizado por entidades de la organización, y por eso, para evitar los problemas cabe recalcar la aplicación de manuales y buenas prácticas de prevención y recuperación para errores que se puedan presentar.

Mantener eficientes los procesos internos de una organización es prioridad para poder entregar el mejor servicio a los usuarios del mismo, entendiéndose como entrega del servicio al procedimiento de brindar un producto de excelente calidad o proveer el uso adecuado de las herramientas disponibles por parte de la organización para facilitar algún proceso por parte del usuario. La utilización de buenas prácticas en este

proceso de entrega de servicio es una figura esencial debido a que una empresa u organización debe basarse siempre en la calidad que entrega a sus usuarios en todos los procesos que éstos utilicen; pero para poder llevar todo un control adecuado de la implantación de buenas prácticas se necesita de procesos innovadores que mantengan en un orden adecuado las funciones que se dan en la organización.

1.2. Problema

1.2.1. Descripción del problema

El Departamento de Informática no ha sufrido la ocurrencia de un desastre de proporción alta que haya producido pérdida de información, pero el hecho de que no lo hayan experimentado no los exenta de la ocurrencia de los mismos y por ésta razón es que el proyecto puede sustentarse. El problema general encontrado es que al no existir un plan que detalle qué medidas se pueden tomar en caso de dificultades o ataques por parte de terceras personas a la información que se maneja en el servidor de aplicaciones, incrementa la probabilidad de un desastre informático de gran magnitud. Controlar este tipo de riesgos es vital, ya que la información que se maneja en el servidor es aquella con la que todas las personas dentro de la institución operan y en este caso al no contar con un plan de contingencias, se pueden correr riesgos altos de pérdida de información, desbalances, e incluso

ser un obstáculo en el proceso de acreditación institucional y de carreras.

1.2.2. Preguntas básicas

- ¿Cómo aparece el problema que se pretende solucionar? No Aplica.
- ¿Por qué se origina? No aplica.
- ¿Qué lo origina? La necesidad de mantener segura la información del servidor.
- ¿Cuándo se origina? No aplica
- ¿Dónde se origina? En los servidores de aplicaciones.
- ¿Dónde se detecta? No Aplica

1.3. Justificación

Basado en los estándares de calidad de la educación superior hoy en día en el país, es necesario mantener un adecuado nivel de madurez de calidad en los procesos realizados en las instituciones de educación superior. La Pontificia Universidad Católica del Ecuador Sede Ambato mediante el Departamento de Informática mantiene en orden todos los procesos de manejo de información referentes a los aspectos Académicos, Administrativos y Contables, y debido a reformas recientes dadas en cuanto a infraestructura interna del Departamento, se han descuidado varios aspectos en cuanto a seguridad de

información y aseguramiento de equipos en el caso de ocurrencia de algún desastre informático, es por eso que la implementación de un plan de contingencias que ayude a la prevención de estas posibles desastres, que cuente también con acciones correctivas para el momento en el que se está presentando la ocurrencia del inconveniente y una fase de recuperación después del fallo es muy importante para garantizar la entrega de información y servicios a los usuarios en cuanto se requiere.

Además cabe resaltar el hecho de que en el presente proyecto el punto clave a tratar es el servidor de aplicaciones, ya que debido a su prioridad en el manejo de información que afecta a toda la institución sería desastroso que en caso de ocurrir algún desastre no se cuente con medidas de seguridad para recuperación de información o continuidad de servicio. La falta de medidas de seguridad siempre implica un riesgo grande en cualquier organización porque puede significar pérdidas o robo de información por parte de terceras personas.

1.4. Objetivos

1.4.1. Objetivo General.

Desarrollar un plan de contingencias basado en un estándar de seguridad, orientado al servidor de aplicaciones de la PUCESA.

1.4.2. Objetivos Específicos.

- Realizar un análisis de los riesgos a los que está expuesto el servidor de aplicaciones de la PUCESA.
- Analizar distintos estándares de seguridad para la selección y aplicación del que mejor se adapte a los requerimientos de seguridad del servidor de aplicaciones.
- Elaborar el plan de contingencias en base a los riesgos identificados y al estándar elegido.
- Validar el Proceso de realización del plan mediante socialización de resultados.

1.5. Fundamentos Teóricos

1.5.1. Plan de Contingencias

Un plan de contingencias, básicamente está enfocado a una prevención de incidentes, no necesariamente informáticos, sino un incidente debido a cualquier factor; y además también consta con una plan de acción de cómo se debe tratar el incidente en el momento en el cual está sucediendo, y finalmente un plan de recuperación, que

permita que la organización después del fallo no esté propensa a falta de información o daños en ciertos aspectos.

El objetivo principal de una plan de contingencias, basado en lo que dice [6], es “Ejecutar acciones oportunas ante cualquier contingencia que se pudiera presentar como consecuencia de un siniestro para salvaguardar a las personas, bienes y el entorno de los mismos que se encuentren dentro de la Institución.”, lo que indica que las acciones llevadas a cabo sean precisas y a tiempo de minimizar la ocurrencia de un desastre, y que a pesar de no poder mantener bajo control a un riesgo al 100% es vital poder controlarlo lo antes posible y mantener la seguridad e integridad de los activos empresariales tanto los tangibles como los intangibles.

1.5.1.1. Características

Dar solución a una necesidad. Debe plantear una mejora en los procesos o servicios brindados dentro de la organización.

Factibilidad. La ayuda es el factor importante y se debe contar con las herramientas adecuadas para llegar a lograr una meta, y el plan debe dar las pautas adecuadas para este objetivo.

Conocido y divulgado interdepartamentalmente. Necesariamente todas las unidades organizativas deben conocer y divulgar las mejoras

que proveerá el plan de contingencias, además deberán involucrarse totalmente dentro del mismo para su efectividad.

Suscrito y Legitimado. La aplicación del mismo debe tener la aprobación y soporte de las partes interesadas de la empresa u organización; es decir, contar con la autorización superior de los administrativos.

Actualizado. Los procesos que se detallan dentro del plan deben contener los procesos y servicios actuales, mediante investigaciones que se dan dentro de forma organizacional [1].

1.5.1.2. Alcance

Dentro del alcance se denotará que, la frontera que se planteará sería los servidores de aplicaciones y lo que conlleva a dichos servidores, ya que mantener un alcance corto es importante para llevarlo a cabo en el tiempo establecido y también manejar las condiciones de operación del mismo plan, para así no exceder las limitaciones y definir el marco de trabajo [1].

1.5.1.3. Tipos

Ambientales. Son aquellos planes de contingencia enfocados en el comportamiento de la naturaleza y los fenómenos que se presentan en ella, intervienen dentro de este tipo los planes de evacuación, reforestación, promoción ambiental, entre otros.

Defensa. Ambientados en la seguridad, y como ejemplos se tienen los planes de ayuda humanitaria, planes estratégicos en conflictos entre países, y varios más.

Bioambiental. Es similar a los ambientales, aunque están más enfocados en cuanto a materia ambiental con la ayuda de la tecnología, ayuda a la mejora de la calidad de vida ambiental con la aplicación de procesos tecnificados.

Hospitalaria. Son aquellos que buscan la mejora en servicios de la salud, mejorar la atención y recepción de personas. Buscan la mejora de los procesos actuales y de la gestión de las políticas de servicio, para hacerlas lo más eficientes posible.

Informáticos. Tienen la visión de evitar la ocurrencia y concurrencia de desastres de tipo informático en cuanto se refiere a infraestructura e información, asegurar calidad en la entrega de un servicio, mantener la fiabilidad e integridad en la información que se entrega a los usuarios, entre otros.

1.5.1.4. Plan de Contingencia Informático

Un plan de contingencia informático está enfocado en el correcto mantenimiento y control de lo sucedido en cuanto a materia de información, que aunque la información es la parte fundamental en cualquier organización, dentro de un plan informático de contingencias

se controlan varios otros aspectos también, como aquello respecto a la infraestructura, los activos empresariales y ambiente de desenvolvimiento de la información, es decir el entorno el cual la rodea y los usuarios que acceden a todos estos elementos.

Un plan de contingencias netamente informático no se basa sólo en lo referente a informática, también hace uso de varias estrategias para definir las mejoras a aplicarse para una gestión de procesos y servicios tales como análisis de riesgos, estadísticas de incidencia de fallas, vulnerabilidades y amenazas a las cuales se está expuesto.

Análisis de Riesgos

Se hace una evaluación de los posibles impactos que puedan estar inmersos al momento de la ocurrencia de un desastre que puedan afectar de forma sustancial a la organización, sea de forma mínima, grave o crítica. Para la realización de un análisis de riesgos; las preguntas que deben ser contestadas son:

- ¿Qué puede ocurrir?
- ¿Con qué frecuencia?
- ¿Cuáles serían los resultados de una ocurrencia?

Los riesgos que van a ser analizados deben ser tomados de forma muy profunda y buscar desde lo más pequeño que pueda ocasionar una catástrofe hasta los aspectos más generales, la protección de los equipos y de la infraestructura es vital; ya que tanto los equipos pueden sufrir algún percance por lo que no proporcionen los resultados de las peticiones de información, o bien se pueden destruir o perder. Igualmente los activos deben estar en áreas preparadas exclusivamente para los mismos, ya que incluso las instalaciones físicas pueden ser una causa de aislamiento o daño de información, la preparación adecuada del cableado, el control de la temperatura ambiente, el acceso a los activos de personas que no tengan el debido acceso autorizado, entre otras.

Desastres y Amenazas

Hay que enfatizar que lo que busca el plan de contingencias es asegurar la continuidad de entrega del servicio a los usuarios, ya que el recurso es el motivo vital de la organización, y por tanto el desconocimiento de las amenazas que afectan dentro o fuera de la organización, aumenta el riesgo de ocurrencia y concurrencia de algún tipo de desastre. Las personas que intervienen en la organización deben ser las primeras en conocer dicho plan y estar preparadas en caso de existir alguna dificultad o un desastre que implique la aplicación del Plan de Contingencias; y la

recuperación después de ocurrir dicho desastre debe tener efecto inmediato, sin dejar de brindar el servicio o en caso de hacerlo, debe ser por un tiempo mínimo hasta recuperarse totalmente [2].

Desarrollo de un plan de contingencias

El desarrollo del marco del plan de contingencias debe darse de forma parcial, siempre estar en concordancia con los procedimientos que se llevan a cabo en las distintas áreas de la organización, denotando así qué es lo que se quiere lograr y cuáles son los alcances que se plantean en el objetivo. Como se plantea que la continuidad del servicio en las operaciones es la parte vital, el desarrollo debe darse entorno a dicha continuidad, así como procurar que todas las acciones que se lleven a ejecución deben estar en concordancia al sistema actual de información en el cuál se maneje, es decir considerar todas las oportunidades que la información representa y qué aspectos de la misma son aquellos que permiten la operación organizacional [3].

1.5.2. Estándares de Seguridad

Un estándar de seguridad es aquel que ayuda a mantener la confiabilidad e integridad, mediante la utilización de parámetros o procesos definidos en manifiesto con la definición de pasos para poder cumplir con el objetivo central que es la seguridad. Lo más importante

en lo que está enfocado es en la seguridad de la información, y además en la correcta definición de las adecuadas direcciones que deben establecerse siempre teniendo en cuenta a toda la organización y lo que ésta requiere.

La importancia de seguir la implementación de un estándar de seguridad es muy alta, debido a que permite tener una ventaja en cuanto a problemas que se pueden dar y además la prevención de una futura catástrofe dentro de la organización, ya sea por la falta de implementación de un estándar o medida de seguridad, o por el descuido del propio personal que interviene en la organización. Se debe establecer que los estándares de seguridad deben estar en concordancia y línea directa con los requerimientos de servicios que se dan en la organización en la cual se pretende implementar, además de realizar estudios para constatar qué medidas serán las que mejor se adhieran al proceso o cuáles son las medidas que mejor intervienen en ciertos procesos.

Está contextualizado básicamente como un modelo de requerimientos dentro de la organización que proveerá cambios mínimos para así poder llegar a un nivel de calidad de los servicios o procesos, que sea aceptable y perfectible. Este proceso necesariamente requiere la identificación de las oportunidades y de las amenazas que existen, para así poder identificar los riesgos a los que está expuesto y la manera de cómo disminuir la concurrencia de estos al mínimo.

- **ISO/IEC 27001**

Es un estándar desarrollado por la ISO una organización Internacional de Estandarización, la cual provee un apoyo completo en lo referente a las prácticas necesarias para la realización y control de planes basados en seguridad de la información, está enfocada en la gestión de los objetivos organizacionales [4].

- **ITIL**

ITIL o Information Technology Infrastucture Library es uno de los estándares más importantes, que contiene una recopilación de buenas prácticas, que son las mismas aplicables a cualquier tipo de gestión en cuanto se refiere a los servicios que se entregan en el marco de las Tecnologías de la Información y Comunicación (TIC), ofrece varios procedimientos aplicados que son independientes de la organización en la que se lo está aplicando y además son una guía de cómo llevar a cabo el manejo de todo lo que interviene en las TIC, así como las operaciones, los servicios de infraestructura y el desarrollo de gestión de servicios y aplicaciones [5].

- **SARBANES**

Este estándar está enfocado en las secciones que hacen referencia a la calidad de productos de información, tomando como base las características, los atributos y de ésta forma plantear correctamente

objetivos que serán aquellos que guíen la investigación y así determinar las correctas herramientas que facilitarán la aplicación y generación de valor en los procesos y servicios brindados [6].

- **COBIT**

COBIT (En español Objetivos de Control para la Información y Tecnologías Relacionadas o en inglés Control Objectives for Information and related Technology) es un marco de trabajo relacionado que incluye las partes de la empresa y alinean los objetivos para la mejora de procesos de TI con los objetivos superiores empresariales planteados por los administrativos de rango superior. Éste marco de trabajo permite que sea un ambiente adecuado el de trabajo para la aplicación de un plan de contingencias, ya que permite estar al tanto de toda la organización y en constante flujo de información entre todos quienes la componen [7].

