UNAP

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

EXAMEN DE SUFICIENCIA PROFESIONAL

"PLAN DE CONTINGENCIA DE LOS ACTIVOS INFORMÁTICOS DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA"

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR:

KEYNES PAUL REYNA REYNA

IQUITOS, PERÚ

2014

UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

ACTA DE EXAMEN ORAL DE SUFICIENCIA PROFESIONAL

Siendo las **19:00** horas del día **15** de **Octubre del 2014**, en las instalaciones del Auditorio de la Facultad de Ingeniería Química de la Universidad Nacional de la Amazonia Peruana, sito en la calle Freyre N° 616 - Iquitos, el Jurado Examinador, compuesto por los siguientes miembros:

Presidente : Ing. Saul Flores Nunta
Primer Miembro : Lic. Adm. Ángel Ildefonso Catshunga Torres
Segundo Miembro : Ing. Elvis del Águila López

Se procedió al acto académico del examen oral de suficiencia profesional del bachiller: **Keynes Paul Reyna Reyna**, quien sustento el tema; **"PLAN DE CONTINGENCIA DE LOS ACTIVOS INFORMATICOS DE LA FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA".**

Posteriormente al Acto de Sustentación del Informe Final del bachiller, se procedió al cálculo de la Calificación y Condición Final, obteniéndose el siguiente resultado:

	Calificaciones	
	En número	**En letras**
Promedio de la Calificación Final de las Asignaturas.	15.0	QUINCE
Calificación de la Evaluación del Desarrollo del Informe.	13.1	TRECE Y 1/10
Calificación de la Evaluación de Técnicas y Procedimientos	12.4	DOCE Y 4/10
Calificación de la Sustentación del Informe Final	12.8	DOCE Y 8/10
Calificación Final	**13.8**	TRECE Y 8/10

Se desprende que la Condición Final del Bachiller es (marcar el que corresponde):

( ) Aprobado con excelencia (18 a 20 puntos).
( ) Aprobado por unanimidad (15 a 17.9 puntos).
(X) Aprobado por mayoría (12 a 14.9 puntos).
( ) Desaprobado (Menos de 12 puntos).

Siendo las **20:00** horas del mismo día, se da por concluido el acto, firmando en conformidad los miembros del Jurado Examinador.

Ing. Saul Flores Nunta
Presidente

Lic. Adm. Ángel Ildefonso Catshunga Torres
Miembro

Ing. Elvis del Águila López
Miembro

DEDICATORIA

Dedicado a mis seres queridos: a mi querida madre, a mí mujer, a mi hijita y a la que está por nacer.

También a mí hermano y mis sobrinos

A la memoria de mi hermano Keyser (Q.E.P.D.)

AGRADECIMIENTOS

Gracias a Dios por mí vida, por haberme ayudado durante estos años de estudios, el sacrifico es grande, pero tú siempre me diste la fuerza necesaria para continuar y lograrlo. Para mi hermano Keyser quien desde el cielo guía mi camino y siempre me acompaña.

A mi madre Ysabel, Gracias por ayudarme, por animarme y empujarme a seguir adelante, sin ti nada hubiera sido posible.

A Diana Gracias por ser la persona que me ama, acompaña y siempre tiene una palabra de aliento cuando lo necesito. A mi hijita Abigail sin su ternura y su inocencia no sería nada posible, la lucha del día a día. A la luz que Dios puso en el vientre de mi mujer para darme la alegría de mi vida, ser padre por segunda vez, a ti que te espero con ansias mi pequeña Alexandra.

A Keir mi hermano por cada consejo puntual y oportuno que has sabido darme, por tu apoyo incondicional, por ser mi amigo. A mis sobrinos, Christian y Jhossef que llenan de alegría cada día de mi vida, de quienes espero se sientan muy orgullosos de mí, así como yo de ellos.

A los docentes, personal administrativo y compañeros de la universidad, a quienes les debo gran parte de mis conocimientos, gracias por prepararnos para un futuro competitivo no solo como los mejores profesionales sino también como mejores personas.

A todos ustedes, ¡Gracias!

CONTENIDO GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

PLAN DE CONTINGENCIA DE LOS ACTIVOS INFORMÁTICOS DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

POR: BACH. KEYNES PAUL REYNA REYNA

Con el objetivo de que la Facultad de Ingeniería cuente con un plan de contingencia de los activos informáticos, se realizó el análisis, detección, evaluación y la priorización de amenazas potenciales de las que puede ser víctima la institución, así mismo se priorizó las tareas más relevantes e importantes para la facultad de Ingeniería. Para lograr este propósito se utilizó MAGERIT debido a que es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, el cual está directamente relacionado con la generalización del uso de los medios electrónicos, informáticos y telemáticos. El producto final contribuye para que la institución conozca sus vulnerabilidades y de esta manera lograr precautelar la integridad de la información y componentes físicos y lógicos con los que se cuenta.

PALABRAS CLAVES

Plan de contingencia, amenazas, MAGERIT, vulnerabilidades.

CAPITULO I

ANTECEDENTES

1.1. INTRODUCCIÓN

La seguridad informática ha venido evolucionando a lo largo del tiempo. Las necesidades de protección, de control de acceso, de confidencialidad y disponibilidad de la información han originado la manera de comprender las posibilidades de la seguridad informática en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, desde sus inicios ha buscado la manera de aumentar con certeza el seguimiento de las actividades de los trabajadores, con el fin de mantener un adecuado control (comprendido como capacidad de regulación) de la evolución del sistema de información y un registro óptimo de los empleados en el uso de los diferentes sistemas informáticos o electrónicos.

Esta evolución ha estado confinada entre una rápida transformación tecnológica y una mediana apropiación de la tecnología. Si bien las motivaciones en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, fundadas en mayor capacidad de interacción y eficiencia, son un factor decisivo para promover el desarrollo de sistemas de información de amplia cobertura. La capacidad de absorción (capacidad de comprender y usar las TI) de esta nueva tecnología y sus posibilidades, podría no ser tan rápida como se espera, generando posibles diferencias, que puedan comprometer la información que en ellos se maneja.

En este sentido, la seguridad informática, por una tradición académica y científica, donde la inversión en protección y control de información son los factores comunes, se ha confinado al contexto de dispositivos, iniciativas, estrategias técnicas y experimentales para elevar cada vez más los niveles de control sobre los datos disponibles. Esta realidad, se ha afirmado a lo largo del tiempo en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, generando un paradigma eminentemente técnico alrededor del tema de seguridad informática, generalmente de dominio de los profesionales de la ingeniería, donde el espacio para individuos de otras disciplinas generalmente no es muy amplio.

En razón a lo anterior y explorando en profundidad el concepto de seguridad informática, este documento busca repensar dicho concepto integrando la realidad organizacional y sus procesos, la tecnología informática que lo soporta y el contexto individual que hace realidad la dinámica de la seguridad informática en la Facultad de Ingeniería de Sistemas e Informática de la

Universidad Nacional de la Amazonía Peruana, como una iniciativa para establecer una integración sistemática del concepto para hacer de la seguridad informática un tema multidisciplinario inmerso en la evolución.

Este esquema de trabajo debe ser repetitivo, pues los sistemas rara vez son inmutables; más aún se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

1.2. **FORMULACIÓN DEL PROBLEMA**

¿De qué manera podría contribuir con la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana ante vulnerabilidades informáticas que puedan afectar el normal funcionamiento del mismo?

1.2.1. DESCRIPCIÓN DEL PROBLEMA

La RED LAN:

Los cables de red en algunos casos están expuestos a soportar daños, puesto que no están aseguradas de acuerdo a un estándar de calidad.

Es decir, el estado en la que se encuentra la red que se utiliza en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, no es la adecuada, este sistema está propenso a sufrir daños y así retrasar las labores de la institución.

HARDWARE:

Muchos de ellos están mal ubicados, expuestos al público, generando el problema en cuanto a la seguridad de las PC.

Corren el riesgo de ser sustraídos, este daño perjudica la economía de la institución.

También se pudo apreciar que existen dispositivos en mal estado y en algunos casos obsoletos.

SOFTWARE:

Se pudo apreciar que los informes finales y las informaciones más relevantes se guardan en CD. Estos dispositivos al pasar el tiempo se deterioran.

1.3. OBJETIVOS

1.3.1. GENERAL.

Elaborar un plan de contingencia para proteger los activos informáticos de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

1.3.2. ESPECÍFICOS.

- Determinar los activos informáticos relevantes para la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, su interrelación y su valor actual.

- Detectar los riesgos y amenazas tanto físicas como lógicas que puedan causar fallos en el normal funcionamiento de los sistemas de información.

- Definir las actividades de ejecución de las tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicio eléctrico, fenómenos naturales o humanos.

- Establecer un plan de recuperación, formación de componentes e instruir al personal para recuperar la operatividad del sistema en el menor tiempo posible.

1.4. JUSTIFICACIÓN

La elaboración del plan de contingencia para proteger los activos informáticos, ayudará sustancialmente a la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, dando una solución alternativa y confiable, ante la eventualidad de todo aquello que pueda paralizar el normal funcionamiento de la misma.

CAPITULO II

MARCO TEÓRICO

2.1. BASES TEORICO

2.1.1. PLAN DE CONTINGENCIA:

Se puede definir a un plan de contingencia como una estrategia planificada con una serie de procedimientos que faciliten tener una solución alternativa que permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total. El Plan de Contingencias de los Activos Informáticos es una herramienta que le ayudará a que los procesos críticos de la institución continúen funcionando a pesar de una posible falla en los sistemas de información.

Todas las instituciones están expuestas a diversos tipos de riesgos en sus sistemas de información, y la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana no está excepto. Estos riesgos pueden ser tanto físicos (fuego, inundación, sabotaje, entre otros) como lógicos (virus, problemas de seguridad en la información, calidad de software, almacenamiento de datos inapropiado, entre otros), que pueden paralizar parcial o totalmente la normal actividad de los mismos, con el consiguiente perjuicio para la institución.

