CAPÍTULO II

2. INVESTIGACIÓN DE CAMPO.

2.1 Generalidades de la investigación de campo.

Este capítulo presenta en su contenido la investigación de campo que se realizó con el propósito de determinar si existe la factibilidad de realizar la propuesta de diseño y desarrollo de Honeynets Virtuales utilizando VMware, para detección de intrusos informáticos y ser aplicada en la Dirección de Tecnología y Comunicaciones.

La investigación de campo cuenta con distintas partes que la integran, estas son: metodología de la investigación utilizada como; las fuentes de información primaria y secundaria, la determinación del universo en donde se realizó.

Posteriormente, se procedió a recolectar la información la cual fue procesada en una matriz vaciado de datos, proporcionándole un análisis e interpretación de los resultados obtenidos.

2.1.1 Objetivos de la investigación de campo.

General

Recopilar información de la Dirección de Tecnología y Comunicaciones de la Universidad Francisco Gavidia, a fin de conocer si es factible la realización de diseño y desarrollo de Honeynets Virtuales para detección de intrusos informáticos.

Específicos

a. Conocer los mecanismos de seguridad que utilizan la Dirección de tecnología y comunicaciones.

b. Descubrir las deficiencias que pueda tener la DTC en cuanto al monitoreo contra los ataques informáticos y sus incidencias.

c. Investigar la factibilidad de desarrollar herramientas de apoyo para mejorar y fortalecer la seguridad de los sistemas informáticos de la Universidad.

2.1.2 Justificación de la investigación de campo.

La investigación realizada por medio del trabajo de campo es de mucha importancia, ya que permitió obtener información de primera mano, las necesidades que la Dirección de Tecnología y Comunicaciones tienen acerca de la seguridad informática, dando así una herramienta de apoyo, y permitiendo dar posibles soluciones a los problemas.

Además permitió identificar aspectos relevantes tales como la falta de reglamentos o políticas de seguridad ante una incidencia o ataques informáticos.

La seguridad informática es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de herramientas y de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

La implementación de medidas de seguridad, es un proceso técnico administrativo, proceso que debe abarcar toda la Universidad en cuanto a organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector de rectoría, ya que

sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria. Resulta claro que proponer la propuesta de diseño de un sistema de seguridad con honeynet genera ganancias a la Dirección de Tecnología y Comunicaciones y a toda la Universidad, pero que trae nueva tarea para la parte técnica, pero es importante recalcar un componente muy importante para la protección de los sistemas, consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la seguridad de la información y de la red.

Metodología para la investigación de campo.

En este punto de investigación se describe detalladamente la forma en que se realizó la investigación.

Las herramientas que se utilizaron para la recopilación de información fue el cuestionario que se paso a la Dirección de Tecnología y Comunicaciones, con el fin de obtener información de primera mano, que permita la consecución de los objetivos propuestos, utilizando la técnica de la encuesta.

El cuestionario está estructurado en seis partes, la primera contiene la solicitud de colaboración, la segunda, el nombre del proyecto, la tercera, el objetivo, la cuarta, las indicaciones, la quinta cuerpo del cuestionario, la sexta los datos de presentación. (ver anexo 1).

a. Fuentes de información.

   Las fuentes de información son todas aquellas personas, empresas, instituciones, documentación, libros, revistas y todo aquello que pueda brindar información relacionada con la investigación. Con el objetivo de obtener información para la investigación de campo, fue necesario obtener todos los datos por medio de las siguientes fuentes.

Fuentes primarias: Para esta investigación la información se obtuvo a través del cuestionario dirigido al personal de la DTC (Dirección de Tecnología y Comunicaciones) y entrevistas a usuarios selectos que velan por la seguridad de la información de la Universidad Francisco Gavidia.

Fuentes secundarias: Fue necesario recopilar información de carácter bibliográfico tales como: libros, informes de seguridad y de toda aquella información escrita relacionada directamente con la manera de cómo realizan el monitoreo de incidentes o ataques informáticos e implementan soluciones de Honeynet, como de proyectos que están actualmente vigentes y que han servido de ejemplo para guiar la propuesta en estudio, así como en bibliotecas, Internet, etc.

b. Determinación del universo o población.

El tipo de universo que se determinó es de carácter finito, ya que se conoce la cantidad de personal que labora en la Dirección de Tecnología y Comunicaciones.