1.5.2.1. ISO 27001

De acuerdo al portal ISO, la norma 27001; que fue publicada en su primera edición el 15 de octubre de 2005 es una norma de gestión de seguridad en cuanto a información; para poder conocer acerca de su correcta aplicación se puede hacer uso de los auditores de SGSI (Sistema de Gestión de Seguridad de la Información). Conteniendo varios anexos en cuanto a la aplicabilidad de controles de seguridad,

esta norma internacional busca la especificación de requerimientos que son necesarios para establecer la continuidad de operación de una organización y minimizar la ocurrencia de riesgos que puedan afectar a dichas operaciones estableciendo y satisfaciendo las necesidades que surjan en cuanto a la organización se trate [8].

1.5.3. Servidor

Un servidor es aquel que provee de información o brinda algún servicio a los usuarios. En concordancia con AnerData, se acota que un servidor es esencialmente un equipo de tipo informático, que está incluido dentro de una red que puede ser de forma local o también de forma mundial y que es aquel que ayuda a compartir recursos y servicios a los usuarios que deseen acceder de forma controlada e identificable a la información [9], refiriéndose a que de forma identificable un usuario necesariamente deba tener el acceso a la información y no cualquiera pueda poner en riesgo la información. Existen diversidad de servidores, de los cuales se referencia cada uno:

- **Servidor de Directorio:** Se encarga de mantener la información necesaria sobre los equipos conectados en la red, los grupos, también los usuarios, entre otras aplicaciones.

- **Servidor de archivos:** Es el que sirve de almacén de los ficheros y archivos, además que reparte los mismos a los usuarios.
- **Servidor de Correo:** Lo que se busca es la gestión en cuanto al flujo de la mensajería electrónica, es decir el control de los correos que un usuario recibe, envía o mantiene almacenados.
- **Servidor de Impresión:** Para añadir elementos a la cola de impresión y proveer las impresoras disponibles a los usuarios.
- **Servidor de Fax:** Similar al servidor de correos, pero con fax.
- **Servidor DNS:** Permite el establecimiento de una conexión entre la dirección IP y los nombres de los dominios en una red.
- **Servidor Proxy:** Ayuda a que el acceso a páginas web visitadas frecuentemente sea mucho más rápido, guardándolas en la memoria caché al momento del acceso.
- **Servidor Web:** Mantiene guardado los contenidos de la web y los pone a disposición de los usuarios.
- **Servidor de Base de Datos:** Proveedor de los servicios de una base de datos (BD) a equipos o aplicaciones.
- **Servidor FTP:** Ayuda al intercambio de archivos para los usuarios de una red.
- **Servidor DHCP:** Asigna a un equipo cliente una dirección IP para la configuración una vez lanzada una petición. [9]

1.5.3.1. Servidor de Aplicaciones

Un servidor de aplicaciones es una implementación de la especificación J2EE [10], es decir del estándar Java 2 Platform Enterprise Edition [11]. Básicamente lo que se indica es que un servidor de aplicaciones tiene como objetivo o utilidad la de ser el centro de varias aplicaciones, a las cuales se les debe dar el adecuado soporte para poder ser ejecutadas y también tengan la disponibilidad correspondiente para los usuarios, que además son los que manejan la información necesaria, de la cual dependen aquellos que intervienen en la organización, pero con las debidas restricciones o impedimento de usuarios no autorizados.

Este tipo de servidor es vital dentro de organizaciones, en donde se están manejando aplicaciones específicas, o dónde necesariamente manejen varios usuarios, que están constantemente accediendo a información; un ejemplo muy claro son las instituciones educativas, donde se maneja información, que va desde un simple registro de notas, hasta el total costos de toda la organización.

Técnicamente puede decirse que un servidor de aplicaciones suele utilizar la intercomunicación para varios servicios, que además generan seguridad; acotando además que dentro del servidor web también está prevista una interfaz de programación, ya que existe diversidad de sistemas operativos con los cuales debería lidiar en caso de no contar con la interfaz mencionada.

En comparación con varias arquitecturas de otros tipos de servidores que generalmente son de dos capas, dentro del servidor de aplicaciones se ven enfocadas tres capas que son la que ayuda a la estructuración del sistema de una forma mucho más eficaz y rendidora, a pesar de que es necesario recalcar que en todo caso de organizaciones que sean pequeñas no es necesario siempre el contar con un servidor de aplicaciones para el manejo de las mismas. En cuestión de costos es un poco complicado el hecho de mantener un servidor para pequeñas empresas, ya que tal vez requieran el uso de una o dos aplicaciones y baste con la implementación de otro tipo de servidor que no necesite de muchos recursos.

Para la implementación de un servidor de aplicaciones se cuentan con características (software de conectividad, interfaz de programación, soporte a estándares) que pueden hacer mucho más llamativa la implementación. Basados en el concepto dado por EcuRed [12] , se destaca algunas de las implementaciones más utilizadas:

- BEA WebLogic
- IBM WebSphere
- Sun-Netscape IPlanet
- Sun One
- Oracle IAS
- Borland AppServer
- HP Bluestone

Información Manejada

Un servidor de aplicaciones básicamente está enfocado en lo que su nombre indica, es decir al manejo de la información basada en las aplicaciones que son utilizadas para el control interno o externo de la empresa, información que siempre va a estar sometida a manipulación por parte de los usuarios, que son los que aumentan los riesgos de afectación por no mantener los adecuados accesos a la misma. En este caso en particular la información que va a ser manejada será:

- Información de los usuarios (Estudiantes, Docentes)
- Información Académica (Notas, Faltas, Promedios)
- Información Financiera (Balances, Cuentas, Estados, Datos)
- Información Institucional (Horarios, Syllabus, Tutorías, Encuestas)
- Información General (Institucional, Personal Administrativo, Docente y Servicios Generales)

Riesgos

Estar propenso a riesgos es una naturalidad a la cual se expone todo tipo de organización, ya que los riesgos siempre están presentes sea de una u otra forma, unos de mayor alcance y otros en estado pasivo, pero aun así siempre hay que tener un control y estar preparados para afrontar cualquier tipo de riesgo y evitar que se convierta en catástrofe.

CAPÍTULO II.

METODOLOGÍA

2.1. Metodología de Investigación

Dentro del desarrollo llevado a cabo en la metodología usada se denota como de tipo explicativa, teniendo en cuenta que éste tipo no se establece en un punto seguro de describir conceptos o fenómenos que se suscitan, sino va más allá de todo y busca las respuestas a las causas de eventos dados sean estos de cualquier naturaleza. Mantienen un ambiente mucho más estructurado, debido a que todo el estudio que se da, busca los propósitos del mismo proyecto y los fenómenos que lo conforman [13]. La metodología sirve para la estructuración del plan de contingencias y todas las herramientas que intervienen para su formalización y aplicación.

2.2. Técnicas de Recolección de Información

Las técnicas de recolección de información son utilizadas para conocer la realidad actual de la organización y así conocer mejor si es que el personal está al tanto de los procesos que se llevan a cabo dentro del funcionamiento del Departamento y si están lo suficientemente involucrados con el mejoramiento en la entrega de los servicios que ofrecen al personal docente, administrativo y estudiantes. La recolección de información va a estar basada en 3 tipos fundamentales que son:

2.2.1. Encuestas

Las encuestas se realizan debido a que es necesario tener una situación actual de la organización y además conocer si es que las personas que están involucradas en la misma tienen conocimiento acerca del manejo de todo lo que se maneja internamente como la información y además si tienen definidas formalmente sus funciones; además de saber cómo actuar en caso de suscitarse algún problema que necesite alguna medida correctiva.

2.2.2. Entrevistas

El objetivo central de las entrevistas es comprender las funciones centrales que se dan dentro de la organización y como se llevan los procesos de mantenimiento actuales al servidor de aplicaciones, o en el caso de que se realicen procesos específicos considerarlos de utilidad; además se han aplicado para que las personas involucradas directamente con el manejo de la información de los servidores puedan aportar con información para el planteamiento de la solución.

2.2.3. Observación

Es un recurso muy valioso, ya que determina la razón del estudio mediante observación de cómo se realizan los procesos, en el caso de que se manejen procesos por períodos de tiempo como respaldos, mantenimientos. Revisa la forma en la que se realizan y de qué forma aporta la propuesta.

2.3. Población

Cargo	Nombre	Frecuencia
Jefe Departamental	Ing. Gabriel Altamirano	1
Asistente de Base de Datos	Ing. José Enríquez	1
Asistente de Plataforma y Aplicaciones	Ing. Mónica Mena	1
Asistente de Redes y Telecomunicaciones	Ing. Eduardo Remache	1
Auxiliar de Mantenimiento Técnico	Ing. Marlon Castro	1
Total		5

Tabla 2.1. Población del Departamento de Informática PUCESA
Fuente: Departamento de Informática PUCESA
Realizado por: Jonathan Llerena

2.4. Metodología de Desarrollo

La metodología utilizada fue desarrollada por parte de la Oficina Nacional de Gobierno Electrónica e Informática (ONGEI) [14] .Las fases que comprende la metodología general para desarrollo de planes de contingencias es la siguiente:

2.4.1. Fase 1. Planificación

Este es la fase más importante de la metodología, debido a que dentro de ésta se establecen los procesos, tomando consideraciones a futuro para la aplicación y desarrollo del plan de contingencias, basado en una serie de requerimientos y recolectando la información necesaria; mediante entrevistas hacia el personal que labora en el Departamento de Informática de la PUCESA, y así obtener la suficiente información para proceder a mantener una agenda de actividades a cumplirse.

2.4.1.1. Diagnóstico

Se debe encontrar las actividades que son las que requieren con prioridad un rediseño que solucione falencias en las mismas y que expongan al funcionamiento correcto del recurso dentro de la organización, ya que esto conllevaría a la ralentización en la entrega de un servicio de calidad. La etapa de diagnóstico permite tener acciones correctivas para las funciones menos desarrolladas.

2.4.1.2. Organización Estructural

Conocimiento de cómo está conformado la organización, departamento o institución es fundamental, establecer las personas involucradas en los procesos llevados a cabo y a la jerarquía establecida.

2.4.1.3. Inventario de Recursos Informáticos

Este recurso se obtiene por medio de dependencias y en forma de clasificación con respecto a tres ejes fundamentales.

- Equipos
- Programas
- Aplicativos

2.4.1.4. Planificación (Establecimiento)

Establecimiento y preparación de las tareas que se van a realizar durante el proyecto, detallando actividades que son de tipo alcance, fases, eventos, enfoque. Se desarrolla los grupos de trabajo iniciales o tareas iniciales en caso de ser un proyecto unitario. El coordinador del proyecto debe establecer las prioridades de las tareas:

- Alcance
- Eventos a realizar
- Partes más importantes
- Fuentes de investigación
- Comunicación
- Estrategias
- Aprobación de lo anterior por parte de las entidades de la empresa / departamento.

2.4.2. Fase 2. Identificación de Riesgos

Se busca la minimización de errores que sean producidos por cualquier situación que no está prevista en el funcionamiento normal de la organización o por causa de alguna herramienta, activo o tercer supuesto que pueda estar afectando al funcionamiento. Se debe partir del análisis organizacional de cómo funciona la empresa, es decir tener un balance del estado actual de la organización en cuestión de aspectos generales como:

- Infraestructura
- Activos
- Personal

Se definen también ciertas fases más como:

2.4.2.1. Análisis y Evaluación de Riesgos

Conocer los riesgos y evaluarlos es fundamental para poder reducir el impacto que puedan llegar a generar en cierto estado del tiempo y que los servicios o productos que se ofrecen no se vean afectados. Es importante tener en cuenta la evaluación al personal que interviene en el departamento, que conozca y le den un grado de importancia a los riesgos que puedan ser identificados, para lo cual deben estar plenamente involucrados en cada proceso.

2.4.2.2. Identificar Procesos Críticos

Los procesos críticos son aquellos que la organización considera como vitales para su funcionamiento, y que en caso de ocurrencia de algún siniestro en alguno de ellos el tiempo de reacción debe ser inmediata y evitar en lo más posible que afecte a la organización o que fallen otras partes de la misma.

2.4.2.3. Técnica de Análisis de Procesos

Considerando para el uso de la técnica de análisis de procesos:

- Para poder analizar el ciclo de vida de los procesos, se realiza una descripción de estos que tiene que estar basada y alineada con las metas que se han propuesto para el negocio, mientras también se hace uso de los recursos disponibles que se describieron anteriormente en el proceso.
- Un proceso se mantiene fijo cuando los recursos que va a utilizar son asignados al mismo.
- Los procedimientos que se van a llevar a cabo pueden realizarse de forma automática o también de forma manual, es decir que un miembro del equipo de trabajo o un grupo de trabajo del mismo lo siga.
- Todo el proceso que se va llevando a cabo debe estar siempre supervisado, controlado y también debe registrar informes de proceso.
- Luego de realizados los procesos anteriores, la documentación obtenida es evaluada. Una descripción del proceso es vital para comenzar con un informe actual del mismo, supervisarlo y revisarlo para la respectiva documentación.

2.4.3. Fase 3. Identificación de Soluciones

No debe quedar únicamente en especificaciones de que se puede hacer en caso de suscitarse un siniestro, sino comenzar con el plan de acción que contemple todos los procesos institucionales que bien pueden ser manuales o automáticos y además evaluarlos en base a la cantidad de información que

transmiten o la importancia en el esquema del proceso que llevan a cabo y también definir concretamente la criticidad de cado uno de ellos. La magnitud del plan de contingencias siempre se evaluará en acuerdo a la criticidad establecida de los procesos, su complejidad, importancia dentro de los procesos institucionales y costo total que genera.

Se deben determinar objetivos de alcance total en función de la criticidad y tiempo de trabajo de cada proceso, definir las dependencias e impactos de la organización que son necesarias para poder implementar una alternativa para las posibles problemáticas a encontrar.