El plan de Contingencias se basa en la minimización del impacto que pueda tener un siniestro en los activos informáticos de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

Las contingencias afectan a las personas y los medios con los que estas desarrollan su actividad, su trabajo.

No sólo se deben identificar los riesgos, también evaluarlos para posteriormente decidir sobre las medidas que puedan mitigarlos. Para ello, se

identificó los activos de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, así como las debilidades que puedan padecer, estimando probabilidades de ocurrencia y asignándoles una importancia para la misión de la institución, entre los principales activos tenemos.

Organización	= Personas
Objetos, funciones	= Misión
Información	= Datos
Procesos	= Tecnología

En los negocios la tecnología de la información del entorno actual (TI), incluyendo datos, son algunos de los más importantes activos de propiedad de las instituciones. Las inundaciones, hackers, virus informáticos, sabotaje son desastres que amenazan a estos activos.

Las instituciones tienen que estar preparadas y ser capaces para responder a estos ataques. Para asegurar su supervivencia, deben ser capaces de forma rápida recuperar sus datos, continuar sus operaciones y proteger su reputación.

2.1.2. METODOLOGÍA DE ANALISIS Y GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

El Consejo Superior de Administración Electrónica ha elaborado y promueve la metodología MAGERIT, como respuesta a la percepción de la Administración.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios. Conocer los riesgos al que están sometidos los sistemas de información con los que se trabaja es imprescindible

para poder gestionarlos y por este motivo existen multitud de guías informales para la realización del análisis y gestión de riesgos, aproximaciones metódicas y herramientas de soporte. Todas estas guías (informales, metódicas) buscan poder evaluar cuanto de seguros (o inseguros) están los sistemas de información, para evitar llevarse a engaño.

2.1.2.1. OBJETIVOS DE METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

- Concienciar a los responsables de los sistemas de información (dueños del proceso) de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos:

Modelo de valor

Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.

Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo

Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

2.1.2.2. IDENTIFICACIÓN DE RIESGOS

La identificación de riesgo se realiza de acuerdo al (Cuadro 1.) valorando así de esta manera los impactos y riesgos de las diferentes amenazas que puedan materializarse sobre los activos de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonia Peruana, es el siguiente:

Tabla 01. Valoración de impactos y riesgos.

Descripción sucinta de lo que puede pasar											
TIPOS DE ACTIVOS: • Que se puede ver afectado por este tipo de amenazas.					**DIMENSIONES:** 1. De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante.						
DESCRIPCIÓN: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas											
ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACION**				**RIESGO**		**FRECUENCIA**			
		1 %	**10 %**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA		IMPACTO	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MB	MA
	M	MB	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

MOTIVO:
Razón detallada por la cual se considera el impacto y el riesgo de la amenaza en el gobierno autónomo descentralizado municipal del cantón Junín.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

2.1.2.3. VALORACIÓN DE LAS AMENAZAS

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- **Degradación:** Cuán perjudicado resultaría el activo
- **Frecuencia:** Cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresión es como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias, pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años

2.1.2.4. DETERMINACIÓN DEL IMPACTO

Se denomina impacto a DETERMINACIÓN DEL RIESGO la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del
Sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Para la valoración del impacto, se consideró la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MB:** muy bajo
- **B:** bajo
- **M:** medio
- **A:** alto
- **MA:** muy alto

2.1.2.5. DETERMINACIÓN DEL RIESGO

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.
La escala para calificar la frecuencia del riesgo según la metodología MAGERIT mediante alguna escala sencilla: es la siguiente:

- **MF:** muy frecuente (a diario)
- **F:** frecuente (mensual)
- **FN:** frecuencia normal (anual)
- **PF:** poco frecuente (cada varios años)

2.1.2.6. SALVAGUARDAS

Las salvaguardas son procedimientos o mecanismos tecnológicos con los cuales se reduce el riesgo en una organización. Las salvaguardas entran en el cálculo del riego de dos formas:

- **Reduciendo la frecuencia de las amenazas**

Estas son denominadas salvaguardas preventivas las cuales se aplican antes de que se materialice una amenaza con lo cual se puede cubrir las mismas en su totalidad.

- **Limitando el daño causado**

En este tipo de salvaguardas, en todos los escenarios se materializan las amenazas sobre uno o varios activos, el objetivo de este tipo de salvaguardas es identificar las amenazas y minimizar su impacto para de esa forma limitar sus consecuencias.

Las salvaguardas se miden por su eficacia frente a la amenaza a la cual pretende minimizar su riesgo, la salvaguarda ideal es 100% eficaz lo que implicará que:

- Es teóricamente idónea.
- Está perfectamente desplegada, configurada y mantenida.
- Se emplea siempre.
- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posible fallo.

CAPÍTULO III.

DESARROLLO METODOLÓGICO

El trabajo de tesis se realizó en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, el cual tuvo una duración desde 07/04/2014 hasta 15/06/2014.

3.1. MÉTODOS CIENTÍFICOS

Para el análisis y gestión de riesgos de los activos informáticos se utilizó MAGERIT, ya que el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo los pasos siguientes:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean “potenciales”: caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

En la primera etapa se determinaron los activos relevantes de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, los resultados se obtuvieron realizando un censo de ámbito informático, incluyendo en este: Hardware, software, talento humano y servicios.

3.1.1. ACTIVOS INFORMÁTICOS RELEVANTES DE LA FACULTAD DE INGENIERIA DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

3.1.1.1. HARDWARE

El censo se realizó minuciosamente en la parte del hardware tomando en cuenta todos los computadores, impresoras, de cada uno de los departamentos dependientes de esta institución, así como también los dispositivos de la red, y servicios de ámbito informático que la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, detallándolos de la siguiente manera:

COMPUTADORAS

Mediante este censo, una vez analizando los datos, se determinó que la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, en el área administrativa cuenta con un total de Veinte y nueve computadoras, los cuales se describen en la siguiente tabla, la información que se muestra en este detalle, los computadores e información correspondiente a compra y precios, determinando el valor actual de los bienes con su respectiva depreciación según la ley y reglamento de régimen tributario vigente.

Tabla 02. Valor actual de las computadoras de la Facultad de Ingeniería de Sistemas e Informática de la UNAP. Según su depreciación.

DETALLE	CANT.	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	TIEMPO DE USO	DEPREC. ANUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN
ADVANCE	29	1.800	52,200	2010	4 AÑOS	10%	31,320	1.080

Cálculo de Depreciación Fiscal

- Valor de adquisición: S/. 1,800.00
- Año de adquisición: 2010
- Porcentaje de depreciación: 10% anual
- Valor depreciado: (S/. 1,800.00 – S/.720) = S/. 1,080

Una vez realizada la respectiva depreciación de los computadores según los precios adquisición se determinó que la instrucción actualmente tiene en computadores S/. 31,320.00 Nuevos Soles.

SERVIDORES

La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, en el área informática cuenta con un computador tipo Servidor en óptimo funcionamiento.

Tabla 03. Valor actual del servidor de la Facultad de Ingeniería de Sistemas e Informática de la UNAP. Según su depreciación.

DETALLE	CANT.	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	TIEMPO DE USO	DEPREC. ANUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN
ADVANCE	01	1.800	1.800	2010	4 AÑOS	10%	1.080	1.080

IMPRESORAS

La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, en el área administrativa cuenta con un total de dos impresoras en funcionamiento, así mismo las características como precio y año de compra fueron facilitadas por parte de la institución.

Tabla 04. Valor actual de las impresoras de la Facultad de Ingeniería de Sistemas e Informática de la UNAP. Según su depreciación.

DETALLE	CANT.	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	TIEMPO DE USO	DEPREC. ANUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN
EPSON	02	550.00	1,100.00	2013	01 AÑO	6%	1,034.00	517.00

EQUIPOS DE RED

La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, cuenta con una RED de datos, que comprende el uso de equipos de RED que se detallan a continuación:

3.1.1.2. SOFTWARE

Se realizó un levantamiento de la información en la parte del Software tomando en cuenta todos los sistemas informáticos utilizados en La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, detallándolos de la siguiente manera:

Tabla 05. Costo Anual de licencias de Software utilizado en La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana

SOFTWARE			
DETALLE	**CANTIDA**	**LICENCIA**	**PRECIO**
ESET SMART SECURITY	29	PAGO ANUAL	1,682.00
AUTODESK AUTOCAD	05	SIN LICENCIA	-
MICROSOFT OFFICE	29	SIN LICENCIA	-
		TOTAL	1,682.00

Una vez realizado el respectivo censo de los sistemas informáticos, se determinó que actualmente La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, tiene contratados licencias anuales por las cuales cancela un monto total de S/. 1,682.00 Nuevos Soles.

3.1.1.3. TALENTO HUMANO

Después de haber realizado el levantamiento de la información tanto con el hardware como con el software, se procedió a realizar un censo para determinar el número de personas que trabajan en el área Administrativa y por ende están en constante contacto y utilización de los equipos y servicios informáticos con los que cuenta La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, a continuación, se describe lo indicado:

Tabla 06. Servidores públicos administrativos de La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

TALENTO HUMANO – AREAS ADMINISTRATIVAS		
ITEM	**DESCRIPCIÓN**	**NUMERO**
01	CONSEJO DE LA FACULTAD	3
02	DECANO	1
03	DEPARTAMENTO ACADÉMICO DE CIENCIA S	5
04	OFICINA DE CONSEJERIA Y	2

	BIENESTAR UNIVERSITARIO	
05	DIRECCIÓN DE ESCUELA DE FORMACIÓN PROFESIONAL	2
06	DIRECCIÓN DE INSTITUTO DE INVESTIGACIÓN	1
07	DIRECCIÓN DE EXTENSIÓN Y PROTECCIÓN	1
08	DIRECCIÓN DE SECCIÓN DE POST – GRADO	2
09	OFICINA DE ASUNTO ACADÉMICOS	2
10	CENTRO DE EXPERIMENTACIÓN Y ENSEÑANZA	1
11	CENTRO DE PRODUCCIÓN DE BIENES Y PRESTACIÓN DE SERVICIOS	2
TOTAL		22

El censo realizado determinó que La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, cuenta con un número total de veinte y dos servidores públicos en el área administrativa.