El Universo de la investigación estuvo constituido por 15 personas que conforman la DTC por tal razón no se requirió determinar la muestra, sino que se opto por realizar un censo y fue factible estudiar la opinión de todos.

c. Diseño del instrumento de recolección de datos.

La herramienta que se utilizo es el cuestionario, diseñado con 9 preguntas de esta forma se recopilo la información primaria.

El cuestionario fue organizado de acuerdo a la siguiente estructura:

a. Solicitud de colaboración.
b. Nombre del Proyecto.
c. Objetivo de la Investigación.
d. Indicaciones.
e. Cuerpo del Cuestionario.
f. Datos de Presentación.

Tabulación de la información de la investigación de campo.

Luego de concluida la investigación, se procedió a trasladar los resultados a una matriz vaciado de datos que permitió tener un panorama de todas las interrogantes y sus respectivos porcentajes, para luego proporcionar el análisis de cada una de las preguntas que aparecen en el cuestionario.

A continuación se presentan los gráficos y tablas de cada pregunta con su respectivo análisis.

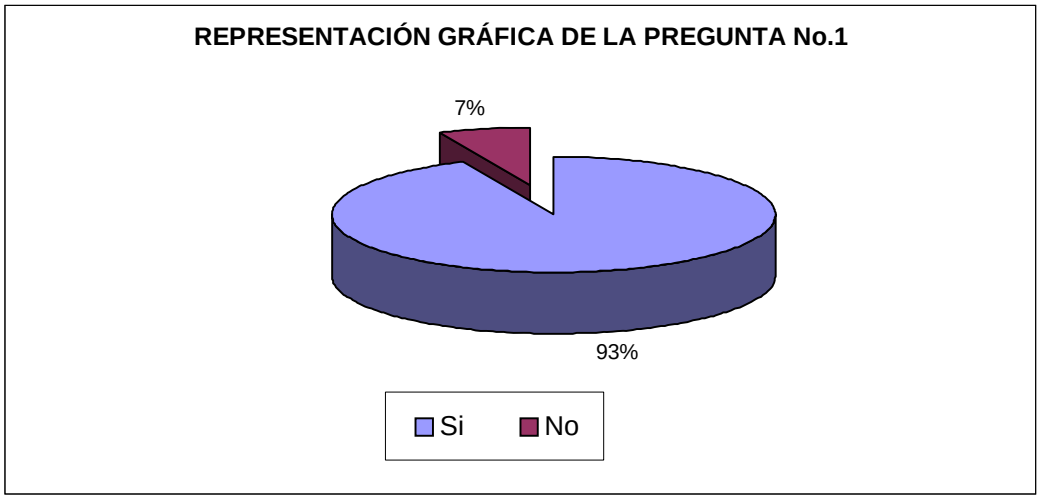
Pregunta No. 1 ¿Conoce usted el riesgo que podrían estar expuestos los sistemas que actualmente poseen a través de las amenazas y/o ataques informáticos?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones tiene conocimiento de la seguridad de la información.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	14	93
No	1	7
TOTALES	15	100

Análisis:

La mayoria de las personas encuestadas están concientes del riesgo en que estan expuextos los sistemas contra los ataques informáticos.



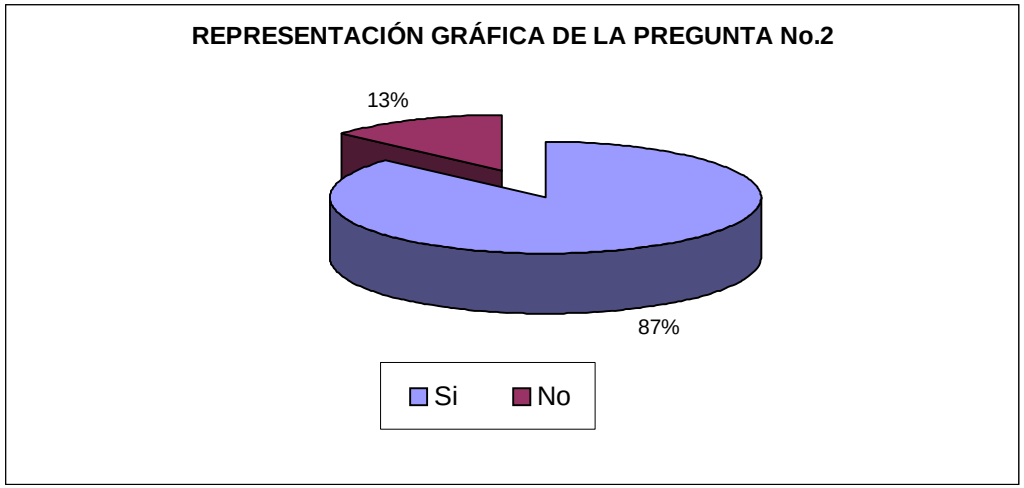
Pregunta No. 2 ¿Se ejerce algún tipo de control en contra de estas amenazas?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones controla la seguridad en los sistemas de información de los ataques informáticos

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	13	87
No	2	13
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que se ejerce un control contra ataques y amenazas a los sistemas informáticos.