2.4.3.1. Identificación de Alternativas

Para poder identificar unas buenas alternativas, se debe tener en cuenta que es crítico contar con los planes de administración de emergencia o de recuperación ante los fallos, aunque de no contar con ellos, se puede consultar los procedimientos hechos anteriormente y definir las mejores alternativas de solución. Algunos de los consejos para la identificación de las alternativas son:

- Planificar las necesidades adicionales del personal
- Tener métodos de concurrencia por algún caso de falla en los sistemas automatizados.
- Tener una planificación adecuada.
- Procurar mantener todos los recursos necesarios.

2.4.3.2. Identificación de Eventos Activadores

Los eventos activadores son la mejor alternativa al momento de un plan de contingencia, porque en este punto se contemplan todos los eventos que por cualquier razón puedan desencadenar que se desate el siniestro afectando a la organización. La planificación, como se recalca en todo el proceso es muy importante para poder tener la mejor alternativa en cuanto se trata de contingencias, y estos activadores son los que van a permitir que en el caso de que el fallo ocurra; se dé paso a la aplicación del plan de contingencias.

Los eventos activadores están enfocados en los procesos o sistemas mismos. Algunos de los que estos eventos que pueden considerarse como activadores son los siguientes:

- Retraso en la comunicación en cuanto a la ocurrencia de un fallo en su entorno de trabajo, sea este propio o de responsables alternos.
- Identificación de problemas que no hayan podido ser detectados de forma más temprana.
- Mantenimiento de datos que no son confiables, de fuentes no autorizadas o que tengan problemas en su correlación de autenticidad (datos corruptos).
- Problemas de entorno físico, que sean provocados por eventos inevitables o evitables.

- Falla con la infraestructura de la empresa pública proveedora de servicios básicos hacia la organización (comunicaciones, energía eléctrica, telefonía, entre otros)

2.4.3.3. Fallas Genéricas Funcionales de los Sistemas

Según lo especificado por INEI en su metodología, existen fallas que son generales propensos a ocurrir para activar un plan de contingencias. [3]

Las fallas más comunes que se pueden presentar son:

- Autentificación
- Cifrado
- Implementación
- Confianza Implícita
- Compartimiento implícito
- Desconexión de línea
- Descuido del operador
- Contraseñas
- Residuos
- Blindaje

2.4.4. Fase 4. Estrategias

Las estrategias de continuidad en recuperación de los negocios deben estar enfocadas hacia el diseño de herramientas de identificación de prioridades y así mismo determinar las soluciones a los problemas encontrados críticos,

para así resolverlos en referencia a su importancia dentro de la organización y que los riesgos que interfieren hacia los mismos sean minimizados en lo más posible; buscar opciones de recuperación más rápidas, y dependiendo a quién afecta las contingencias resolverlas basándose en los responsables directos de los procesos dados.

2.4.4.1. Actividades Importantes

- Hay que mantener una revisión de los procesos internos, de la forma en que se llevan, responsables, funciones, dependencias, nivel de importancia.
- La revisión del cronograma establecido en un principio y desechar las tareas que se consideren en este punto innecesarias, repetidas o que tal vez tienen una fecha de cumplimiento errónea para poder establecer nuevamente un calendario real de cumplimiento de metas establecidas.
- Buscar el establecimiento de soluciones de acuerdo a las personas y a sus funciones, y además basarse en la o las áreas donde estén mucho más enfocados los riesgos de ocurrencia de problemas y contingencias para establecer estrategias globales.
- Buscar la aprobación de parte de las grandes partes de la organización, que en casos pueden ser gerentes, accionistas mayoritarios, rectores, superiores, entre otros, para poder tener la apertura de aplicación de las estrategias y más que todo en el caso de necesitarse; el financiamiento para poder establecer las soluciones.

- Identificar los beneficios que serán traídos a la organización mediante la aplicación de las estrategias para mejorar aspectos claves de la misma y además que el presupuesto que se gastó en la aplicación del plan de contingencias, sea justificado y potencie los beneficios de la misma.

2.4.4.2. Preparativos de Identificación de Soluciones Preventivas

Las soluciones preventivas deben establecerse y cubrir los aspectos esenciales de protección en la organización que cuenta con las siguientes características:

- Mantener de forma ordenada y adecuada los respaldos de información es muy importante y hay que hacerlo con frecuencia, estos respaldos pueden estar en cualquier medio. El aspecto más importante es que debe respaldarse únicamente la información y no las aplicaciones.
- Mantener en vigencia todos los sistemas de antivirus para emergencias que se puedan presentar.
- Mantener la documentación de todo el sistema manejado en medios magnéticos e impresos, ya que se necesita mantener un respaldo en caso de problemas directos con los fabricantes de dichos sistemas (físicos o lógicos, es decir equipos y aplicativos de cualquier tipo)

2.4.5. Fase 5. Documentación del Proceso

La documentación de planes de contingencia es un proceso en donde se identifica todo lo descrito anteriormente y se va desarrollando el plan. Las soluciones aquí son implantadas y se citan las fuentes de documentación necesarias para que esta sea complementaria del proceso de realización del plan de contingencias.

2.4.6. Fase 6. Realización de Pruebas y Validación

2.4.6.1. Plan de Recuperación

Básicamente en la recuperación de desastres lo que se busca es llegar a una acción para cada caso de posible falla que pueda presentarse en el área donde se enfoca el Plan de Contingencias. Al ocurrir una contingencia, se debe estar preparados y el plan de recuperación de desastres debe ser puesto en marcha de inmediato para conocer cómo proceder ante cierta catástrofe. Hay que estar pendientes de los detalles de ocurrencia del desastre, es decir los motivos por los cuales se originó y el daño que se produjo, en tanto a la elaboración de procedimientos hay que determinar los casos de emergencia, cómo serán ejecutados y probados.

Los procedimientos que se dan son:

2.4.6.1.1. Actividades Previas al Desastre

Las actividades a llevarse a cabo buscan la prevención de que la ocurrencia de un desastre sea de gran magnitud; prepararse y planificar la acción de actividades para poder tener respaldo de la información. Hay que definir los procedimientos formales para cumplir las actividades previas a un desastre, que son las siguientes:

2.4.6.1.1.1. Establecimiento de Plan de Acción

Para esta fase, los procesos y procedimientos que intervienen son:

- **Sistemas e Información**

  Mantener organizados los sistemas de información, para que así los mismos entes pertenecientes a la organización tengan conocimiento de la información que se va a tratar y así se pueda llevar de manera adecuada la propia organización.

- **Equipos de Cómputo**

  Mantener un inventario de equipos actualizado de todos los documentos correspondientes a los activos empresariales, sean estos de cualquier tipo.

- **Obtención y almacenamiento de los Respaldos de Información (Back ups)**

  Realizar un calendario y buscar el respaldo de la información que en toda organización es de importancia crítica para su funcionamiento [15], este proceso debe seguirse y realizarse, de preferencia en horarios donde sea

menos accesada la información por usuarios internos o externos de la organización. Los aspectos a tomarse en consideración para los respaldos o “back ups” son:

- Sistema Operativo
- Software Base (Software que interactúa con aplicaciones institucionales)
- Software Aplicativo (Software adicional)
- Bases de Datos
- Hardware

- **Políticas (Normas y Procedimientos de Back ups)**

  La recolección y seguimiento de todas las normas establecidas por parte de la organización es un punto clave, debido a que hay que respetar todos los procedimientos previamente establecidos en el funcionamiento de la misma. También hay que enfocarse en la creación de normas y procedimientos para los respaldos que se van a generar para poder llevar a cabo el trabajo de forma segura. Se incluyen los siguientes puntos:

- Periodicidad
- Formulario de Registro de respaldos
- Constatación del espacio físico

- Reemplazo de respaldos después de cierto tiempo.
- Almacenamiento físico en distinto lugar de donde se encuentra la información
- Pruebas periódicas de los respaldos.

2.4.6.1.1.2. Formación de Equipos Operativos

Dentro del contexto del equipo operativo para la realización del proyecto, hay que poner en práctica los conocimientos adquiridos y buscar el personal adecuado para cada tarea que se ha planteado realizar durante el establecimiento del proyecto.

Basarse además en el conocimiento de las personas que serán postulantes al equipo, verificando las áreas de fortaleza en las que puede ser un apoyo fundamental; o sino verificando en qué áreas tiene un desempeño menor para evitar cruzarse con problemas futuros.

Basta indicar que en éste punto para el proyecto actual, no se aplica la formación de equipos, y los pasos de formación del equipo van a reprimirse. Pero se indica cuáles son los más importantes puntos que se deben tener en la conformación de dichos equipos:

- Contar con el personal capacitado para soporte técnico.
- Capacitar al personal sobre las actividades.

- Supervisores de respaldos, carga de archivos, activos y seguridad.
- Organizador de pruebas (tanto hardware como software)
- Recuperador de archivos perdidos.
- Personal de prueba de los puntos anteriores.

2.4.6.1.1.3. Formación de Equipos de Evaluación (Auditoría de Cumplimiento de los Procedimientos sobre Seguridad)

Se considera como fundamentales los aspectos siguientes:

- Revisión de normas y procedimientos (Políticas)
- Supervisión de los respaldos realizados
- Revisar la relación que guardan los sistemas internos con los respaldos de información
- Informes de los cumplimientos o no de las normas y políticas de acción.

2.4.6.1.2. Actividades Durante el Desastre

2.4.6.1.2.1. Plan de Emergencias

Se establecen las diversas actividades o acciones que van a tomar lugar de ejecución cuando se presente un siniestro o problema, igualmente los escenarios en los cuales se puede presentar el problema; y también, difundir las acciones esperadas por parte de las personas del departamento u organización.

Debe establecer los pasos y acciones que deberán ser seguidas por parte de las personas y ser detalladas de manera concreta para que todos puedan comprenderlos.

2.4.6.1.2.2. Formación de Equipos

En este punto pueden establecerse los equipos desde dos fuentes distintas, el agente proveedor del plan de contingencias, o por parte de las mismas personas de la organización (en este caso puede intervenir el Departamento de Informática de la organización en caso de contar con este). Es posible este tipo de equipos ya que pueden adoptar netamente la observación externa por parte de organizaciones ajenas a aplicar el plan o, por otra parte se puede tener un equipo no numeroso de personas internas que monitoreen el comportamiento de los objetos estudiados por parte del plan y les den su propio seguimiento. Estos equipos de trabajo a su vez deben estar divididos en 2 grupos; el primero el encargado de erradicar el siniestro y el otro encargado de salvaguardar la información que sea posible durante la ocurrencia de dicho siniestro, basándose en prioridades y respecto a las personas que estén en cada equipo.

2.4.6.1.2.3. Entrenamiento

Se trata de mantener a las personas involucradas en constante aprendizaje sobre ocurrencia de los siniestros, además deben saber exactamente la forma

de proceder y así evitar la pérdida de tiempo en cuanto a recuperación de la mayor parte de información, activos y software se trata.

Se debe tomar conciencia de que cualquier problema que se presente, si no se trata de manera adecuada, puede causar un daño mucho mayor a la organización y hay que otorgarle la importancia debida para solucionarlo; antes de que se forme un siniestro de mayor complejidad.

2.4.6.1.3. Actividades Después del Desastre

Una vez que un problema o catástrofe se ha presentado en la organización, y siguiendo las debidas correcciones que se han planteado anteriormente, hay que realizar las evaluaciones de resultados que ha dejado el suceso tales como:

2.4.6.1.3.1. Evaluación de Daños

La evaluación de daños es la parte más importante después de ocurrida una contingencia, ya que aquí es donde se observa cuál fue el daño ocasionado a la organización y en qué magnitud la afectó, en el caso de existir problemas operativos ya sean físicos o por parte de software que sufrió percances y no trabaja adecuadamente.

2.4.6.1.3.2. Ejecución de Actividades

La acción inmediata de las personas responsables que intervienen en la recuperación de la organización después de ocurrida una contingencia es clave, ya que es necesario el funcionamiento normal y continuo de la misma; y evitar que salga del funcionamiento de sus actividades para evitar pérdidas de cualquier tipo.

2.4.6.1.3.3. Evaluación de Resultados

Debe darse la evaluación respectiva de los resultados obtenidos para poder realizar un informe de situación actual después de ocurrida una contingencia y permitir saber cuál fue el daño dado, y en el caso saber si fue de total recuperación.

2.4.6.1.3.4. Retroalimentación

Tomar en cuenta todos los pasos anteriores, para así tener una bitácora histórica de los sucesos pasados, cuáles fueron las medidas adoptadas, cuál fue el daño generado, y si la recuperación dependía de mucho o mediano esfuerzo para poder realizarla.

2.4.7. Fase 7. Implementación

Ésta fase es el plan de acción una vez que se ha desatado una contingencia y es para lo que las 6 fases anteriores de la metodología han estado preparando a la organización. Aquí en el momento de que ocurra o esté por ocurrir la contingencia deben tenerse presente los planes mencionados que se ejecutarán, las medidas adecuadas que van a ser útiles para cada proceso y de qué forma y en qué orden deben ejecutarse.

2.4.8. Fase 8. Mantenimiento

Se hará un seguimiento de lo acontecido y cada cierto tiempo se realizarán actualizaciones de la documentación y nuevos estudios que puedan afectar de forma positiva al plan establecido, ya que con el tiempo las necesidades y riesgos van variando, ya sean por nuevas tecnologías, nuevos equipamientos, nuevas administraciones, nuevo personal, entre otras. Por ésta razón el mantenimiento es la parte más importante de toda la metodología.

Hay que recalcar que las fases 7 y 8 no van a ser ejecutadas en el presente proyecto, por tanto únicamente se nombra el rol que tienen dentro de la metodología.

CAPÍTULO III.

DESARROLLO

3.1. Resultados

Las herramientas utilizadas son proporcionadas por la norma ISO, para basarse en los estándares establecidos. En caso de utilizar otra herramienta, se mencionará de igual manera.