ESTRUCTURA QUE ACOGE LOS EQUIPOS

Una vez determinado los activos informáticos relevantes del La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, los mismos que fueron utilizados para determinar y cuantificar el monto total con el que cuenta la Institución, se procedió a realizar al levantamiento y diseño de la estructura informática de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, está conformado por 9 oficinas, con una serie de computadoras interconectadas a través de equipos de red y todos estos poseen el servicio de internet.

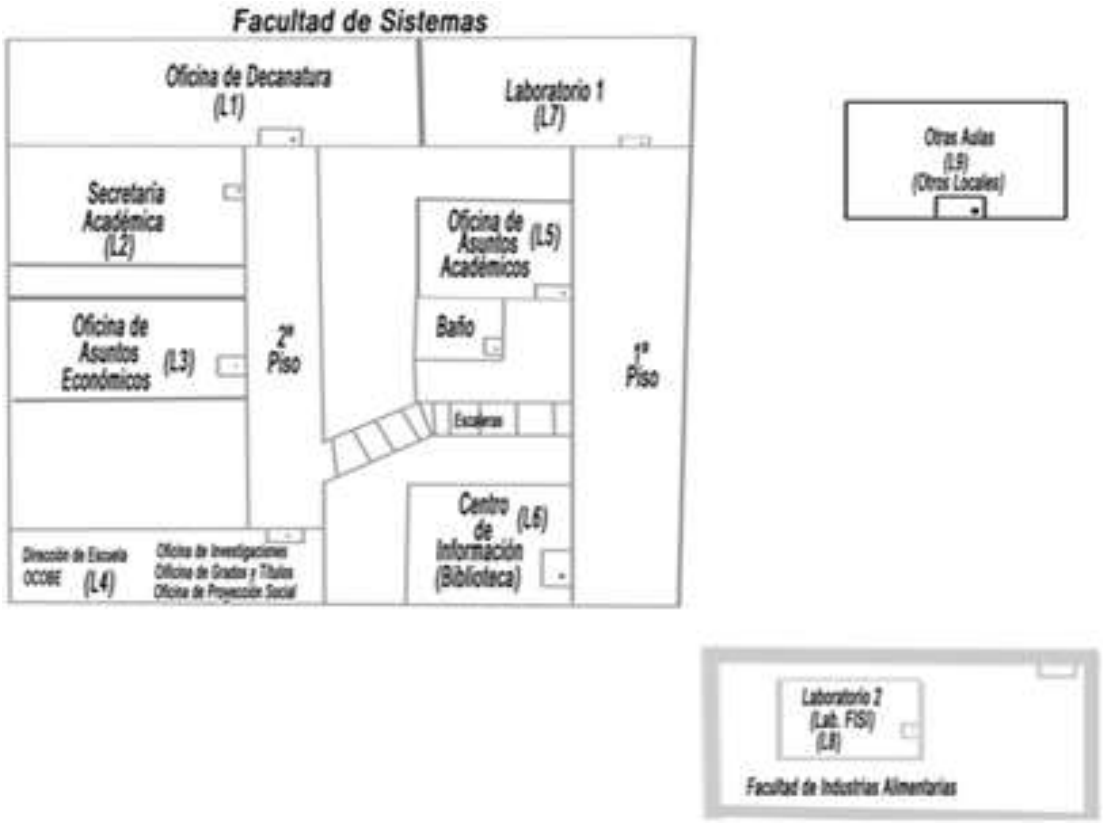


FIGURA 01. AMBIENTES DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

3.1.2. ANÁLISIS DE LA FACULTAD DE INGENIERIA Y SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA

El análisis que realicé a la Facultad de Ingeniería de Sistemas de la Universidad Nacional de la Amazonía Peruana, es el siguiente:

Fortalezas:

- ✓ Nivel profesional con el que cuenta la Facultad de Ingeniería de Sistemas de la Universidad Nacional de la Amazonía Peruana.
- ✓ Plataforma tecnológica disponible, hardware, software y Comunicaciones.
- ✓ Administración comprometida con el uso de tecnología de punta.
- ✓ Trabajo en equipo, solidaridad y colaboración.
- ✓ Trabajo comprometido con ética y profesionalismo.
- ✓ Confianza y actitud positiva.

Debilidades

- ✓ Desconocimiento de la metodología empleada.
- ✓ Falta de Capacitación.
- ✓ Ausencia de Talento Humano formado en esta rama. Pocos proyectos elaborados.
- ✓ Bajo presupuesto para la adquisición de Hardware, Software, Servicios, Capacitación.
- ✓ Falta del Plan de Contingencia Informático.

Amenazas

- ✓ Seguridad de la información ataques de virus, malware, hackers que puedan producirse.
- ✓ Desastres Naturales que puedan provocar afectación a la infraestructura tecnológica.
- ✓ Seguridad Física.
- ✓ Riesgos asociados con la sostenibilidad actual de la plataforma tecnológica.
- ✓ Perdida de información.

3.1.3. GRUPO DE TRABAJO AL INTERIOR DE LA FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA - UNAP.

Conformación del Grupo de Trabajo: El Grupo de Trabajo tendrá a cargo responder por la correcta implementación y desarrollo del plan de contingencia y estará conformado por el personal de la Facultad de Ingeniería de Sistemas e Informática que tiene a cargo el mantenimiento y administración de la red.

Integrantes: Personal de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

01 Jefe de Tecnologías de Información

- ➢ Perfil:

Profesor Universitario, titulado en la carrera de ingeniería de Sistemas o Informática, Electrónica o Comunicaciones.

- ➢ Funciones básicas:

Gestionar nuevas tecnologías para mejorar el funcionamiento de los equipos de la Facultad de Ingeniería de Sistemas de Informático - UNAP.

01 Supervisor de Seguridad

- ➢ Perfil:

Egresado o Bachiller de la carrera de Ingeniería de Sistemas e Informática.

- Funciones básicas:

Estudiar y evaluar las amenazas y riesgos con que cuenta la Universidad Nacional de la Amazonía peruana.
Establecer prioridades ante probabilidades de ocurrencia y conocer los procedimientos para cada eventualidad.

01 Soporte

- Perfil:

Profesional egresado de instituto de educación superior de prestigio especializado en mantenimiento de hardware y software.

- Funciones básicas:

Mantenimientos preventivos de equipos informáticos.
Mantenimientos correctivos de equipos informáticos.

Organigrama:

FIGURA 02. ORGANIGRAMA PROPUESTO PARA PERSONAL DE TECNOLOGÍAS DE LA INFORMACIÓN.

Conformación del Comité de Informática:

- Decano de la Facultad
- Director de Escuela
- Soporte

Funciones del Comité de Informática:

- Evaluar el plan de contingencia de activos informáticos, para su aprobación y ejecución.
- Aprobar la actualización periódica del plan de contingencia informático.
- Emitir políticas sobre el uso racional de bienes informáticos e insumos, acuerdo a las necesidades y recursos de la Universidad Nacional de Amazonía Peruana.
- Promover, difundir y supervisar el uso de estándares señalado por la Facultad de Ingeniería de Sistemas e Informática, en materia de equipos y telecomunicaciones.
- Promover la integración informática y los intercambios tecnológicos a nivel interinstitucional.
- Coordinar los cursos que tiendan a mantener actualizado el talento humano vinculado directamente a la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía peruana y a los usuarios de los mismos.

3.1.4. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a los activos y causar un daño.

Se tomó en cuenta tres clasificaciones principales que puedan haber tales como: accidentes naturales (inundaciones), desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos, y también existen amenazas causadas por las personas, sean estos errores, o ataques intencionados. Deterioro

La tabla que se utilizó para la valoración de los impactos y riesgos de las diferentes amenazas que puedan materializarse sobre los activos informáticos de la Facultad de Ingeniería de Sistemas e Informática - UNAP, como se muestra en el Cuadro 1.

3.1.4.1. (N) DESASTRES NATURALES

Nuestra Región tiene un clima variante, cambios drásticos. Debido a ello puede producirse los desastres naturales, en el siguiente apartado se procedió a determinar las amenazas que se pudieran presentar:

Tabla 7. Amenaza – Fuego

[N.1] FUEGO

TIPOS DE ACTIVOS:

- [HW] equipos informáticos (hardware)
- [COM] redes de comunicaciones
- [SI] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones

DIMENSIONES:

1. [D] disponibilidad
2. [T_S] trazabilidad de los servicios
3. [T_D] trazabilidad de los datos

DESCRIPCIÓN:

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

ESTIMACIÓN DEL IMPACTO

IMPACTO		DEGRADACION		
		B	**M**	**A**
VALOR	**MA**	M	A	**MA**
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO

RIESGO		FRECUENCIA			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	**MB**	B	M	A
	MB	MB	MB	B	M

MOTIVO: incendio una amenaza activa

Según los datos registrados por el cuerpo de bomberos de Iquitos, los daños por incendio no son frecuentes; además hay que tener en cuenta que a un costado del edificio de la Facultad existe una vivienda, que hasta el momento no registra accidente alguno de incendio y el hecho que se materialice esta amenaza afectaría en todos los ámbitos a la institución.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 8. Amenaza – Daños por Agua

[N.2] DAÑOS POR AGUA

TIPOS DE ACTIVOS:	**DIMENSIONES:**
• [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

DESCRIPCIÓN:

Inundaciones: posibilidad de que el agua (por las lluvias que son frecuentes) acabe con recursos del sistema.