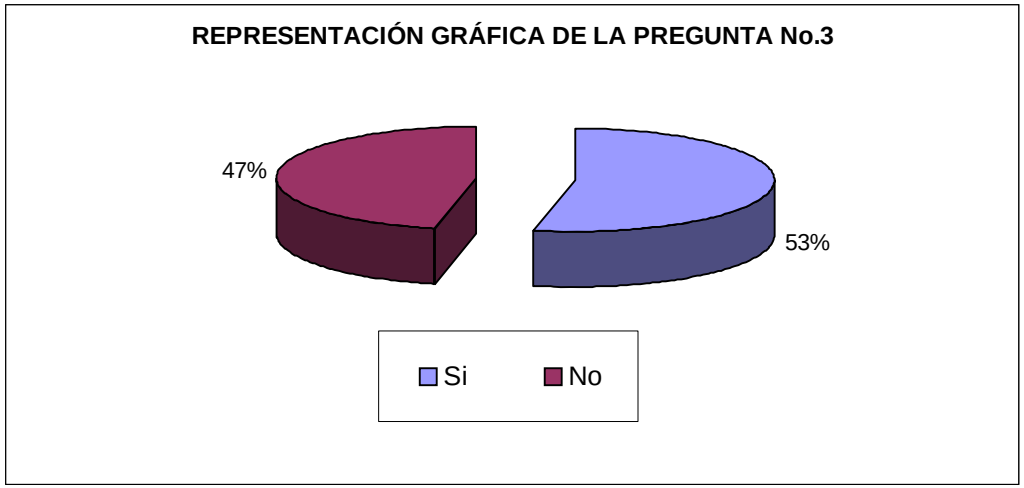
Pregunta No. 3 ¿Se ejerce un control de monitoreo periódico y perenne de estas vulnerabilidades?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones monitorea los sistemas con periodicidad para prevenir los ataques informáticos.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	8	53
No	7	47
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo afirmar por un poco mas de la mitad de las personas encuestadas, que los sistemas están sometidos por un control de monitoreo periódico.



Pregunta No. 4 ¿Si su respuesta es afirmativa a la pregunta anterior, favor comente con que periodicidad estas vulnerabilidades son expuestas a sus sistemas?

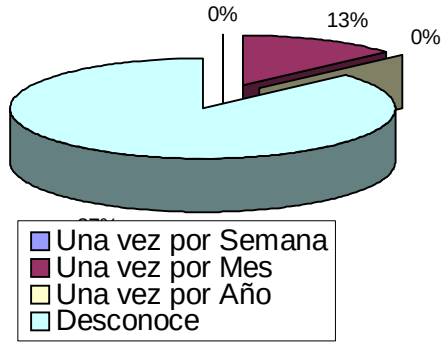
Objetivo: Conocer cual es la periodicidad en que los sistemas son expuestos ante los ataques informáticos.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Una vez por Semana	0	0
Una vez por Mes	2	13
Una vez por Año	0	0
Desconoce	13	87
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que la mayor parte de las personas encuestadas desconoce con que periodicidad se encuentran expuestos los sistemas contra los ataques informáticos.