A continuación se detallan las fases de la metodología utilizada para la realización del plan de contingencias y sus resultados.

Fase 1. Planificación

1.1. Diagnóstico General

La Pontificia Universidad Católica del Ecuador Sede Ambato, es una institución de educación superior que atraviesa por procesos de acreditación contantes establecidos por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES), para mejorar en la calidad de entrega de sus servicios; así entonces es necesario que para realizarlo su estructura esté alineado a los parámetros establecidos.

El Departamento de Tecnología de la PUCESA pasa por cambios y desarrollos contantemente, y de acuerdo a esta evolución de la institución actualmente no se lleva un registro formal en sus procesos

de contingencias y es por eso que surge la necesidad de un control en cuanto a los mismos.

La infraestructura del departamento se encuentra ubicada en el cuarto piso del Bloque 1 de la institución, y cuenta con un data center (centro de datos) donde se encuentran ubicados los mismos. Como se indica por parte del personal del departamento, no se tienen documentos de control que permitan y determinen un manejo de lo realizado, no existen registros de control para accesos formales, no se tienen políticas que manejen la incidencia de algún problema. Actualmente con la implementación de su HelpDesk se puede tener registro de todo lo que se realiza a pedido de los usuarios, pero es un tema que se encuentra en proceso de formalización.

La información sobre aquello que maneja el departamento no se encuentra actualizada y por tanto no se puede hacer uso de la misma en cuanto sea necesario.

El personal tiene pleno conocimiento de lo mencionado anteriormente y en acuerdo total con el mismo se conoce que no existe una delimitante en cuanto a sus funciones. El acceso físico a los servidores no tiene un control de quién ingresa y realiza trabajos dentro del mismo, y por tanto la falta de control es un factor latente en cada aspecto. Actualmente se cuenta con 5 personas quienes están al frente de las actividades y manejan todo lo relevante con el departamento.

1.2. Organización Estructural

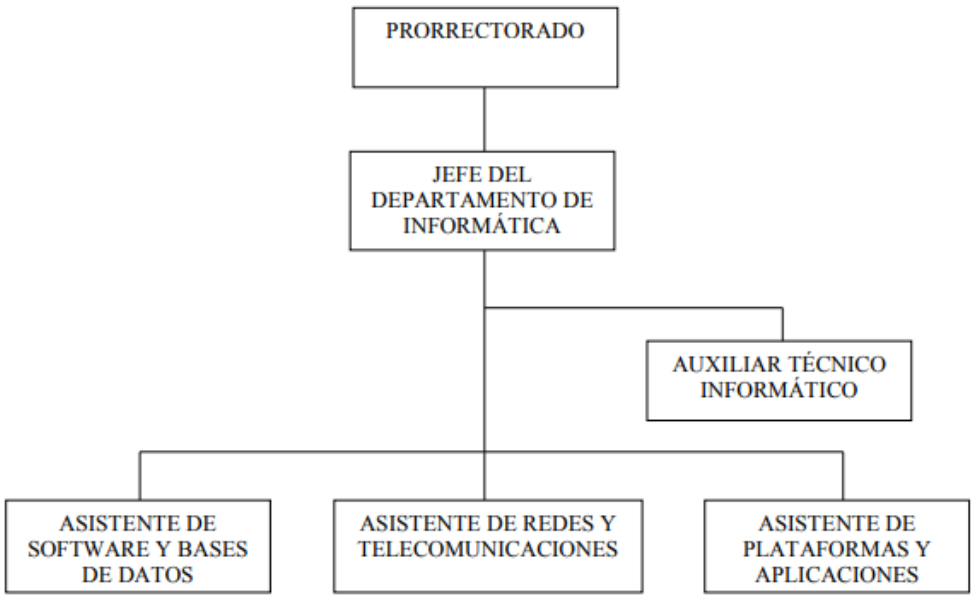


Gráfico 3.1. Organigrama
Fuente: Pontificia Universidad Católica del Ecuador Sede Ambato

La organización estructural es definida por la institución ya que establece una jerarquía en base a como se manejan los procesos y como es el escalamiento, además de quienes intervienen. Es fundamental la revisión del organigrama, ya que así se definen responsables para cualquier problema que se presente y se da el debido seguimiento correctivo por parte de las líneas superiores directas.

1.3. Inventario de Recursos

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO					
INVENTARIO HARDWARE Y SOFTWARE DE SERVIDORES					
	EQUIPO VIRTUALIZACION	EQUIPO VIRTUALIZACION	EQUIPO VIRTUALIZACION	ACADEMICS	SQUARENET/SACI
GENERAL					
Marca	HP	HP	HP	Esxi 6.0	HP
Modelo	ProLiant DL380p Gen8	ProLiant DL380p Gen8	ProLiant DL380p Gen7	VMWare Plataforma Virtual	Proliant ML370 G6
SISTEMA OPERATIVO					
Nombre	VMWare vSphere 6 Essentials	VMWare vSphere 6 Essentials	VMWare vSphere 6 Essentials	Windows Server 2008R2 64bits	Windows Server 2008R2 64bits
PROCESADOR					
Modelo	Intel Xeon E52650 2.0GHz	Intel Xeon E52650 2.0GHz	Intel Xeon X5690 3.47GHz	Intel Xeon E52650 2GHz(4 Vcpu)	Intel Xeon E5649 2.5GHz
MEMORIA					
Fisica Instalada	48GB	48GB	12GB	6GB	8GB
RED					
IP	192.168.1.236	192.168.1.237	192.168.1.238	192.168.1.244	192.168.1.242
Nombre Equipo	esxamb01	esxamb02	esxamb03	PRDAMB01	SRV_INT
Dominio	n/a	n/a	n/a	n/a	pucesa.red1.int
ALMACENAMIENTO					
Unidad C(/):	500GB	500GB	500GB	80GB	931GB
Unidad D:				200GB	n/a
Unidad E:					
Unidad F:					
SOFTWARE					
	ESXi 6.0 Sistema Virtualizacion	ESXi 6.0 Sistema Virtualizacion	ESXi 6.0 Sistema Virtualizacion	SQL Server 2008R2 Standard Edition	Sistema Financiero SACI
				Sistema Academico	Sistema SQUARENET

Tabla 3.1. Inventario de Hardware y Software
Fuente: Departamento de Informática PUCESA
Realizado por: Ing. Eduardo Remache

En cuanto a inventario de recursos se puede verificar que los equipos con los que se trabaja son adecuados, basados en las características y en las adecuaciones dadas como la capacidad de memoria, disco y procesador. El sistema operativo Windows Server 2008 implementado para las aplicaciones SquareNet, SACI y Academics tiene característica de seguridad bastante imponentes como la protección del kernel, mejoras en los registros, prevención ante la ejecución de datos, integridad del código, entre los más importantes. La versión de servidor de Moodle es bastante segura y debido a la arquitectura en la cual está montada como es Linux Centos, proporciona seguridad en cuánto a la incidencia de ataques, primero porque Centos es bastante seguro y cuenta con varias mejoras en base a sus antecesores,

como la inclusión de un canal de fibra sobre Ethernet o soporte para tarjetas Ethernet 40G y también el soporte para UEFI entre las más destacables; y después, Moodle también tiene incorporado sus propias seguridades y características que permite que los ambientes de aulas virtuales puedan crearse con diseños interactivos y amigables al usuario.

1.4. Planificación

Se establecen los alcances del Plan de Contingencias, en acuerdo con el personal del Departamento; una vez definido, se tratan las aplicaciones: Moodle-EVAE, Sistema Administrativo Contable Informático (SACI), SquareNet; se procede con el levantamiento de herramientas de control que tienen la función de mantener organizados y seguros aquellos recursos que intervienen en los mismos sean estos tanto hardware como software.

En la planificación global se establecen los procesos a realizarse para poder asentarse los riesgos. Se especifica por parte de la norma ISO 27001 el uso de anexos claves para lograr la seguridad buscada. Hay que especificar además los prefijos que componen los mismos que son:

PUCE: Pontificia Universidad Católica del Ecuador

SA: Sede Ambato

DI: Departamento de Informática

DOC: Documentación

CON: Constancia

Una vez detallado lo anterior, se pueden enlistar los documentos a utilizar y una breve descripción de cuál será la función dentro del Plan de Contingencias:

- **PUCE_SA_DI_DOC01_Políticas_Seguridad.** Su función es la de establecer políticas a seguir hacia aspectos que intervienen con la información.
- **PUCE_SA_DI_DOC02_Respaldo_Servidores.** Similar a una bitácora, pero es un documento de entrega y realización periódica.
- **PUCE_SA_DI_DOC03_Metodología_Evaluación_Tratamiento_Riesgos**. Documento de cómo se debe proceder para tratar un riesgo.
- **PUCE_SA_DI_DOC04_Plan_Tratamiento_De_Riesgos.** Clasificación de riesgos e identificación de responsables y recursos.
- **PUCE_SA_DI_DOC05_Cuadro_Evaluación_Riesgos.** Categorías de las amenazas.
- **PUCE_SA_DI_CON01_Bitácora_Revisión.** Documento de constancia de revisiones en general (adaptable a la necesidad).

Esta fase de la metodología es la que ayuda a la definición y marco de acción de lo que se hará en los siguientes pasos, y por tanto su establecimiento debe ser de manera correcta y delimitada de la mejor manera posible.

Fase 2. Identificación de Riesgos

Es netamente basado en el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI), para proceder de manera correcta se establece la limitación del alcance, es decir que únicamente se llegará a los servidores de aplicaciones que intervienen en el proceso de las aplicaciones tomadas en cuenta (Academics, Moodle-EVAE, SACI, SquareNet). En orden de priorización establecido por la norma ISO se tiene:

1. Personal
2. Elementos tangibles (Hardware)
3. Elementos intangibles (Software, Información)
4. Comunicaciones e infraestructura (Energía Eléctrica, Redes, Ventilación)

El personal del departamento, tiene dentro de sus funciones el manejo específico de las aplicaciones y son responsables de su operación funcional.

Los procesos críticos son tomados en base a la seguridad de los servidores que contienen a las aplicaciones consideradas críticas, se ha realizado el análisis de cada uno de los sistemas, han sido levantados los procesos que se dan y se determina igualmente el siguiente análisis por cada aplicación.

- **ACADEMICS**

Es el sistema de gestión de la Universidad, alojado en los servidores de aplicaciones del data center de la institución, el cuál es eje principal de fuentes de información correspondiente al ámbito estudiantil de la misma; es decir dentro de éste sistema se obtiene información netamente relacionado con el proceso educativo de los estudiantes, docentes, calificaciones, evaluaciones docentes, syllabus, tutorías, investigación, vinculación, entre otros. Se considera un ERP completo debido a que integra varios módulos en su función, y su estructura es diferente a como estuvo implementado en un principio los procesos que se manejan en el sistema, es decir en procesos de módulos islas; sino ahora es mucho más completa y funcional adaptándose al trabajo en conjunto de los componentes que intervienen en el software.

Cuenta con 28 módulos y basado en los procesos que realiza, la observación e información del administrador de la aplicación, se toman como los más importantes los 3 siguientes módulos:

Hojas de aranceles

Este módulo dentro del sistema tiene un nivel elevado en cuanto a seguridad de información, debido a que en el llenado de la hoja de aranceles se dan procesos muy importantes como la selección de las asignaturas y consecuentemente se obtienen los costos reales a pagar para continuar con la matriculación.

Calificaciones

Dentro del módulo de calificaciones intervienen docentes y estudiantes y es donde se encuentra el ingreso de calificaciones por los parciales establecidos, además de que también se puede constatar el número total de faltas o inasistencias al alumno. Dentro de este módulo se ratifica la aprobación o no del semestre de un alumno dependiendo del número de faltas, calificación y el número de créditos.

Syllabus

La acreditación de instituciones de educación superior ha motivado para que la planificación llevada por los docentes, que anteriormente era informativa para los mismos, hoy en día sea una fuente de información académica de la materia, además de que todos los estudiantes puedan tener acceso a ésta planificación y **dar seguimiento a los temas desarrollados cada semana.**

MÓDULOS

Becas

En el módulo “Becas” se da el proceso del otorgamiento y la aplicación de la beca sobre la hoja de aranceles.

Cierres de ciclo

Se procede con el cierre de semestre de una materia y su auditoría por parte de las secretarías de escuela y la secretaría general.

Control de biblioteca

Aquí se manejan las donaciones de libros, por parte de estudiantes.

Convalidación y equiparación

Procesar las convalidaciones y equiparación de materias entre escuelas, sedes de la SINAPUCE y otras universidades.

Dirección de estudiantes

Validación de estudiantes quienes obtienen beca.

Evaluación académica

Abarca todos los componentes para el cálculo de la evaluación docente, proceso que se realiza dos veces por año y se lo determina en tres categorías que son Docencia, Vinculación, Investigación.

Evaluación docente

Actualmente no se utiliza. Considerado como módulo de consulta histórica. Utilizado hasta el año 2013 para evaluaciones pero su objetividad no estaba muy clara, por lo que el proceso se renovó, aunque el módulo se mantiene.

Ingreso graduados

El seguimiento de graduados e ingreso de los mismos se realiza en éste módulo, se da control al cambio de roles de los estudiantes por medio de tablas de estudiantes a graduados. Se da el ingreso al sistema de los graduados.

Inscripciones

Proceso de Dirección de Estudiantes para los aspirantes a estudiantes, se registran en un formulario web, con sus datos. Los registros hechos se guardan en la base de datos y sólo hasta que el proceso continúa los usuarios cambian de estatus de Inscritos a Matriculados y también pasan a ser Estudiantes.

Todos los estudiantes poseen un perfil para manejo de reglas establecidas y acceso al sistema.

Integración Moodle

Dentro de éste módulo es donde se extraen las notas de cada actividad directamente de la plataforma Moodle al sistema académico.

Matriculación

Manejado por Secretaría General por asuntos de auditoría. Se procede con el establecimiento de un estudiante a matriculado.