ESTIMACIÓN DEL IMPACTO

IMPACTO		**DEGRADACION**		
		1 %	**10 %**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	**B**
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO

RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	**MB**	MA
	M	B	M	A	MA
	B	**MB**	B	M	A
	MB	MB	MB	B	M

MOTIVO:

El edificio de edificio de la Facultad de Ingeniería de Sistemas e Informática está ubicado en un sector céntrico de Iquitos, es por esta razón que se considera el impacto y un riesgo en esta amenaza, cabe indicar que no se registran datos de inundaciones en este sector.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 9. Amenaza – Desastres Naturales

[N.3] DESASTRES NATURALES

TIPOS DE ACTIVOS:	**DIMENSIONES:**
• [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

DESCRIPCIÓN:

Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica.

Se excluyen desastres específicos de inundaciones, por causa de los ríos.

ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	**MB**	MB	MB		MB	**MB**	MB	B	M

MOTIVO:

No existe dato alguno que registre cualquier incidencia de estos fenómenos en la ciudad de Iquitos, razón por la cual se determina el impacto y el riesgo de la amenaza en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.4.2. (I) DE ORIGEN INDUSTRIAL

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

Tabla 10 AMENAZA – Origen Industrial – Desastres Industriales

[I.3]DESASTRES INDUSTRIALES	
TIPOS DE ACTIVOS: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**DIMENSIONES:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
DESCRIPCIÓN: Sobre carga eléctrica, fluctuaciones eléctricas.	
ESTIMACIÓN DEL IMPACTO	**ESTIMACIÓN DEL RIESGO**

IMPACTO		DEGRADACION				RIESGO		FRECUENCIA			
		1 %	10 %	100%				PF	FN	F	MF
VALOR	**MA**	M	A	MA		IMPACTO	**MA**	A	MA	MA	MA
	A	B	**M**	A			**A**	M	A	MB	MA
	M	MB	B	M			**M**	B	**M**	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

MOTIVO:

- Calentamiento de red eléctrica.
- Constantes cortes de fluido eléctrico en el área donde se encuentra ubicada la institución con duraciones mayores de 30 minutos.
- Continuas variaciones del fluido del voltaje de la energía eléctrica
- Cables de tendido eléctrico urbano cerca del edificio

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 11 AMENAZA – Origen Industrial – Contaminación Mecánica

[I.4] CONTAMINACIÓN MECÁNICA	
TIPOS DE ACTIVOS: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**DIMENSIONES:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
DESCRIPCIÓN: Vibraciones, polvo, suciedad, entre otros.	
ESTIMACIÓN DEL IMPACTO	**ESTIMACIÓN DEL RIESGO**
DEGRADACION	**FRECUENCIA**

IMPACTO		1 %	10 %	100%
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	**B**	M
	B	MB	MB	B
	MB	MB	MB	MB

RIESGO		PF	FN	F	MF
IMPACTO	**MA**	A	MA	MA	**MA**
	A	M	A	MB	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

MOTIVO:

El edificio la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, se encuentra ubicado en la arteria principal de la ciudad donde el tráfico es muy constante. y además las oficinas no cuentan con un sistema de aislamiento de influencias externas (polvo), provocan que la presencia del polvo y la suciedad sea constante, es por esta razón que los equipos informáticos sufren un gran deterioro producto de la gran cantidad de esta amenaza.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 12 AMENAZA – Origen Industrial – Corte Del Suministro Eléctrico

[I.7] CORTE DEL SUMINISTRO ELÉCTRICO	
TIPOS DE ACTIVOS: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**DIMENSIONES:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
DESCRIPCIÓN: Cese de la alimentación de potencia.	
ESTIMACIÓN DEL IMPACTO	**ESTIMACIÓN DEL RIESGO**

IMPACTO		DEGRADACION				RIESGO		FRECUENCIA			
		1 %	10 %	100%				PF	FN	F	MF
VALOR	MA	M	A	MA		IMPACTO	MA	A	MA	MA	MA
	A	B	**M**	A			A	M	A	**MA**	MA
	M	MB	B	M			M	B	M	A	MA
	B	MB	MB	B			B	MB	B	M	A
	MB	MB	MB	MB			MB	MB	MB	B	M

MOTIVO:

- Calentamiento de red eléctrica.
- Constantes cortes de fluido eléctrico en el área donde se encuentra ubicada la institución con duraciones mayores de 30 minutos.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 13 AMENAZA – Origen Industrial – Interrupción De Otros Servicios y Suministros Esenciales

[I.10] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	
TIPOS DE ACTIVOS: • [AUX] equipamiento auxiliar	**DIMENSIONES:** 1. [D] disponibilidad
DESCRIPCIÓN: Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, entre otros.	

ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO				
IMPACTO	DEGRADACION				RIESGO	FRECUENCIA			
	1 %	10 %	100%			PF	FN	F	MF

VALOR	**MA**	M	A	MA		IMPACTO	**MA**	A	MA	MA	MA
	A	B	**M**	A			**A**	M	A	MB	MA
	M	MB	B	M			**M**	B	**M**	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

MOTIVO:

Como Institución pública, los trámites para la adquisición de estos insumos y/o repuestos, son un poco tediosos, ya que es todo un proceso que debe de seguirse, y en varias ocasiones se han quedado represados los tramites por fallas administrativas, por lo que esta amenaza ha provocado algunos inconvenientes para el soporte técnico de computadores debido a la escases de los mismos y por ende el retraso en las operaciones

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 14 AMENAZA – Degradación De Los Soportes De Almacenamiento De La Información

[I.11] DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN

TIPOS DE ACTIVOS:	**DIMENSIONES:**
• [SI] soportes de información	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

DESCRIPCIÓN:

Como consecuencia del paso del tiempo.

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACION**				**RIESGO**		**FRECUENCIA**			
		1 %	**10 %**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	**A**	MA		IMPACTO	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MB	MA
	M	MB	B	M			**M**	B	**M**	A	MA
	B	MB	MB	B			**B**	MB	B	M	A
	MB	MB	MB	MB			**MB**	MB	MB	B	M

MOTIVO:
la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, cuenta con tan solo dos dispositivos de almacenamiento masivo, los cuales son utilizados para el respaldo de la información, y por ende la estimación del impacto es muy alto obviamente el daño de estos dispositivos no ocurre con mucha frecuencia.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.4.3. (E) ERRORES Y FALLOS NO INTENCIONADOS

Fallos no intencionales causados por las personas.

La única numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Tabla 15 AMENAZA-Errores y Fallos No Intencionados – Errores de los Usuarios

[E.1] ERRORES DE LOS USUARIOS	
TIPOS DE ACTIVOS: • [S] Servicios • [D] Datos/Información • [SW] soportes de información	**DIMENSIONES:** 1. [I] Integridad 2. [D] Disponibilidad
DESCRIPCIÓN: Equivocaciones de las personas cuando usan los servicios, datos, entre otros.	

ESTIMACIÓN DEL IMPACTO						**ESTIMACIÓN DEL RIESGO**					
IMPACTO		**DEGRADACION**				**RIESGO**		**FRECUENCIA**			
		1 %	**10 %**	**100%**				**PF**	**FN**	**F**	**MF**
VALOR	**MA**	M	A	MA		IMPACTO	**MA**	A	MA	MA	MA
	A	B	M	A			**A**	M	A	MB	MA
	M	**MB**	B	M			**M**	B	M	A	MA
	B	MB	MB	B			**B**	MB	**B**	M	A

	MB	MB	MB	MB			**MB**	MB	MB	B	M

MOTIVO:

la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana , cuenta con un personal capacitado que manipulan todos los equipos y sistemas con los que trabaja la institución, por ende la frecuencia del riesgo por esta amenaza es baja.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 16 AMENAZA -Errores y Fallos No Intencionados – Indisponibilidad Del Personal

[E.17] INDISPONIBILIDAD DEL PERSONAL

TIPOS DE ACTIVOS:	**DIMENSIONES:**
• [P] Personal Interno	1. [D] Disponibilidad

DESCRIPCIÓN:
Ausencia accidental en el puesto de trabajo: enfermedad, entre otros motivos.

ESTIMACIÓN DEL IMPACTO

IMPACTO		**DEGRADACION**		
		1 %	**10 %**	**100%**
VALOR	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	**MB**	MB	B
	MB	MB	MB	MB

ESTIMACIÓN DEL RIESGO

RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	**M**	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

MOTIVO:
La ausencia del personal dentro de ciertas dependencias de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana es frecuente a pesar de esto el impacto en el riesgo es muy bajo, debido a que los sistemas trabajan de una manera correcta.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Tabla 17 AMENAZA-Ataques Intencionados – Robo

[A.15] ROBO

TIPOS DE ACTIVOS:	**DIMENSIONES:**
• [HW] Equipos informáticos (hardware) • [COM] Redes de comunicaciones • [SI] Soportes de información • [AUX]Equipamiento Auxiliar	1. [D] Disponibilidad 2. [C] Confidencialidad

DESCRIPCIÓN:
La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información lo más habituales.
El robo puede realizarlo el personal interno, personas ajenas a la organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

ESTIMACIÓN DEL IMPACTO						ESTIMACIÓN DEL RIESGO					
		DEGRADACION						FRECUENCIA			
IMPACTO		1 %	10 %	100%		RIESGO		PF	FN	F	MF
VALOR	MA	M	A	MA		IMPACTO	MA	A	MA	MA	MA
	A	B	M	**A**			A	M	A	MB	MA
	M	MB	B	M			M	B	M	A	MA
	B	MB	MB	B			B	**MB**	B	M	A
	MB	MB	MB	MB			MB	MB	MB	B	M

MOTIVO:
En caso de que se materialice esta amenaza, el riesgo de impacto a pesar de que sea poco frecuente sería medio.