REPRESENTACIÓN GRÁFICA DE LA PREGUNTA No.4



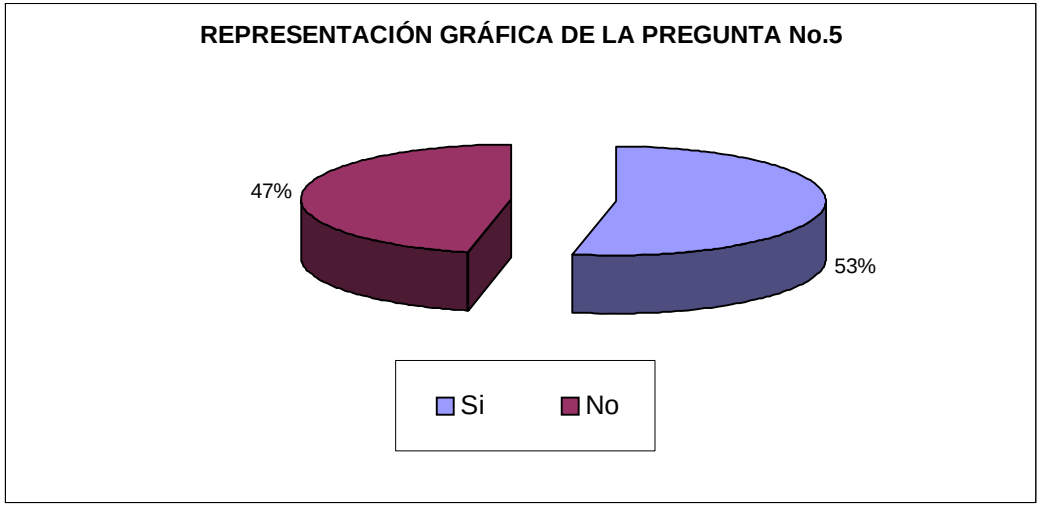
Pregunta No. 5 ¿Tiene usted conocimiento si existe un sistema de seguridad y monitoreo en servidores con servicios públicos en el Internet o la intranet?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones ha implementado un sistema de seguridad y monitoreo en Seridores públicos.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	8	53
No	7	47
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que la mayor parte de las personas encuestadas afirma que existe un sistema de seguridad y monitoreo en los servidores.



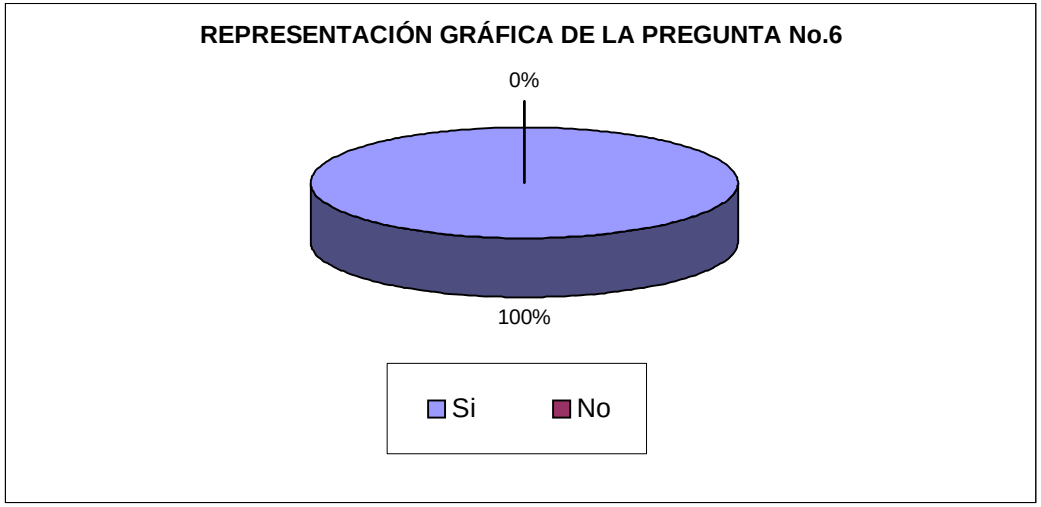
Pregunta No. 6 ¿Le gustaría conocer e implementar un sistema de seguridad con herramientas gratuitas?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones esta interezada en implementar un sistema de seguridad y monitoreo con herramientas gratuitas.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	15	100
No	0	0
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que todas las personas consultadas afirman que están interezadas en implementar un sistema de seguridad y monitoreo con herramientas gratuitas.