Parámetros carrera

Aquí se encuentra los formularios de parametrización de datos, que nos permiten dar mantenimiento a tablas estáticas y manejabilidad de datos.

Parámetros generales

Módulo de formularios donde se manejan en estándar mucho más amplio el conocimiento de parámetros generales.

Pedidos

Los pedidos se ejecutan a través del área de desarrollo. Interviene desarrollos en cuanto a hojas de aranceles.

Pensión diferenciada

Gestión documental de la información requerida, guarda archivos PDF. Además aquí se produce la aceptación y la verificación de los datos ingresados.

Procesos

Módulo del antiguo proceso de inscripciones.

Inscripciones

Módulo que ayuda a la inscripción de los estudiantes, que reemplaza al anterior “Procesos”.

Proyectos de vinculación

Contiene los módulos para el ingreso de los proyectos seguimiento, registro de horas de vinculación y la impresión de los proyectos de vinculación.

Permite rescatar los informes mensuales de los proyectos de vinculación estos auditados por el responsable del proyecto.

Reportes

Toda la reportería del sistema de información se encuentra dentro de este módulo.

Reportes postgrados

Igual función que el módulo Reportes, pero para postgrados.

Reportes secretarias

Dentro de éste módulo se puede evidenciar las asistencias del personal y las evidencias.

Seguimiento a graduados posgrados

Está basado en las experiencias laborales de los titulados de posgrados y donde se van tomando encuestas basadas en el desempeño laboral

Seguridades

Aquí se manejan las cuestiones personales de usuario en cuanto al acceso del sistema, como el cambio de contraseñas (6 meses para la actualización), también las preguntas de seguridad (3 preguntas)

Soluciones biblioteca

Contiene los formularios de los formatos para donaciones bibliográficas

- Tiene que ser parte de los estudiantes aptos para ser Disertantes
- Sistema de donaciones bibliográficas (bitácora de libros donados), la misma que se actualiza cada 2 meses aproximadamente.

Tutorías

Registro y control tutorías registrada por parte de los maestros para el posterior seguimiento y retroalimentación de los estudiantes.

Análisis de Confiabilidad de la aplicación

Para realizar un análisis de la seguridad en cuanto a la aplicación se utiliza la aplicación VEGA. Se revisan las vulnerabilidades y se establece el marco de acción.

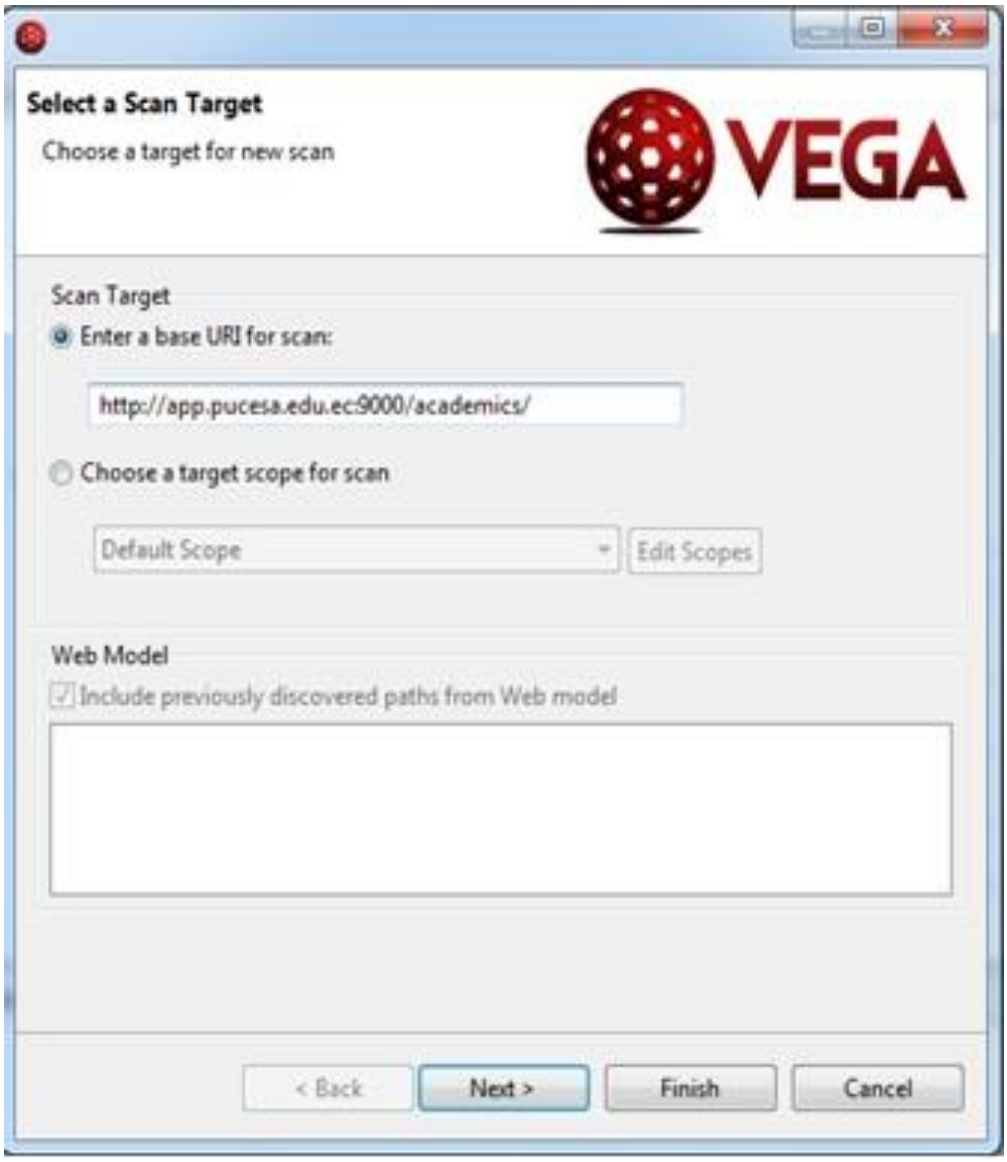


Gráfico 3.2. Target para VEGA de ACADEMICS
Fuente: Aplicación VEGA

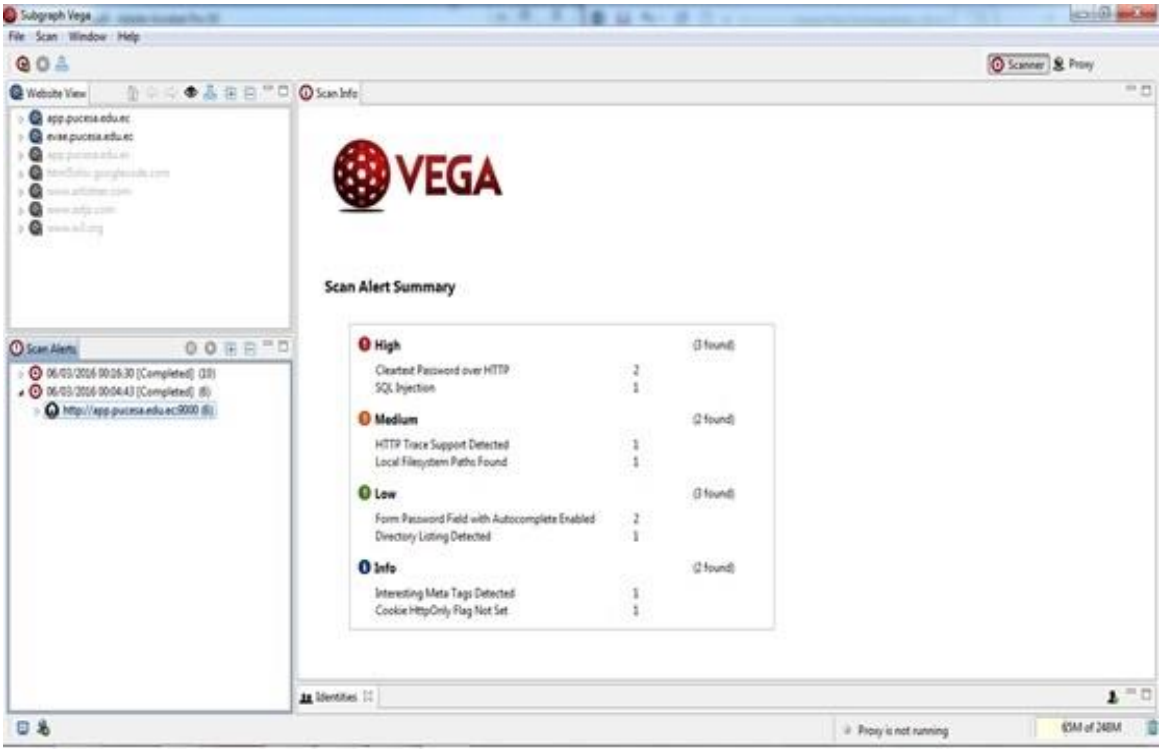


Gráfico 3.3. Resultado del escaneo de ACADEMICS
Fuente: Aplicación VEGA

Resultados

El error grave indica que, al no transmitirse por medio de un canal HTTPS, el riesgo de que la contraseña pueda ser interceptada es alto; y por tanto se lo toma como un riesgo alto. La medida a tomarse es que la contraseña no debe ser enviada como texto normal, sino encriptada.

Los errores menores son basados en la aparición de mensajes de error, que para resolverlos hay que evitar que estos desplieguen información que puede ser sensible o sino deben ser deshabilitados.

- **Sistema Administrativo Contable Informático (SACI)**

  Es el sistema financiero contable de la Universidad, que mantiene los registros financieros de la Universidad, es decir todos los movimientos contables realizados, es un software integrado utilizado para administrar las PYMES, su programación está hecha en Java, con la utilización de una base de datos en Oracle.

  SACI, es un aplicativo externo, que la institución lo adecuó con la asistencia del proveedor para su implementación y configuración; es por eso que sólo se dan aspectos base en cuanto a la aplicación, más no se profundiza porque incluso el personal del Departamento no tiene procesos definidos en cuanto al aplicativo; sino únicamente el soporte que se recibe es por parte del proveedor por medio de control remoto.

  El sistema contable SACI tiene varios aspectos dentro de su estructura que son de importancia para la institución, debe cumplir con parámetros importantes que avalen su confiabilidad, mencionando a continuación los mismos. El producto simplifica de manera razonable el trabajo y sus resultados son los esperados por parte de los miembros que utilizan el sistema que se ajustan a los requerimientos dados por las empresas. SACI es adaptable, debido a que los planes en los cuales trabaja el sistema SACI son bastantes flexibles. Su estructura funcional es bastante definible en cuestión de gustos y función de empresas se puede modificar a lo especificado por los clientes.

La facilidad con la que cada uno de sus módulos puede ser trabajado de forma independiente o correlacionada hace que el sistema SACI lleve la información de una manera íntegra e integrada entre sí mismo para que la transferencia entre aplicaciones sea automático. La manejabilidad y flexibilidad de relacionar la información a gusto del usuario permite ésta integración, ya que hay formas varias de manejo de la información.

No se profundiza más en la aplicación debido a que no se cuenta con la apertura por parte del proveedor que es quién gestiona todo lo referente a SACI.

Análisis de Confiabilidad de la aplicación

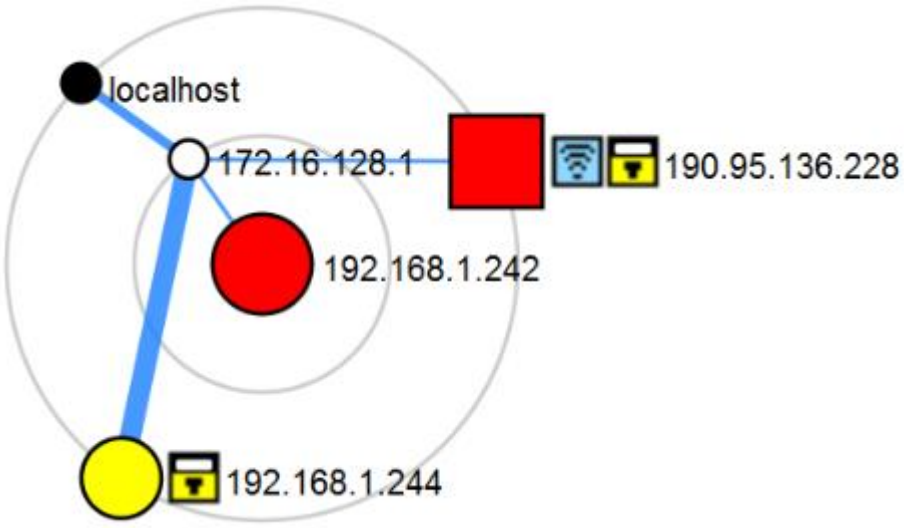


Gráfico 3.4. Topología de red para SACI
Fuente: Aplicación ZENMAP

Puerto	Protocolo	Estado	Servicio	Versión
21	tcp	open	ftp	vsftpd 2.2.2
80	tcp	open	http	Microsoft IIS httpd (Spanish)
1723	tcp	open	pptp	Microsoft
9000	tcp	open	http	Microsoft IIS httpd (Spanish)
9001	tcp	open	http	Microsoft IIS httpd (Spanish)
9003	tcp	open	http	Microsoft IIS httpd (Spanish)
9009	tcp	open	http	Microsoft IIS httpd (Spanish)
9011	tcp	open	http	Microsoft IIS httpd (Spanish)
9040	tcp	open	http	Microsoft IIS httpd (Spanish)
9050	tcp	open	http	Microsoft IIS httpd (Spanish)
9080	tcp	open	http	Microsoft IIS httpd (Spanish)
9081	tcp	open	http	Microsoft IIS httpd (Spanish)
9100	tcp	open	jetdirect	

Gráfico 3.5. Listado de puertos abiertos del servidor para SACI
Fuente: Aplicación ZENMAP

Se puede dar cuenta que en cuestión de la aplicación SACI no existen inconvenientes en cuanto a lo escaneado en la aplicación VEGA para vulnerabilidades por medio de filtros de la WEB.