MA muy alto, A alto, M medio, B bajo, MB muy bajo
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.5. SALVAGUARDAS

Las salvaguardas a establecer han sido seleccionadas teniendo en cuenta los atributos del bien y la información a proteger (confidencialidad, integridad y disponibilidad). En la selección de las salvaguardas se consideraron las características de la amenaza, la vulnerabilidad o probabilidad de materialización y el impacto o daño producido por una potencial amenaza.

En las tablas se describe cada una de las amenazas, además se determina la o las salvaguardas para cada una de estas y el costo monetario que esta implica.

Tabla 18. SALVAGUARDA – Determinación de Salvaguardas – Fuego

AMENAZAS			SALVAGUARDA		
NUMERO	AMENAZA		TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
01	FUEGO		Se debe situar el equipamiento que soporta a la aplicación, así como los soportes de información en áreas seguras y protegidas adecuadamente.		4920,00
			Se debe proteger los ambientes de amenazas potenciales: eléctricas, incendios, clima, agua, interferencias, agentes químicos y otros.	4000,00	

			Dotar de extintores, estos serán ubicados en lugares estratégicos para que sean utilizados de manera oportuna, además se debe de tomar en cuenta que son equipos de fácil manejo y por ende la capacitación de todo el personal en el manejo de las mismas en muy importante ya que serán estos quienes serán los encargados de utilizarlos en el momento adecuado	920,00	

Tabla 19. SALVAGUARDA – Determinación de Salvaguardas – Daños Por Agua

AMENAZAS			**SALVAGUARDA**		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
2	DAÑOS POR AGUA	6580,07	Los activos informáticos tienes que estar ubicados estratégicamente.		0,00
			Mantenimiento de la red de agua, ya que por razones del paso del tiempo tiende a deteriorarse y es necesario el mantenimiento de la misma		

Tabla 20. SALVAGUARDAS – Determinación de Salvaguardas – Desastres Industriales

AMENAZAS			**SALVAGUARDA**		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
3	DESASTRES INDUSTRIALES	29199,08	Se deben adoptar medidas adicionales específicas para el control de acceso de terceras partes		17965,00
			Climatización de las oficinas, para ofrecer un ambiente de trabajo más	7200,00	
			Mantenimiento constante a la red de cableado eléctrico	10765,00	
			Se deberá preparar y mantener operativo un plan de contingencias.		

Tabla 21 SALVAGUARDA – Determinación de Salvaguardas – Contaminación Mecánica.

AMENAZAS			SALVAGUARDAS		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
4	CONTAMINACION MECANICA	308440,96	Limpieza especializada de las oficinas, este tipo de actividad se encarga de remover todo el polvo con máquinas apropiadas para dicha labor y así de esta manera todo el polvo que se acumula sea extraído por estos equipos y no afecten a los sistemas informáticos	1054,00	1054,00

Tabla 22. Determinación de Salvaguardas – Corte De Suministro Eléctrico

AMENAZAS			SALVAGUARDA		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
5	CORTE DE SUMINISTRO ELÉCTRICO	25549,19	Mantenimiento constante a la red de cableado eléctrico.	10765,00	49965,00
			Repotenciar el sistema eléctrico de la Facultad de Ingeniería - UNAP, debido al crecimiento de oficinas.	7200,00	
			Adquirir una planta generadora de electricidad, que en el caso de que el fluido de energía sea suspendido por cualquier inconveniente esta se ponga en marcha.	32000,00	

Tabla 23. SALVAGUARDA – Determinación de Salvaguardas – Interrupción De Otros Servicios Y Suministros Esenciales

AMENAZAS			SALVAGUARDA		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.

6	INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	4935,06	Elaboración de un plan de adquisición, de esta manera se puede mantener abastecida las oficinas con suministros de impresión tales como papel para las impresoras, tóner, refrigerante, entre otros.		0,00

Tabla 24. SALVAGUARDA – Determinación de Salvaguardas – Degradación De Los Soportes De Almacenamiento De La Información

AMENAZAS			**SALVAGUARDA**		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
7	DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	7402,58	Respaldo de la información, es de suma importancia el Backup de la información en la nube esto ayudará en el inmediata recuperación del dato y por ende en la pronta utilización del mismo	0,00	600,00
			Utilización de nuevos y modernos dispositivos de almacenamiento masivo sean estos discos duros externos, flash, memory; esto servirá para tener a disposición en cualquier momento la información y sobre todo respaldada la información en varios medios	600,00	

Tabla 25. SALVAGUARDA – Determinación de Salvaguardas – Errores De Los Usuarios

AMENAZAS			**SALVAGUARDA**		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
8	ERRORES DE LOS USUARIOS	4112,55	Se deben definir y documentar las funciones y obligaciones del personal		0,00
			Se debe suministrar al personal que maneje datos de carácter personal u otra información cuya protección sea necesaria, el mobiliario adecuado para guardar la información		

Tabla 26. SALVAGUARDA - Determinación de Salvaguardas – Indisponibilidad Del Personal

AMENAZAS			**SALVAGUARDA**		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
9	INDISPONIBILIDAD DEL PERSONAL	4935,06	Capacitación a los servidores públicos en temas relacionados con código de ética profesional.	2000,00	2000,00

Tabla 27. SALVAGUARDA – Determinación de Salvaguardas – Robo

AMENAZAS			SALVAGUARDA		
NUMERO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR S/.	COSTO ESTIMADO S/.
10	ROBO	2056,27	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		5000,00
			Utilización de cámaras de seguridad, esto servirá para tener una idea más clara de los sucesos que ocurren dentro de la institución, por lo general estos equipos generan cierto respeto o temor a las personas a ser filmadas y descubiertas en cualquier tipo de ilícito	5000,00	
			Limitar el acceso a personas ajenas, esto evitara que personas no autorizadas tengan acceso a las oficinas y así evitan la posible pérdida equipos		

3.2. PLAN DE CONTINGENCIA

3.2.1. PROCEDIMIENTOS GENERALES

3.2.1.1. Procedimientos Preventivos

1. No ubicar ni almacenar elementos inflamables como papel, gasolina, éter, bebidas alcohólicas, alcohol, trapos sobre los activos analizados.

2. Se debe garantizar una temperatura adecuada para el buen funcionamiento de los activos.

   - En cuartos que no posean equipos electrónicos, la temperatura debe mantenerse continuamente entre 10 y 33 grados centígrados y la humedad relativa debe mantenerse en 85%.
   - En cuartos donde existan equipos electrónicos la temperatura debe mantenerse entre 18 y 24 grados centígrados y la humedad relativa entre 30% y 55%.

3. La ubicación de los equipos debe ser preferiblemente en lugares donde existen paredes de concretos.

4. No se deben ubicar papeleras de basura en el rugar destinado como nodo de comunicaciones, ya que se pueden convertir en la causa de un posible incendio.

5. Se debe tener extintores de polvo químico seco y de bióxido de carbono, en lugares visibles y cercanos donde de se encuentran ubicados los nodos de comunicaciones.

6. Se debe capacitar al personal sobre el manejo de los diferentes extintores con que cuenta.

7. No fumar en lugares donde se encuentra los equipos de comunicaciones y especialmente en la Facultad de Ingeniería de Sistemas e Informática.

8. Nunca consumir alimentos ni ingerir bebidas cerca de los equipos de comunicaciones.

9. No manipular los equipos de comunicaciones en estados de embriaguez ni ba.jo efecto de sustancias alucinógenas.

10. Controlar el acceso de paquetes en los locales que albergan a los nodos de comunicaciones.

11. Tener una excelente distribución eléctrica, evitando conectar los equipos en una misma fuente.

12. Evitar extensiones y cables sueltos cerca de los equipos.

13. Instalar alarmas de activación manuar o automáticas en caso de incendio o sobrecalentamiento de los equipos.

14. Evitar la acumulación de la energía estática, referenciado todos los equipos a una misma tierra.

15. Todos los equipos deben tener protección contra cortocircuitos y sobre voltaje ya sea interna o externa.

16. Usar siempre brazalete antiestático cuando se manipulen componentes electrónicos.

17. No ubicar aparatos eléctricos dentro de los nodos de comunicaciones y puntos de energía regulada tales como grabadoras, hornos microondas, licuadoras, televisores y demás.

18. Verificar diariamente el correcto funcionamiento de las lámparas y tomacorrientes ubicados en los nodos de comunicaciones.

19. La ubicación de los nodos de comunicaciones debe estar en sitio interior, de alta seguridad, no tener ventanales y no existir tuberías alrededor.

20. Los equipos de comunicaciones soro deben ser manipulados por el personal que tenga los suficientes conocimientos acerca de ellos.

21. Permitir solo el acceso ai personal que realice labores de operación y mantenimientos de los equipos de comunicaciones.

22. Mantener información en archivos e impreso de los proveedores y garantías vigentes de todos los equipos utilizados en los nodos de comunicaciones.

23. Tener actualizada la información de los proveedores y empresas que brinden soporte y mantenimiento de los diferentes equipos de comunicaciones.

24. Tener pólizas de los seguros vigentes de los bienes informáticos, que cubran daños, actos mal intencionados, hurto y una póliza de transporte de equipos móviles.

25. Guardar en un archivo, la información sobre la configuración inicial de todos los equipos de comunicaciones, tanto dentro como fuera de la Universidad Nacional de la Amazonía peruana.

26. Destinar un sitio seguro y de acceso restringido, para guardar manuales, software de instalación, documentación de los equipos de comunicación; ejerciendo un estricto control sobre su uso.

27. Capacitar continuamente al personal sobre tecnología de punto para que tengan conocimientos sobre esto.

28. Ubicar sensores de humedad, en ros locales que albergan los nodos de comunicaciones; para regular las condiciones ambientales óptimas para los equipos de comunicaciones.