Las medidas adoptadas actualmente son muy importantes para tener seguridad en base a los ingresos a la aplicación y se determina que no existen tampoco vulnerabilidades de filtros por medio de internet.

- **PLATAFORMA MOODLE**

La plataforma de educación implantada en la institución está basada en el esquema de la herramienta para aulas virtuales MOODLE. Está

desarrollada de manera segura y es un hito en aulas virtuales para educación; por lo que ha sido bastante utilizada en implantaciones similares en otras instituciones. Maneja varios reportes de seguridad, contiene políticas, manuales de usuario y para la cuestión de administración maneja procedimientos estrictos de seguridad.

Es controlada por el Departamento de Tecnología, y es a este al cual deben presentarse los distintos requerimientos que se tengan en la institución con lo relacionado a la creación, modificación o eliminación de cursos.

MOODLE que es la base en la cual está desarrollada la plataforma es un ente sólido para el desarrollo de plataformas virtuales, ya que cuenta con módulos basados netamente en la privacidad y normas de seguridad, además toma en cuenta aspectos como recomendaciones de seguridad para llevarse a cabo.

La Plataforma Moodle actualmente presenta una alta disponibilidad y asegura su servicio ya que ha sido migrada a una infraestructura cloud, lo cual ha hecho necesario un plan de contingencia que trata sobre replicación de la información. Como política de seguridad se ha establecido la creación de una instancia que es en donde se aloja el servidor web y un RDS el cual gestiona la base de datos MySQL

Al encontrarse alojada con los servicios de Amazon Web Services (AWS), Moodle necesita de una disponibilidad muy alta y las características de los servidores donde está asentada deben cumplir con requisitos que aseguren dicha disponibilidad.

Análisis de Confiabilidad de la aplicación

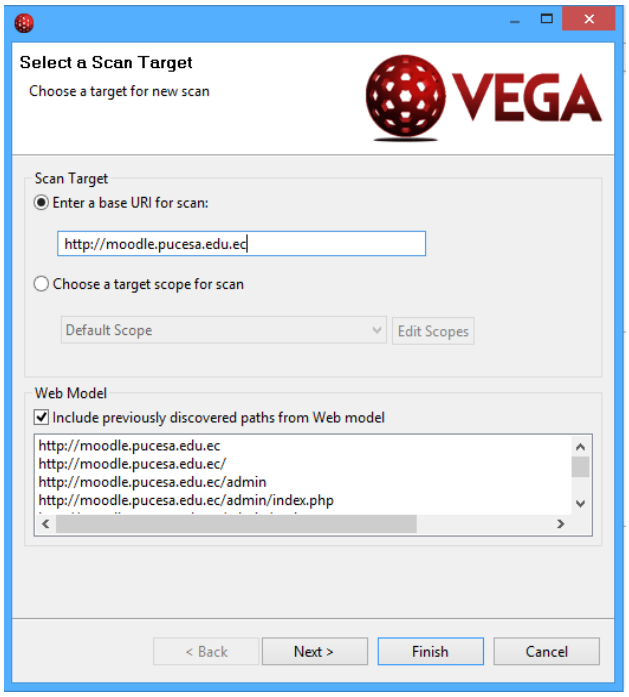


Gráfico 3.6. Target para VEGA de MOODLE
Fuente: Aplicación VEGA

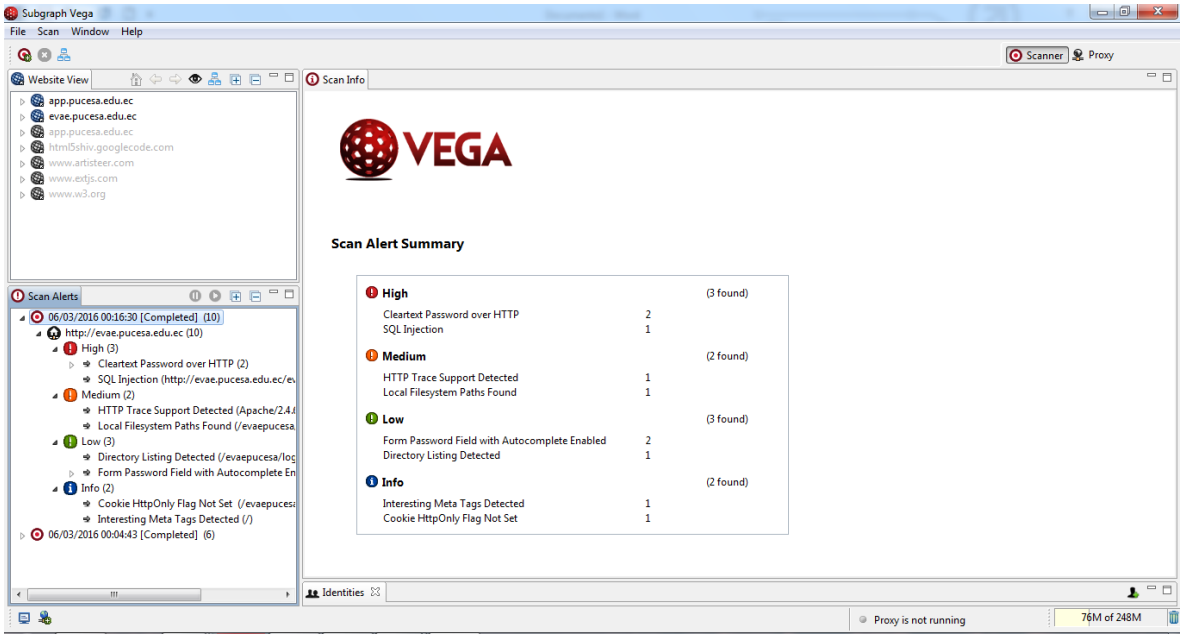


Gráfico 3.7. Resultado del escaneo de MOODLE
Fuente: Aplicación VEGA

Resultados

El primer error grave nos advierte algo similar como en ACADEMICS, así que la medida a tomarse es que la contraseña debe ser enviada encriptada. En cuanto al segundo la solución es utilizar instrucciones parametrizables y configurar los controles de acceso a la base de datos por el administrador. En los errores intermedios lo consecuente es que se tiene vulnerabilidades en cuestión de las contraseñas, ya que no se la cifra y además revela rutas en el código fuente que pueden ser aprovechadas por los atacantes.

Se debe, por parte del administrador del sistema, revisar los controles y la forma de definición de rutas para cambiarlas de ser necesario y no entregar información adicional que pueda perjudicar.

- **SQUARENET**

SquareNet integra varios módulos que adaptables y brinda un total apoyo en cuestión de control sobre las acciones que afectan a los empleados de la organización en el trabajo diario de una manera eficaz y fácil a las necesidades de la organización en donde se está implementando.

El sistema SquareNet es una herramienta modular que puede adaptar varios de ellos en su estructura, pero siempre debe contar con al menos

3 módulos base que son Control de Asistencia, Nómina y Recursos Humanos.

Recalcando para SquareNet igualmente, no se realizará un análisis ni se tomarán medidas muy profundas ya que este sistema también es externo y toda acción de soporte se da por parte del proveedor, mismo que indica que sólo se puede elaborar una descripción de procesos en base al sistema en sí con la documentación existente.

Los módulos aplicados en la institución son:

Asistencia

Dentro del mismo se asignan los perfiles de horario, manejados de forma genérica para la institución, se registran las marcaciones del personal. Aquí se asignan los valores correspondientes a horas extras y su aprobación, además de la justificación de ausentismos y vacaciones del personal de la institución Todo el proceso de marcación se lo realiza por medio del sistema de molinetes de la empresa Tech-IN quienes son los encargados de migrar la información correspondiente al personal de la institución.

General

Es un módulo donde se tiene especificado lo correspondiente a tributación y codificación dadas por la entidad gubernamental controladora de la misma (Servicio de Rentas Internas SRI). Además se tiene el módulo para justificación general de asistencia para días festivos en donde el proceso individual sería repetitivo.

Nómina

Están especificados los procesos de integración del personal y asignados a un centro de costo que es dónde se lo referencia a una entidad de pertenencia, que en este caso se lo toma a la institución como un global. Además se maneja el descuento del impuesto a la renta y se elaboran las plantillas de rubros. Aquí se especifican también los roles de pagos, hay 3 tipos de roles generados para la institución que son: dependencia (contrato fijo), jubilados (personal que culminó su período de trabajo y se acoge a la pensión jubilar) y prestación de servicios (contrato temporal de prestación de servicios).

Existe también especificada la asignación de rubros fijos para el personal que debido a funciones propias de su cargo deben recibir un adicional para el cumplimiento de sus funciones y este se acredita al valor percibido mensualmente (en ésta categoría se encuentra el Prorrector y direcciones académicas, de estudiantes y administración superior).

Recursos Humanos

Aquí se encuentra la ficha de las personas, contiene con sus datos personales. La ficha de recursos humanos además establece el perfil de las personas para conocer su estado y sus diferentes actividades asignadas como su perfil de cuentas bancarias, experiencia, competencias, entre otras. Se establecen además los contratos en donde hay que establecer el formulario 107 para su continuidad.

Se encuentra también especificada la modularidad de capacitación y estudios en donde se registran los títulos de maestrías de las personas y donde se generan los reportes de la misma.

Sistema

Es el módulo de control de quién tiene registrados su equipo y sus usuarios disponibles para el uso del aplicativo. Aquí se pueden controlar las activaciones de los usuarios, su cambio de contraseñas, y el código al cuál están atados. Actualmente únicamente está siendo usado por parte de Diego Caicedo (Director Administrativo PUCESA) y David Camacho (Director de Talento Humano PUCESA).

Seguridades

Existen dos tipos de seguridades con los cuales se tiene registros para el acceso netamente de la aplicación SquareNet

1. Los computadores para el acceso necesitan obligatoriamente ser registrados por parte de la consola de administración, mediante el nombre del equipo para el rastreo de cambios y verificación de personas que no tengan acceso por fuera del dominio corporativo u organizacional o con nombre distinto del equipo registrado.
2. Dentro del segundo modo de control de seguridad están involucrados los perfiles y permisos, en los que se enfocan directamente en permisos a opciones dentro de cada uno de los módulos, que pueden ser de lectura, lectura y escritura o específicamente a un campo del formulario.

La política de seguridad no se reduce a los dos pasos anteriores, se enfoca también en mucho más que la integridad de los datos procesados por el sistema para que sean lo más transparentes posible y que los reportes llevados a cabo sean lo más precisos igualmente.

Seguridad en permisos a reportes

No todos los usuarios pueden ver reportes, sino se pueden especificar que usuario va a tener acceso a cierto tipo de reporte y además esto involucra que los reportes sean manejados independientemente para

que no exista confusión por parte de los usuarios a los cuales se les asigna un perfil.

Seguridad en permisos a procesos

La seguridad en cuanto a procesos es referente, se enfoca netamente en la capacidad de permitir que un usuario realice operaciones con la información registrada y referente de los miembros de la organización, un ejemplo claro donde se denota esos permisos es para la persona encargada del manejo de la nómina y de aprobar o registrar las horas extras realizadas por un usuario.

Seguridad para permisos tablas

Modificar, cambiar, eliminar es básicamente lo que se controla en los permisos a ciertas tablas. Existen registros de información que son muy importantes y críticos, por lo que si un usuario que no está autorizado llegara a cambiar o modificar, o incluso a borrar los mismos; esto causaría un grave impacto y no permitiría que el funcionamiento normal del flujo de información se lo lleve de manera normal, por tanto es necesario hilar hasta el punto de permitir que ciertos usuarios puedan modificar o alterar los registros, o los puedan borrar.

Dentro de SquareNet no se realiza el análisis ya que se encuentra en el mismo servidor de la aplicación SACI y por tanto comparten características del servicio.

Priorización de Aplicaciones

Para poder levantar los procesos, se han analizado cada una de las aplicaciones, su estructura y además su nivel de criticidad ha sido establecido por el propio personal del Departamento, mediante un cuestionario estructurado que se ha llevado a cabo. Los niveles de criticidad se han impuesto en que el número 1 es mayor prioridad y el número 4 menor prioridad:

	Moodle	Academics	SACI	SquareNet
Encuesta 1	4	3	2	1
Encuesta 2	1	2	3	4
Encuesta 3	1	2	3	4
Encuesta 4	2	1	3	4
Encuesta 5	1	3	4	2

Tabla 3.2. Tabulación de Encuestas
Fuente: Encuestas
Realizado por: Jonathan Llerena

Prioridad 1	3	1	0	1
Prioridad 2	1	2	1	1
Prioridad 3	0	2	3	0
Prioridad 4	1	0	1	3
TOTAL	5	5	5	5

Tabla 3.3. Priorización de Criticidad
Fuente: Encuestas
Realizado por: Jonathan Llerena

El alcance dado es llegar a la protección de datos de los servidores implicados en las aplicaciones de más alto impacto; por tanto, se han clasificado por orden de importancia igualmente las aplicaciones:

1. Moodle
2. Academics
3. Contable (SACI)
4. Nómina (SquareNet)

Fuentes de Investigación

Toda información a la cual se hace referencia, ha sido proporcionada por el Departamento de Tecnología de la PUCESA por medios electrónicos, además de las fuentes para la realización del Plan de Contingencias que ha sido la norma ISO/IEC 27001, que aporta con los pasos a seguirse y las herramientas a considerar para más adelante poder tratar adecuadamente los riesgos.

Comunicación

Para realizar y aplicar de manera efectiva la metodología y los procesos de identificación y minimización de riesgos, cada avance y modularidad de aplicación de las prácticas son socializadas con el personal del Departamento, que son los que van a determinar la utilidad, aplicabilidad y aprobación del Plan. La comunicación es un factor muy importante también, ya que así se

pueden conocer mejor los procesos que se llevan a cabo dentro del Departamento y también los recursos que se utilizan para brindar los servicios a la institución.