29. Ubicar sensores de humos, en los locales que albergan los nodos de comunicaciones.

30. Tener un sistema automatizado que permita el registro, control, administración; que permita manejar una ficha u hoja de vida detallada de

los equipos de comunicaciones; que contengan, además, el seguimiento de los mantenimientos, preventivos y correctivos, realizados y programados de los equipos; esto permitirá mantener actualizado el inventario de hardware en forma permanente.

31. Tener un sistema automatizado que permita el registro, control, administración de todas las aplicaciones, programas y licencias, adquiridos por la entidad; al máximo nivel de detalle posible; esto permitirá mantener actualizado el inventario de software en forma permanente.

3.2.1.2. Procedimientos Correctivos

1. Verificar el sistema de protección Eléctrica, que esté funcionando correctamente, para tal fin ver procedimientos del sistema de Protección Eléctrica.

2. Verificar si el sistema de switches, que esté funcionando correctamente, para tal fin, ver procedimientos del sistema de Switches.

3. Verificar que el o los sistemas de servidores al que se desean acceder estén encendidos.

3.2.2. SISTEMA DE SWITCHES

3.2.2.1. Procedimientos Preventivos

1. Instalar los switches en gabinete cerrado con seguro, para impedir el acceso de persona no autorizado.

2. Marcar adecuadamente los puertos de switches mediante un código que tenga relación con ia estructura de la red.

3. Al instalar un módulo en los switches, con este equipo encendido, asegúrese de no introducir objetos extraños dentro del slot.

4. Después de insertar un módulo verificar, que el LED de encendido quede finalmente en verde para garantizar su buena instalación.

5. Revisar periódicamente los LEDS ubicados en la parte frontal de los switches, que indica el estado de operación del mismo y de sus componentes. Estos LEDS pueden ser muy útiles en determinados casos, especificando las causas de determinados problemas.

6. Habilitar el protocolo RIP para que genere sus tablas de enrutamiento con los routers y los servidores que trabajan con dichos protocolos.

7. Habilitar el protocolo ARP para que los switches interactué con los diferentes routers que se encuentran en la red.

8. Se configurará direcciones estáticas a los módulos y sus puertos como una forma de dar seguridad a la red.

9. En casos que existan segmentos que trabajen con protocolos que sólo se requieren en dicho segmento, se podrían habilitar filtros para evitar su tráfico en otros segmentos.

10. Implementar filtros que eviten la comunicación de determinadas estaciones segmentos con otros, con el objeto de dar mayor seguridad a la red.

3.2.2.2. Procedimientos Correctivos

1. Verificar que los niveles de voltaje de alimentación sean los correctos, posiblemente el software del Switch no está funcionando correctamente, llamar al distribuidor del equipo o a la empresa encargada del mantenimiento.

2. Verificar que la temperatura ambiente donde se encuentra instalado el Switch cumpla con los requerimientos del sistema.

3. En caso de que la temperatura sea muy alta, tomar las medidas necesarias de acuerdo a la situación para asegurar el correcto funcionamiento del equipo.

4. Reiniciar el equipo.

5. Encender el sistema. Si el sistema opera por lo menos 10 minutos, sin apagarse, reemplazar el modulo.

6. Verifique que los cables UTP estén bien conectados a los puertos RJ 45 de los Módulos ESM.

7. Remueve el módulo en cuestión, instálelo de nuevo y reinicie el equipo.

8. Acceder al Switch a través de Telnet con el usuario administrador, y corre la opción de diagnóstico sobre el módulo en cuestión.

9. Verifique la integridad de los cables que están conectados a los puertos del módulo.

10. Si el puerto continúa en amarillo contacte a su distribuidor ó empresa de mantenimiento.

11. Verifique que los cables de potencia estén finalmente conectados al equipo y que haya suministro de energía.

12. Verifique que el interruptor de encendido se encuentre en posición “ON”.

13. Reinicie el equipo apagando y encendiendo repetidamente a través del interruptor de encendido.

14. Verificar que las rejillas de ventilación estén limpias y despejadas.

15. Verifique que el ventilador del equipo esté funcionando correctamente (Ver manual "setup guide").

16. Verifique que el sistema esté conectado debidamente al suministro de AC y el voltaje adecuado.

17. Conectar los equipos (Servidores, consolas, etc.) más necesarias a los Switches.

- Se delegará un responsable para la configuración del Firewall.
- Se bloqueará todo el tráfico, excepto el explícitamente aprobado.
- Se revisará semanalmente el tráfico autorizado.
- Se revisará diariamente las trazas de actividad.
- Se ocultará los puertos internos.

- Se debe instalar las nuevas versiones del fabricante del producto.
- Se instalará los parches del fabricante del producto.
- Se realizará pruebas de regresión antes de instalar una nueva versión o parche.

3.2.3. SISTEMA DE PROTECCIÓN ELÉCTRICA

3.2.3.1. Procedimientos Preventivos

1. Revisar periódicamente todos los mensajes y el menú de control del UPS, para precisar el estado general de la misma sus parámetros de medición, el estado de la batería y alarmas y la configuración del sistema. Para luego confrontarlo con los valores requeridos y recomendados por el proveedor.

2. Asegurar la buena ventilación y alimentación del UPS.
3. Definir una política de finalización de tareas con el objetivo de disminuir gradualmente la carga del uso del UPS, en el momento de una interrupción eléctrica, según las necesidades certificadas y la potencia de las baterías.

4. Emplear las tomas que estén conectados al UPS sólo para conectar los equipos de comunicación de misión crítica en ningún momento pueden ser conectados lámparas, ventiladores, hornos microondas y otros.

5. El UPS tiene una fuente propia de energía (baterías), cuando no está conectado a una fuente de corriente directa pueden estar presentes altos voltajes en los terminales 9 y 10 (terminales para conexión remota de la batería), cuando el UPS está funcionando con la batería.

6. Al desenergizar completamente el UPS, disparar el breque de salida. Luego dispara el breque de entrada y el breque de la batería.

7. Se corre el riesgo de una descarga eléctrica al instalar la batería, esta tarea debe ser realizada por personal de servicio especializado.

8. No disponer de las baterías en caso de presentarse un incendio. Las baterías pueden explotar al estar expuestas a las llamas.

9. Todos los gabinetes donde se encuentren equipos de comunicaciones deben ser de seguridad.

10. Una batería puede presentar riesgo de una fuerte descarga eléctrica, por esta causa puede quemarse o explotar. Se debe tener todas las precauciones.

11. Proteger colocando una banda en el botón Emergency Power – Off para evitar que sea presionado por personal no autorizado.

12. Se debe instalar un generador de respaldo para los nodos que conforman el Back Bone de Fibra Óptica e Inalámbrica.

13. Poso a Tierra para Descarga Eléctrica

14. La inspección de los pozos a tierra para descargas eléctricas, se realizan cada trimestre; para elegir el día de la inspección se debe de tomar en cuenta que no haya llovido por lo menos tres días antes; para garantizar poca humedad en los suelos para evaluar la resistencia y las conexiones de los pozos.

3.2.3.2. Procedimientos Correctivos

1. Si el fallo de energía es de un periodo prolongado se debe activar el generador de respaldo.

2. Poso a Tierra para descarga eléctrica

3. Los trabajos para el mantenimiento de los pozos a tierra para descarga eléctrica se deben realizar con la supervisión de un Ingeniero Electrónico o Eléctrico y un Personal de Apoyo para cubrir todos los alcances y medidas de seguridad que permitan realizar estos con la confiabilidad y seguridad Eléctrica, que amerite un óptimo trabajo.

4. Se usará para mediciones de resistividad del terreno y de voltaje (para casos que exista alguna línea de voltaje cercana al pozo, o voltajes indirectos que se refleje en el pozo) un medidor digital, Instrumento que facilita efectuar 02 tipos de medición (medición normal y método corto).

5. De acuerdo a los resultados medidos iníciales en cada uno de los pozos; estos serán agrupados o clasificados para la realización

3.2.4. RED LAN

3.2.4.1. Procedimientos preventivos

1. No se debe realizar empates es decir múltiples apariciones del par de cables en diversos puntos de distribución.

2. El destrenzado de pares individuares en los conectores y paneles de empate debe ser menor a 1.25 cm.

3. En la ruta del cableado de los clósets a los nodos se debe evitar el paso por dispositivos eléctricos como equipos de soldaduras, aire acondicionado, ventiladores, intercomunicadores, luces fluorescentes y balastos; debe pasar mínimo a una distancia de 12 cm.

4. El cableado debe pasar mínimo a 1.2 m de los motores eléctricos grandes o transformadores.

5. EI cableado debe estar distantes de los cables de corriente alterna con 2KVA o menos de 13cm, de cables de 2KVA a 5KVA debe estar distante de 30cm y de cables de 5KVA mínimo 91cm.

6. Ubicar en la Facultad de Ingeniería de Sistemas e Informática el diagrama del cableado de red, éste debe indicar claramente el diagrama de distribución, el puerto asignado a cada toma de información, a cada servidor y en general a cada una de las conexiones.

3.2.4.2. Procedimientos Correctivos

1. Verificar el estado del conector RJ-45 y los colores estándar utilizados en la conexión.

2. Conectar otro equipo al Terminal del RJ45; comprobar si este realiza todas las operaciones en la red.

3. Por medio de un chequeador de cableado, comprobar el funcionamiento del cable según el estándar EIA/TIA 568A desde el punto de la red hasta el Patch panel donde se encuentra ubicado el centro del cableado.

4. Verificar el estado de conexión en el concentrador respectivo.

5. Observar si existen cables de energía cerca, y evaluar la influencia de estos sobre el par trenzado del cable UTP.

6. Llevar un cable desde el puerto de conexión ubicado en el centro de cableado, hasta la tarjeta de red del equipo y verificar su funcionamiento de red.