Riesgos

En base a la documentación dada por parte de la norma ISO 27001 dentro del PUCE_SA_DI_DOC05_Cuadro_Evaluación_Riesgos, se han tomado las siguientes entidades y riesgos específicos para poder evaluar los mismos. Se tiene el siguiente cuadro en dónde se especifican los riesgos y la categoría a la cual corresponde respecto a la clasificación dada por el mismo documento establecido por ISO.

No	Categoría	Intermediario, Equipo afectante y/o afectado	Riesgos
1	Personas	Empleados	Acceso físico no autorizado
2	Personas	Personas externas que visitan la organización	Daños provocado por actividades de terceros
3	TI, comunicaciones y demás equipamiento	Equipamiento de red	Acceso no autorizado a la red
4	Servicios tercerizados	Mantenimiento	Deterioro de soportes
5	Personas	Otros empleados	Error de usuario
6	TI, comunicaciones y demás equipamiento	Equipos	Fallas en equipos
7	TI, comunicaciones y demás equipamiento	Aire acondicionado	Incendio
8	TI, comunicaciones y demás equipamiento	Equipamiento de red	Interceptación de información
9	Servicios tercerizados	Suministro energía	Interrupción del suministro eléctrico
10	Infraestructura	Oficinas	Inundación
11	Personas	Otros empleados	Modificación accidental de datos del sistema de información
12	Infraestructura	Oficinas	Otros desastres
13	Servicios tercerizados	Mantenimiento	Pérdida de servicios soporte
14	Personas	Empleados	Revelación de contraseñas
15	Personas	Personas	Robo

Tabla 3.4. Cuadro de Evaluación de Riesgos
Fuente: Documentación ISO 27001
Realizado por: Jonathan Llerena

La priorización de los riesgos basados en la norma ISO; en acuerdo a la escala determinada por importancia en medida de que pueda ocurrir son:

1. Físicos
2. Naturales
3. Personal
4. Sistemas

Debido a lo encontrado, es posible que se determinen las contingencias a tratar, además de que la norma establece la lista de amenazas o riesgos que pueden encajar en el marco de acción del lugar en dónde está siendo implantada la norma. Se han tomado los siguientes riesgos para analizarse:

- Acceso físico no autorizado
- Daños provocados por actividades de terceros
- Acceso no autorizado a la red
- Deterioro de soportes
- Error de usuario
- Fallas en equipos
- Incendio
- Interceptación de información
- Interrupción del suministro eléctrico

- Inundación
- Modificación accidental de datos del sistema de información
- Otros desastres
- Pérdida de servicios soporte
- Revelación de contraseñas
- Robo

Análisis de Riesgos

Es necesaria la realización de una evaluación basada en cuestión a los riesgos identificados, y tomando como referencia la metodología del Instituto Nacional de Ciberseguridad de España (Plan Director de Seguridad) [16] se realiza el análisis de cada riesgo, basado en lo siguiente:

TABLA DE ESTIMACIÓN DE PROBABILIDAD	
CATEGORÍA	**RELACIÓN**
Bajo (1)	Se presentan aproximadamente una vez cada año.
Medio (2)	Se presentan aproximadamente una vez cada mes.
Alto (3)	Se presentan aproximadamente una vez cada semana.

TABLA DE ESTIMACIÓN DE IMPACTO	
CATEGORÍA	**RELACIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Tabla 3.5. Tablas de estimación de probabilidad e impacto
Fuente: Instituto de Ciberseguridad de España

Y para poder clasificar el riesgo se toma en cuenta la tabla de Probabilidad vs. Impacto y así se logra definir un impacto en cada uno de los riesgos:

		IMPACTO		
		Bajo	**Medio**	**Alto**
PROBABILIDAD	**Bajo**	Muy Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Muy Alto

Tabla 3.6. Tabla de probabilidad vs impacto
Fuente: Instituto de Ciberseguridad de España
Realizado por: Jonathan Llerena

Por tanto; se debe realizar el análisis y la determinación de cada uno de los riesgos y especificarlas en la tabla de probabilidad contra impacto

La seguridad de información es el ámbito más importante de protección, el valor de la misma es un solo núcleo en cuanto a las 4 aplicaciones críticas; ya que; hecho el análisis de estas se determina que las mismas no presentan probabilidad de fallo en cuanto a su seguridad; sino que hay que controlar los aspectos a las cuales están sometidas estas en el Data Center y los servidores como aspecto físico.

La norma de identificación de los riesgos establece que, en caso de ocurrencia de un riesgo de intensidad BAJA, no es necesaria la corrección inmediata;

pero si la toma de alguna medida de protección; y en caso de un riesgo con intensidad MEDIA o ALTA, buscar las medidas correctivas para evitar que la consecuencia de alguna de estas nos lleve a la pérdida de información.

Fase 3. Identificación de Soluciones

En base a los problemas mencionados anteriormente y los grados de impacto de los mismos en caso de presentarse; se presenta la descripción de los riesgos, y también sus responsables, la categorización dada y la observación. La solución adecuada para prevención del problema de pérdida de la información es la replicación de datos, basado en tecnologías en la nube. Es muy importante esto debido a que la utilización de las nuevas tecnologías de información siempre es clave y además de que son muy útiles Hay que recalcar que las mismas son descritas en el anexo dado por la norma ISO/IEC 27001 y que para el efecto se lo ha llamado PUCE_SA_DI_DOC04_Plan_Tratamiento_De_Riesgos. En este se detallan los riesgos de una forma general, para posteriormente entregar las soluciones que se detallan a continuación:

- Mantener inventariados los activos de tecnología del Data Center que se tienen para disponer de la información de los mismos en forma rápida con información actualizada. Levantar además la información acerca de lo que contiene cada uno de los servidores.

- Asegurar las condiciones de ambiente para el funcionamiento correcto de los equipos y asegurar la continuidad de entrega de sus servicios.

- Implementar el sistema de replicación de datos de los servidores para minimizar el riesgo de pérdida de información en caso de ocurrencia de algún problema.

- Definir las responsabilidades y un marco de acción de cada persona involucrada en el Departamento mediante un documento formal de las responsabilidades y actividades, las cuales estarán siendo cumplidas.

- Mantener un contrato de soporte y la comunicación adecuada con los proveedores de sistemas externos para que, en caso de no poder proceder con ayuda inmediata por parte del Departamento, ésta sea dada por los proveedores en el menor tiempo posible.

- Considerar la posibilidad de contratar una persona especializada para los sistemas externos que no son propios de la Universidad y que esté capacitado para poder desempeñar las funciones de soporte y resolución de problemas.

Descripción del riesgo	Recursos generales necesarios	Responsable	Nivel			Observación
			B	M	A	
Acceso físico no autorizado	Sistema de acceso seguro al personal	Jefe Departamental		X		Dar acceso sólo a quien sea necesario
Daños provocados por actividades de terceros	Sistema de acceso seguro al personal	Jefe Departamental		X		Dar acceso sólo a quien sea necesario
Acceso no autorizado a la red	Firewalls, actualizaciones de seguridad, sistemas de control	Asistente de Redes y Telecomunicaciones			X	Controlar los accesos de correo electrónico y redes
Deterioro de soportes	Personal de Mantenimiento	Auxiliar de Mantenimiento Técnico	X			Resguardar la infraestructura
Error de usuario	Capacitaciones en aspectos generales de infraestructura	Jefe Departamental	X			Buscar las mejores opciones de capacitación para el personal
Fallas en equipos	Registros históricos de lo realizado	Asistentes de Base de Datos, Plataforma y Aplicaciones, Redes y Telecomunicaciones, Auxiliar de Mantenimiento Técnico		X		Documentar todos los procedimientos
Incendio	Alarmas, extintores, detectores de humo, sistema de enfriamiento	Auxiliar de Mantenimiento Técnico, Jefe Departamental			X	Tener los sistemas de alarmas siempre vigilados y dar mantenimiento
Interceptación de información	Herramientas de control	Asistente de Redes y Telecomunicaciones			X	Utilizar herramientas y preparar al departamento para su uso.
Interrupción del suministro eléctrico	Generadores, UPS	Jefe Departamental, Auxiliar de Mantenimiento Técnico			X	Comunicación con las personas encargadas de toda la infraestructura
Inundación	RACKS, infraestructura adecuada, cableado estructurado, seguridad de acceso	Auxiliar de Mantenimiento Técnico, Asistente de Redes y Telecomunicaciones, Jefe Departamental		X		Respaldar la información debido a que no se pueden evitar desastres naturales
Modificación accidental de datos del sistema de información	Capacitaciones en aspectos generales de infraestructura	Jefe Departamental		X		Buscar las mejores opciones de capacitación para el personal
Otros desastres	Infraestructura en general	Auxiliar de Mantenimiento Técnico, Asistente de Redes y Telecomunicaciones, Base de Datos, Plataforma y Aplicaciones, Jefe Departamental		X		Evaluación de la infraestructura y levantamiento de observaciones en bitácora
Pérdida de servicios soporte	Personal del Departamento	Jefe Departamental		X		Preparación del equipo del Departamento para brindar apoyo en soporte base de reemplazo de algún miembro del equipo
Revelación de contraseñas	Personal del Departamento	Auxiliar de Mantenimiento Técnico, Asistente de Redes y Telecomunicaciones, Base de Datos, Plataforma y Aplicaciones, Jefe Departamental		X		Socialización de normas del departamento establecidas en la política de seguridad realizada
Robo	Personas internas o externas	Auxiliar de Mantenimiento Técnico, Asistente de Redes y Telecomunicaciones, Base de Datos, Plataforma y Aplicaciones, Jefe Departamental			X	Aseguramiento de la información con respaldos y de los equipos con garantía

Tabla 3.7. Plan de Tratamiento de Riesgos
Fuente: Anexo ISO/IEC 27001
Realizado por: Jonathan Llerena

El cuadro especificado es el anexo del tratamiento de riesgos una vez identificados los riesgos y su nivel de criticidad en base a lo determinado por parte del personal del Departamento.

Eventos Activadores

Los eventos que pueden disparar la ocurrencia de una falla o de un riesgo son determinados en base a la observación y la socialización conjunta con el

personal del Departamento. Ésta información está determinada en el Plan de Contingencias pero se la referencia a continuación:

- El no adecuado control de documentos de control y gestión del Departamento, es decir no existen políticas regulatorias, lo que genera que varias de las acciones correctivas que se dan no son formales.
- La infraestructura en mal estado y que no sea adecuada, la falta de los procesos formales de mantenimiento y tampoco contar con revisiones técnicas en un período de tiempo, incrementa el riesgo en los equipos.
- Los fenómenos naturales son eventos activadores por seguro debido a que al momento de ocurrir se verán afectadas las infraestructuras y no se puede estar predispuestos a la ocurrencia de problemas.
- Las fallas en el sistema eléctrico de la institución y de la localidad en la cual se encuentra el Data Center físico también puede desembocar en un evento activador. Fallas que desemboquen en el daño de los equipos físicos o sino ocurrir un corto y un consecuente incendio.
- Intento de accesos no autorizados a la red para provocar colapso en servicios o robar la información que se mantiene.
- Desastres físicos en cuanto al hardware de los equipos donde se alojan las aplicaciones y la información crítica.
- Los eventos activadores pueden ocurrir en cualquier momento y hay que tratar de prevenir el impacto con la implantación de acciones correctivas, en este caso pueden darse los anexos de políticas como documentación de

formalización de procesos para que así se pueda minimizar la probabilidad de activación de alguno de estos eventos.

Los eventos activadores pueden ocurrir en cualquier momento y hay que tratar de prevenir el impacto con la implantación de acciones correctivas, en este caso pueden darse los anexos de políticas como documentación de formalización de procesos para que así se pueda minimizar la probabilidad de activación de alguno de estos eventos.

Fase 4. Estrategias

4.1. Actividades Importantes

Para poder seguir con el trabajo y mantener el funcionamiento, es necesario la aplicación de estrategias que puedan asegurar el mismo y que sean aplicables inmediatamente. Para eso se han identificado algunas estrategias basadas en la relación de la norma ISO con la continuidad de entrega del servicio de información.

En acuerdo a la continuidad de la entrega del servicio lo definido han sido un conjunto de políticas establecidas a las cuales se harán referencia para poder llevar a cabo el cumplimiento del presente Plan de Contingencias. Se enlistan los mismos:

- PUCE_SA_DI_CON01_Bitácora_Revisión. Documento de Constancia, en el cuál se van a registrar las revisiones históricas de las revisiones dadas en base a los activos.
- PUCE_SA_DI_DOC01_Políticas_Seguridad. Conjunto de políticas de seguridad en los cuales se enfoca las actividades que deben llevarse a cabo para la seguridad de los recursos tecnológicos.
- PUCE_SA_DI_DOC02_Respaldo_Servidores. Documentos de constancia, que llevará a cabo el registro de los respaldos llevados de los servidores. Únicamente para constatar los respaldos de servidores.
- PUCE_SA_DI_DOC03_Metodología_Evaluación_Tratamiento_Riesgos. Metodología especificada por la norma ISO para poder completar adecuadamente los documentos anexos Plan de tratamiento de riesgos y Cuadro de evaluación de riesgos.
- PUCE_SA_DI_DOC04_Plan_Tratamiento_De_Riesgos. Documento de tratamiento de los riesgos, identificación de los responsables y asentamiento de indicaciones de observación.
- PUCE_SA_DI_DOC05_Cuadro_Evaluación_Riesgos. Documento de identificación de las amenazas a las cuales están expuestos los servidores, basado en la norma ISO.

Plan de Recuperación

Procedimiento para la recuperación de los desastres en información

En caso de ocurrir una pérdida de información causada por inconvenientes en los servidores, se deberá proceder con la recopilación de los respaldos llevados a cabo en el último período, es decir optado por el almacenamiento en nube; proceder a la descarga y reposición de la información.

Los respaldos deben llevarse además con almacenamiento físico también en caso de alguna ocurrencia que esté fuera del alcance de definición por algún factor desconocido fuera del entorno de trabajo del marco actual.