7. Si el equipo funciona luego del procedimiento anterior, cambiar el cable UTP que va por el tendido horizontal.

3.3. PLAN DE CONTINGENCIA ADICIONAL

Para realizar el plan de contingencia se tomó en cuenta la parte del software, hardware, y redes incluyendo la seguridad de estos artículos, se estimó lo siguiente:

3.3.1 Instalación de tarjetas inalámbricas

Se tiene que existe la necesidad de implementar con tarjetas de red inalámbricas para las PC'S de los laboratorios para el mejor desempeño en cuanto al compartido de recursos, para mejorar la red en esos ambientes deben ser de forma inalámbricas.

Esto implica que se necesita lo siguiente:

Tabla 28. Presupuesto de tarjetas inalámbricas

Cant.	Descripción	Precio Unitario S/.	Precio total S/.
60	Tp-link Tarjeta Inalámbrico N 300m Tl-wn881nd Pci	42	2520
	Mano de obra	20	1200
2	Access point	135	270
Total			3990

Para realizar esta actividad se tiene el siguiente cronograma:

Tabla 29. Cronograma de actividades para instalación de tarjetas inalámbricas.

Nº	Nombre de la tarea	Duración dias	Precede
01	Compra de los elementos	07	
02	Instalación de las tarjetas inalámbricas lab 1	07	1
03	Prueba de las tarjetas inalámbricas lab 1	03	2
04	Instalación de las tarjetas inalámbricas lab 2	07	3

05	Prueba de las tarjetas inalámbricas lab 2	03	4
06	Instalación y configuración de los ap en cada uno de los laboratorios.	03	5

Instalación de cámaras de seguridad para evitar robos.

La compra de estos accesorios es en conjunto y es de acuerdo a la ubicación de los ambientes donde serán necesarios, esto quiero decir que la compra de estas cámaras será por grupo. Y esto se ubicará de la siguiente forma:

Instalación en la dirección de la More Nº 280:

1. Una cámara de seguridad en la entrada de la facultad.
2. Una cámara de seguridad en el corredor del primer piso.
3. Dos cámaras de seguridad tanto en la entrada del interior del laboratorio 1, como la parte frontal de la puerta para tener el percato de quien ingresa, la vista de las PC'S.
4. Una cámara de seguridad en el interior de la oficina de asuntos académicos.
5. Una cámara de seguridad en el interior del centro de Información (Biblioteca).
6. Una cámara de seguridad en el corredor del segundo piso.
7. Una cámara de seguridad de en el interior de la Dirección de Escuela.
8. Una cámara de seguridad en el interior de la Oficina de Asuntos económicos.
9. Una cámara de seguridad en el interior de la Oficina de la Secretaría Académica.
10. Una cámara de seguridad en el interior de la Oficina de decanatura.

Haciendo un total de 11 cámaras, lo cual nos hace precisar del siguiente kit* de cámaras incluyendo un DVR:

- 8 CAMARA TUBO COLOR CMOS IR
- 8 CAMARA DOMO COLOR CMOS IR

* Fuente http://digitalcomperu.com/home/226-kit-de-16-camaras-sunivision.html

- 1 H.264 Real Time 16CH DVR AP-7316LV support mobile view Network DVR video & audio
- Control remote y mouse
- 16 Fuentes de Poder
- Haciendo un costo de S/2,099.^{00}
- Otros materiales como:
    - [**]Cable Utp X Rollo De 305 Mts Cat 5e - 6 - 6a – 7 a un costo de S/. 110.^{00}
    - Cintas aislantes con un monto de S/. 20.^{00}
    - Cuter S/. 10.^{00}
- Con una mano de obra de S/.300.^{00} instalación y configuración de los equipos

Con un total de S/. 2539.^{00} es el coste total de esta operación.

La ubicación del DVR debería estar en el decanato ya que la no hay mucho acceso a este ambiente, y así propiciar la seguridad de este dispositivo.

Instalación en la dirección de la Pevas 5º cuadra

Para este ambiente solo dos cámaras wifi uno a la entrada y otra a la salida.

- 2 [***]CAM IP WANSCAM/ WIFI ROTATORIO A un costo de S/. 249.^{00} a un costo total de S/. 498.00,
- Mano de obra de S/. 100.^{00}

Para realizar esta actividad se tiene el siguiente cronograma:

Tabla 30. Cronograma de actividades de instalación de cámaras de seguridad

Nº	Nombre de la tarea	Duración días	Precede
01	Compra de los elementos	14	
02	Instalación de las cámaras de seguridad del lab 1	10	1
03	Instalación del DVR	03	2

[**] Fuente http://listado.mercadolibre.com.pe/rollo-de-cable-utp-nivel
[***] Fuente http://digitalcomperu.com/home/camaras-ip/156-camara-ip-rotatoria.html

04	Instalación de las cámaras de seguridad lab 2	04	3
05	Prueba de las cámaras de seguridad lab1	03	4
06	Prueba de las cámaras de seguridad lab 2	03	5

Servicio de Seguridad: Para reforzar la seguridad de los equipos que existen en la facultad se propone una persona netamente en la seguridad, con el siguiente perfil:

- Egresado de las fuerzas armadas.
- Mayor de 18 menores de 40 años.
- Siendo un sueldo de s/. 800.^{00} mensuales.

Resguardo de la Información en la Nube (Cloud).

Esto implica conseguirse o suscribirse en servicios de resguardo de información el más recomendado es el siguiente:

- **www.mediafire.com**,[@] que da un espacio gratuito de 50 Gb de almacenamiento, pero superado esta capacidad se puede pagar por un monto de $ 15.^{00} para una capacidad de almacenamiento de 500 Gb.

Esto permitirá que el personal, docentes y alumnos de la facultad puedan guardar su información en la nube y lograr de esa forma tener respaldo (Back up) de información donde quiera que vayan, en el caso de incendio u otros accidentes propios que puedan existir en la Facultad.

Incluir [(*)]extintores de incendio:

Esto es para uso correctivo en caso de incendios, los cuales deben estar ubicados en zonas estratégicas de fácil acceso.

El costo de estos extintores esta alrededor de S/. 300.^{00} por extintor en este caso se necesitaría 5 haciendo un costo total de S/. 1500.^{00}, con un mantenimiento anual de recarga de S/. 80.^{00} anual, siendo un costo de S/. 400.^{00} por los 5 extintores.

Corte de suministro de energía:

De lo encontrado se propone establecer dos cosas:

- Instalar un Generador[@@] de luz:

[@] Fuente http://es.gizmodo.com/los-mejores-servicios-para-guardar-tu-contenido-en-la-n-458373905

[(*)] Fuente http://extintoresperu.com/productos.html

[@@] Fuente http://articulo.mercadolibre.com.pe/MPE-410090358-generador-7kw-tahoe-diesel-honda-hecho-en-canada-_JM

FIGURA 03. GENERADOR DE LUZ

- **UPS**:
  Instalar por lo menos un UPS en cada ambiente, esto equivale comprar:

FIGURA 04. UPS

Tabla 31. Presupuesto de UPS

Cant.	Descripción	Precio Unitario S/.	Precio total S/.
08	Ups Apc 500v Modelo Br500ci-apc	**224.00**	1792.00
	Mano de obra	**100.00**	
Total			1792.00

Software Propuesto:

Los softwares propuestos son los siguientes:

- Sistema de Trámite de documentario.
- Sistema de control de asistencia.
- Sistema de resguardo de información de Titulación.

CAPITULO IV

RESULTADO

En el análisis realizado a la Facultad de Ingeniería de Sistema e Informática de la Universidad Nacional de la Amazonía Peruana, me permitió determinar la cantidad de equipos y sistemas informáticos con los que cuenta la Institución, así como también se obtuvo el valor real de los mismos; entre los activos se encuentran, computadores, impresoras, computador tipo servidor, llegando a un monto total de treinta tres mil cuatrocientos treinta y cuatro Nuevos Soles; de igual manera se obtuvo datos de las licencias (software) llegando a un monto total de Un mil seiscientos ochenta y dos Nuevos Soles, el valor de información asciende a un monto total de Treinta y cinco mil ciento diez y seis Nuevos Soles.

Tabla 32. Costo de HARDWARE y SOFTWARE encontrados (Costo inicial y Actual)

DETALLES	COSTO INICIAL	COSTO ACTUAL
Hardware	55100,00	33434,00
Software		1682,00
Información (Dato)		35116,00

Con la estimación del riesgo y del impacto sobre el activo, se obtuvo un catálogo de posibles amenazas sobre los activos de un sistema de información, para cada amenaza se recurre a una matriz tal como se ilustra en el Cuadro 1 y se determinó la priorización de los activos a ser intervenidos de manera prioritaria.

Se elaboró un listado amenazas para los equipos y sistemas de información valorando el riesgo para cada una de ellas según el impacto y la frecuencia de estas, además se establecieron salvaguardas para cada una de estas amenazas según la magnitud de riesgo dentro de la institución.

Se desarrolló un plan de contingencia con la utilización de todos los componentes que forman parte de los sistemas informáticos, en el mencionado Plan se encuentran recomendaciones de soluciones que ayudaran a reducir el riesgo de cada una de las amenazas contempladas, así mismo un Plan de Contingencia Adicional con soluciones que la institución puede adoptar para

asegurar la continuidad de las funciones en caso de que se materialice amenazas.

CAPITULO V

DISCUSIÓN

Para el desarrollo del plan de contingencia de los activos informáticos, se realizó el análisis, detección, evaluación y priorización de las amenazas potenciales de las que puede ser víctima la institución, así mismo se priorizó las actividades más relevantes para la organización, además a través de este se pudo determinar el valor económico actual de los equipos y principalmente de los sistemas informáticos (valor del dato); en comparación de otros trabajos que se limitan en abarcar solo el hardware o la parte del software en su defecto tratan de manera superficial cada uno de estos, en varios repositorios que se encuentran ubicados en la nube se pueden encontrar trabajos con el tema titulado **PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA**, inclinado este para los Laboratorios de Redes e Informática que comprenden tres sub-planes (Prevención Contención y Recuperación), permitiendo que el personal que labora en los Laboratorios de Redes e Informática pueda actuar ante cualquier desastre, ya este sea natural o accidental reduciendo el costo y tiempo.