Mantener actualizados los respaldos una vez restablecido los mismos y además informar de los problemas a quien corresponda en cuestión de estructura organizacional de la institución (jefatura inmediata).

En caso de pérdida de información de aplicaciones SACI y SQUARENET, realizar la recuperación de la información de medios físicos o de respaldos en la nube y comunicarse inmediatamente con los proveedores del servicio para la ayuda oportuna en cuanto al soporte de las aplicaciones y la configuración de las mismas, ya que se considera que al ser proveedores externos; siempre se debe actuar en base a los estatutos establecidos en el contrato de prestación del servicio de software.

Notificación

Al presentarse algún problema en cuanto a lo relacionado, deberá hacerse la notificación a:

- Dirección Académica
- Dirección Financiera
- Usuarios

Persona de Acción de Notificación

- Jefe Departamental

Realizar siempre esto en un marco de acción de no más de 3 horas fuera de servicio. Considerar los aspectos dados en las estrategias para los riesgos cómo mantenerse preparados y realizarlo para cualquier problema.

Procedimiento para la recuperación de los desastres físicos

La ocurrencia de un desastre físico debe manejarse con mayor cautela, ya que puede afectar no sólo a los equipos; sino también al recurso humano.

El plan de acción debe ejecutarse de manera que, la revisión de los equipos y demás infraestructura que haya sido afectada revisada a profundidad, el

personal de mantenimiento debe encargarse de la valoración del entorno físico y de los equipos; que previamente determinados el orden de importancia debido a su criticidad deben irse levantando sus servicios y en caso de ser necesario; ser reemplazados los equipos más afectados por los equipos de respaldo que previamente han sido configurados con las especificaciones de ambiente productivo para cada aplicación. Se debe determinar si el personal del departamento está capacitado para actuar frente a la ocurrencia de un desastre físico y tratar de contenerlo para que no se expanda y erradicarlo.

Mantener la comunicación adecuada con los servicios que proveen el recurso de seguridad hacia el departamento y en general para el Data Center para que puedan dar la ayuda pronta y evitar o minimizar los daños establecidos en la infraestructura y los espacios adecuados.

Notificación

Al presentarse algún problema en cuanto a lo relacionado, deberá hacerse la notificación a:

- Dirección Académica
- Dirección Financiera
- Usuarios

Persona de Acción de Notificación

- Jefe Departamental

Los servicios físicos deben manejarse siempre de una manera más cautelosa y siempre mantener documentado todo lo realizado.

Procedimiento para la recuperación de los desastres de infraestructura

Cortar inmediatamente la comunicación de los servicios entregados por parte de los equipos involucrados con los usuarios, todas las comunicaciones serán interrumpidas hasta determinar cuál es el tamaño de la afectación. Proceder con la revisión de los servidores para asegurarse de cuál es el nivel de afectación a su información y sus servicios.

Corroborar el funcionamiento que sea adecuado como para poder continuar con la ejecución o entrega de servicio. Una vez actualizados los diferentes sistemas de información implementados tanto como sistema operativo, aplicativos y firewalls, proceder con la revisión de la información que pudo ser afectada y limpiarla. Realizado ya la verificación de la misma no demorar más de 2 horas en el restablecimiento de la comunicación.

Notificación

Al presentarse algún problema en cuanto a lo relacionado, deberá hacerse la notificación a:

- Dirección Académica
- Dirección Financiera
- Usuarios

Persona de Acción de Notificación

- Jefe Departamental

Procedimiento para la recuperación de los desastres eléctricos

Se deberá primero poner en funcionamiento los UPS que están disponibles para que se pueda continuar con la entrega del servicio.

Notificar a quien corresponda el funcionamiento de la planta generadora de la institución para que se ponga a funcionar y restablecer todo el fluido eléctrico hasta que el problema sea resuelto.

Comunicarse con los servicios de energía locales para conocer el estado del suministro eléctrico de la zona.

Continúa con el uso normal de la energía establecida.

Notificación

Al presentarse algún problema en cuanto a lo relacionado, deberá hacerse la notificación a:

- Mantenimiento de la Institución
- Dirección Académica
- Dirección Financiera
- Usuarios

Persona de Acción de Notificación

- Personal del departamento

Fase 5. Documentación

La documentación se llevó a cabo con el proceso del Plan y los adjuntos que corresponden.

Se hará uso de los anexos:

La descripción breve de cuál será la función dentro del Plan de Contingencias:

- **PUCE_SA_DI_DOC01_Políticas_Seguridad.** Su función es la de establecer políticas a seguir hacia aspectos que intervienen con la información.
- **PUCE_SA_DI_DOC02_Respaldo_Servidores.** Similar a una bitácora, pero es un documento de entrega y realización periódica.
- **PUCE_SA_DI_DOC03_Metodología_Evaluación_Tratamiento _**Riesgos. Documento de cómo se debe proceder para tratar un riesgo.
- **PUCE_SA_DI_DOC04_Plan_Tratamiento_De_Riesgos.** Clasificación de riesgos e identificación de responsables y recursos.
- **PUCE_SA_DI_DOC05_Cuadro_Evaluación_Riesgos.** Categorías de las amenazas.
- **PUCE_SA_DI_CON01_Bitácora_Revisión.** Documento de constancia de revisiones en general (adaptable a la necesidad).

Todo el proceso fue documentado y entregado al personal.

Fase 6. Validación

La norma ISO 27001, recalca que la validación deberá darse por parte de un auditor de la norma, para conocer la correcta aplicación de la misma. En este caso como no se dispone del mismo debido a que no es un proceso formal de implementación del Plan, sino únicamente todo el proceso se basa en la norma para dejar a consideración su aplicación; la validación se la dará por parte del Jefe Departamental.

CAPÍTULO IV.

RESULTADOS

4.1. Análisis de Resultados

Basados en el resultado encontrado por el análisis realizado de riesgos, se encuentra que se debe mejorar el nivel en cuanto a la seguridad de los servidores analizados y a la seguridad en cuanto a las aplicaciones que se alojan en ellas. Siguiendo las recomendaciones dadas en el anexo plan de contingencias se pueden minimizar los riesgos de ocurrencia de catastros y también en caso de ocurrirlos prevenir con seguridad sus respaldos y recuperación.

La norma ISO 27001 en su versión más actual busca la minimización de pérdidas y si se siguen las medidas estandarizadas en el plan, entonces se estará cumpliendo lo establecido por la norma.

El Plan de Contingencias que se ha dado cumple con las especificaciones entregadas por parte del personal del Departamento de Informática de la PUCESA, y en acuerdo con los mismos se ha comprobado el proceso que se realiza durante los pasos que intervienen en dicho Plan y se tiene su aprobación mediante la socialización de los resultados.

Al tomarse su validación de lo que se da en el Plan se logra determinar que:

1. Los procesos que se llevan a cabo dentro del Plan de Contingencias se enfatizan hacia la protección previa de los desastres.
2. Los procesos están establecidos para seguirlos; aunque actualmente no se tiene establecido el presupuesto asignado, por lo que la realidad se ajusta a la sugerencia de la aplicación de las medidas establecidas y lo que conlleva en la misma.
3. El documento es flexible y se puede adecuar a la realidad de la institución, conforme se van dando cambios a lo largo de la línea de tiempo.
4. Los anexos establecidos para la utilización de la verificación y guía de procesos, han sido tomados directamente de cómo los entrega la norma ISO 27001.
5. La planificación se ha realizado con datos reales entregados por parte del Departamento de Informática de la PUCESA, lo cual acerca los resultados a la realidad.

4.2. Validación de Resultados

La validación de los resultados está netamente ligado a la aplicación y correcta implementación de la norma ISO en base a documentos proporcionados por la misma.

CONCLUSIONES

- El desarrollo de un Plan de Contingencias aporta a la mejora de los procesos dentro del Departamento de Informática, ya que así es más fácil conocer la distribución de responsabilidades y personas a cargo sobre dichos procesos.
- La investigación y recopilación de información del personal interno es vital para poder conocer mejor los aspectos en los cuales se debía mejorar y formalizar procesos para cumplir los objetivos planteados y llevar a cabo lo establecido.
- La información debe estar protegida y respaldada ya que es un recurso extremadamente importante dentro de una organización, y es la que mantiene trabajando y hace que funcione la organización para entregar los servicios de forma adecuada.
- La comunicación interna entre los involucrados del negocio ayuda a que se coordine de mejor manera la pronta acción sobre problemas que se presenten.

RECOMENDACIONES

- Se recomienda mantener actualizado el portafolio de servicios entregados por la organización o departamento para llevar de forma correcta todos los procesos internos.
- Se deben mantener documentadas las revisiones realizadas en cierto período de tiempo, mediante un formato de constatación propia del Departamento que se ajuste a los parámetros que se tienen.
- Es muy importante la actualización de todos los servicios y de las tecnologías que se utilizan debido a que si no se cuenta con la información o los sistemas adecuados, la organización está mucho más propenso a que en caso de ocurrencia de un problema se vea afectada más de lo que pudiese evitarse.
- Mantener actualizada la documentación es parte fundamental para poder tener una acción inmediata y estar enfocados a los aspectos reales del departamento.

BIBLIOGRAFÍA

[1] C. R. Departamento de Planificación, «Comisión Nacional de Emergencias,» Enero 2010. [En línea]. Available: http://www.cne.go.cr/CEDO-CRID/pdf/spa/doc1071/doc1071-c.pdf. [Último acceso: 09 Diciembre 2014].

[2] P. Aguilera, Seguridad Informática, España: Editex, 2010.

[3] S.-J. d. I. Instituto Nacional de Estadística e Informática, Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información, Lima: Centro de Edición del INEI, 2001.

[4] ISO, «ISO 27000.ES,» ISO, 2013. [En línea]. Available: http://www.iso27000.es/iso27000.html. [Último acceso: 10 Diciembre 2014].

[5] Axelos, «Axelos,» [En línea]. Available: http://www.axelos.com/what-is-itil. [Último acceso: 10 Diciembre 2014].

[6] L. Mora y W. Salinas, Análisis de la Ley Sarbanes Oxley como herramienta para el mejoramiento de la calidad de la Información Financiera en Colombia, Bogotá, 2008.

[7] ISACA, «Isaca,» 2007. [En línea]. Available: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx. [Último acceso: 10 Diciembre 2014].

[8] ISO, «AENOR,» ISO ORG / AENOR, 1 Enero 2014. [En línea]. Available: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053761#.Vx7tEdLhDIU. [Último acceso: 25 Abril 2016].

[9] A. S. Informáticos, «Aner División de Sistemas,» [En línea]. Available: http://www.anerdata.com/que-es-un-servidor.html. [Último acceso: 04 Diciembre 2014].

[10] «Experto Java,» 2014-2015. [En línea]. Available: http://www.jtech.ua.es/j2ee/2003-2004/abierto-j2ee-2003-2004/sa/sesion1-apuntes.htm. [Último acceso: 04 Diciembre 2014].

[11] J. Sun Microsystems, «Oracle,» 24 Noviembre 2003. [En línea]. Available: http://www.oracle.com/webfolder/technetwork/jsc/xml/ns/j2ee/index.html. [Último acceso: 2014 Diciembre 2014].

[12] EcuRed, «EcuRed,» 2007. [En línea]. Available: http://www.ecured.cu/index.php/Servidor_de_Aplicaciones. [Último acceso: 04 Diciembre 2014].

[13] M. Cortés Cortés y M. Iglesias León, Generalidades sobre Metodología de la Investigación, Ciudad del Carmen, Campeche, México: Colección Material Didáctico, 2004.

[14] S. J. d. Informática, «Plan de Contingencia de los Sistemas de Información,» Centro de Edición del INEI, Lima, 2001.

[15] B. Berelson, The State of Communication Research, United States: The American Association for Public Opinion Research, 1959.

[16] INCIBE, «INCIBE, trabajando por la confianza digital,» INCIBE, 30 Abril 2014. [En línea]. Available: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/analisis_riesgos_pasos_sencillo. [Último acceso: 31 Mayo 2016].

[17] OSIATIS, «ITIL V3,» [En línea]. Available: http://itilv3.osiatis.es/itil.php. [Último acceso: 04 Diciembre 2014].

[18] M. Intituto Tecnológico de Sonora, «Plan de Contingencias,» [En línea]. Available: http://www.itson.mx/micrositios/laboratorios/Documents/plan_de_contingencia_csh.pdf. [Último acceso: 04 Diciembre 2014].

[19] OSIATIS, «OSIATIS,» 2011. [En línea]. Available: http://itil.osiatis.es/Curos_ITIL/Gestion_Servicios_TI/service_desk/introduccion_objetivos_service_desk/estructura_service_desk.php. [Último acceso: 10 Diciembre 2014].

ANEXO 1. ENCUESTA

ENCUESTA PARA EL PERSONAL DEL DEPARTAMENTO DE SISTEMAS DE LA PUCESA

1. **¿En qué nivel de criticidad sitúa la información manejada por el servidor de aplicaciones?**

   Muy Alta ( ) Alta ( ) Media ( ) Baja ( )

2. **¿En caso de ocurrir algún siniestro, usted está preparado para enfrentarlo?**

   Si ( ) No ( )

3. **¿Cuál considera que es la priorización de las aplicaciones? Enliste del 1 al 4 (1 = mayor prioridad, 4 = menor prioridad)**

Académico	( )	EVAE	( )
Sistema Contable	( )	Sistema Administrativo	( )

4. **¿La PUCE Sede Ambato está actualmente implementando algún estándar de seguridad o calidad actualmente?**

   Si ( ) No ( )

5. **¿Considera que la información manejada por el servidor de aplicaciones está en riesgo?**

   Alto ( ) Medio ( ) Bajo ( ) No existe riesgo ( )

6. **¿La ocurrencia de fenómenos que amenacen en general la información que frecuencia tienen?**

   Muy frecuente ( ) Frecuente ( ) Ocasional ( ) Nula ( )