Otro tema que sirvió de análisis para el desarrollo de esta tesis fue el proyecto titulado **PLAN DE CONTINGENCIA INFORMÁTICO PARA EL CONJUNTO DE BODEGAS PARKENOR.**

En ambos trabajos implica el estudio de los componentes del Hardware y Software abarcando de esta manera el estudio de los mismos sin determinar el valor de los activos y mucho menos de los datos; es por esta razón que se considera que el presente trabajo investigativo tiene relevancia, ya que se considera de un valor muy importante los activos y de mayor consideración la información ambas necesarias para llevar a efecto un plan de contingencia en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana.

CAPITULO VI

CONCLUSIONES

1. Mientras el valor del hardware se deprecia en su valor monetario el valor de la información incrementa de una manera considerable para la Institución.

2. Con la ponderación del riesgo se puede establecer que los activos dentro de la institución están propensos a múltiples amenazas de diversa índole que podrían materializarse en cualquier momento.

3. Con la utilización de actividades destinadas a la protección de los equipos y sistemas de información se puede mitigar el riesgo de una forma considerable para la institución.

4. Con la implementación de cualquier tipo de salvaguardas no existe la seguridad de eliminar totalmente la amenaza y por ende el riesgo que conlleva para los activos.

5. El Plan de contingencia servirá como una guía didáctica en caso de que se materialice una amenaza afectando al normal funcionamiento de la Institución.

6. Estableciendo además una manera ordenada de actividades que se deben de poner en práctica, en la Facultad de Ingeniería de Sistema e Informática de la Universidad Nacional de la Amazonía Peruana, contará con una herramienta muy importante la cual le permitirá recuperarse ante las posibles fallas y siniestros ocasionados por agentes internos o externos a la misma.

CAPITULO VII

RECOMENDACIONES

1. Crear las políticas de seguridad que apoyen a los procedimientos preventivos implantados en el plan de contingencia.

2. Los usuarios finales deben ser capacitados anualmente para que sepan advertir las amenazas que surgieran en los activos asignados.

3. Se debería activar el Servicio del Directorio Activo para la mejor administración de objetos de la red.

4. Adoptar MAGERIT como metodología que permite establecer fases que nos ayudará a proyectar el objetivo de la seguridad a largo plazo.

5. El personal que asumirá los roles establecidos en el plan de contingencia debe ser capacitado anualmente en sus funciones.

6. Se propone 3 perfiles para el personal de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana los cuales son: Jefe de Tecnologías de Información, Soporte, supervisar de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

- **[MAGERIT – I – METODO: 2012]**
  Ministerio de Administración públicas, Madrid Octubre del 2012, “MAGERIT - Versión, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, I - Método”, Versión 3.0, http://publicaciones.administración.es,

- **[CONTINGENCIA: 2005]**
  Plan de contingencia para los Bienes Informáticos. pdf, Versión 2. Medellín: Unidad de Sistemas e Informática; 2005, páginas 48-90.

- **[Redes y Comunicaciones: 2007]**
  William Stallings, Richard van Slyke; Prentice Hall. Bussiness Data Communications. 2007. Pág. 100 – 133.

- **[MAGERIT – I – MÉTODO: 2012]**
  Ministerio de Administración públicas, Madrid Octubre del 2012 “MAGERIT versión 3, Metodología de Análisis y Gestión de Riesgo Información, I Método", Versión 3.0, MAP, http://publicaciones. administracion.es, 127 páginas.

- **[MAGERIT – II – CATÁLOGO DE ELEMENTOS: 2012]**
  Ministerio de Administración públicas, Madrid Octubre del 2012, “MAGERIT – versión 3, Metodología de Análisis y Gestión de Riesgo de los sistemas de Información, II catálogo de Elementos”, versión 3.0, MAP, https://www.ccn-cert.cni.es/publico, 75 páginas.

- **[MAGERIT – III – GUÍA DE TÉCNICAS: 2012]**
  Ministerio de Administración públicas, Madrid Octubre del 2012, MAGERIT – versión 3, Metodología de Análisis y Gestión de Riesgo de los sistemas de Información, III Guía de Técnicas", versión 3.0, MAP. https://www.ccn-cert.cni.es/publico, 42 páginas.

- [**CONTINGENCIA: 2005]**
  Plan de contingencia para los Bienes Informáticos.pdf. Versión 2. Medellín: Unidad de Sistemas e Informática; 2005, 99 páginas,

- **[URL01]**

Secretaria del Consejo Superior de Administración Electrónica, fecha de acceso el 15 de enero del 2007, URL disponible en: http://www.csi.map.es/

- **[URL02]**
  Ministerio de Administraciones Públicas, fecha de acceso et 10 de febrero del 2007, URL disponible en: http://www.map.es/index.html

- **[URL03]**
  Asociación de Técnicos de Información, fecha de acceso el 20 de febrero del 2007, URL disponible en: http://www.ati.es

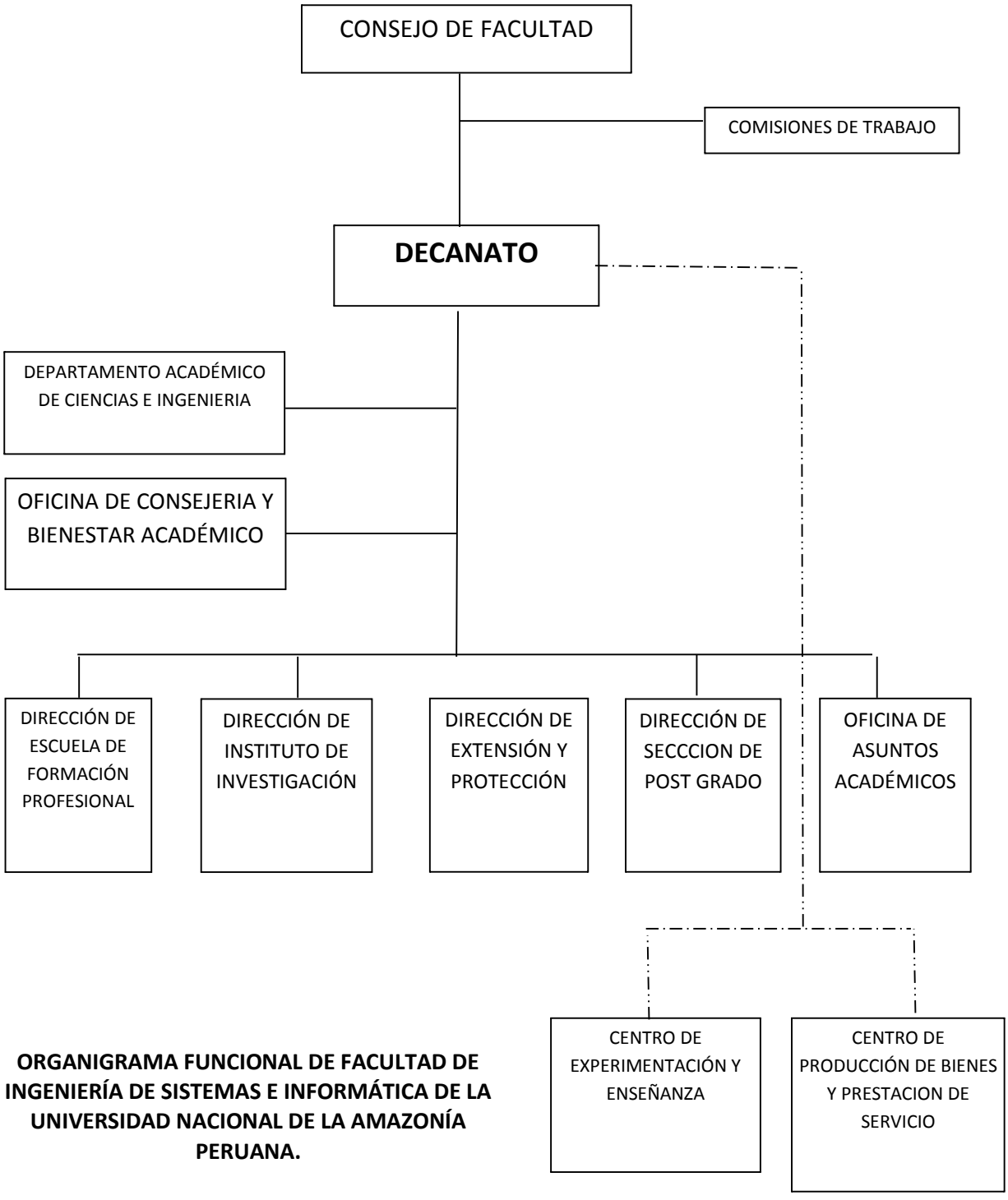
- **[URL04]**
  Oficina Nacional, fecha de acceso el 06 de marzo del2007, URL disponible en: http://www.ongei. gob.pe

- **[URL05]**
  Anuario de Estadísticas Ambientales, fecha de acceso el 07 de marzo del 2007, URL disponible en: http://www.inei.gob,pe

- **[URL06]**
  VOIP: Seguridad y Continuidad del Servicio, fecha de acceso el 08 de marzo del 2007, URL disponible en: http://www.tecnotendencias.com/modules.php?name:News&file:article&sid=741.

- **[URL07]**
  Diarios Tecnológicos, fecha de acceso el 08 de marzo del 2007, URL disponible en: http://www.conocimientosweb.net/dt/article5597.htrnl

ANEXOS



ORGANIGRAMA FUNCIONAL DE FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA.

ESTADO DE LA RED LAN