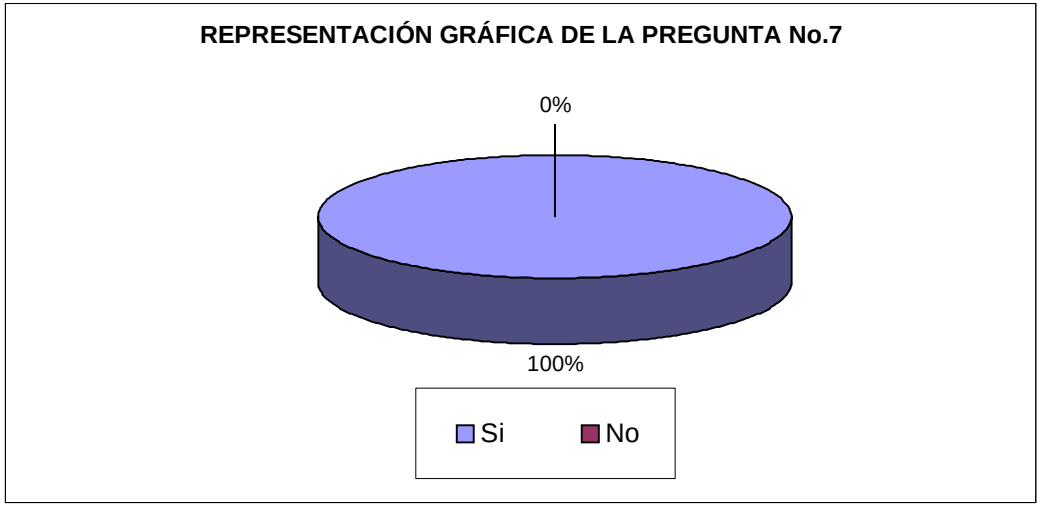
Pregunta No. 7 ¿Le gustaría implementar el control y captura de datos y visualizarlos de forma gráfica como software de monitoreo de ataques al sistema de seguridad?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones esta interezada en implementar un software de monitoreo y control de datos con visualización gráfica.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	15	100
No	0	0
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que todas las personas consultadas afirman que están interezadas en implementar un software de monitoreo y control en forma gráfica.



Pregunta No. 8 ¿Conoce usted el sistema de seguridad Honeynet con Vmware?

Objetivo: Investigar si la Dirección de Tecnología y Comunicaciones conoce el sistema de seguridad Honeynet con Vmware

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	1	7
No	14	93
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que la mayor parte de las personas consultadas afirman que no tienen conocimiento de la existencia de un sistema de seguridad.

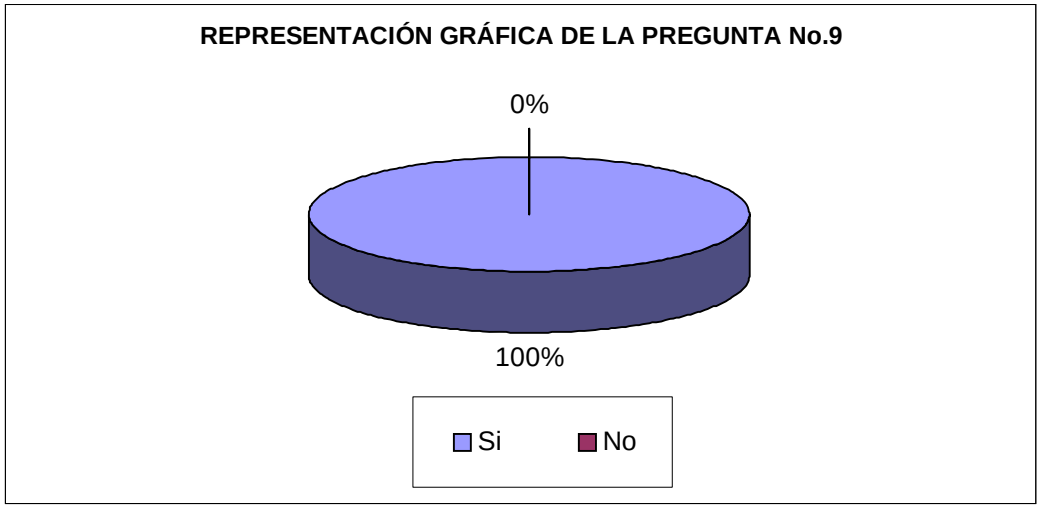
Pregunta No. 9 ¿Le gustaría conocer una propuesta de diseño de Honeynets Virtuales utilizando VMware, para detección de intrusos y ser implementado en su área?

Objetivo: Conocer si la Dirección de Tecnología y Comunicaciones esta interezada en la propuesta de diseño de Honeynets Vituales para la detección de intrusos informáticos.

Alternativas	TOTALES	
	FRECUENCIA	PORCENTAJE (%)
Si	15	100
No	0	0
TOTALES	15	100

Análisis:

De acuerdo al resultado obtenido se pudo determinar que todas las personas consultadas afirman que están interezadas en la propuesta de diseño de Honeynets Virtuales para la detección de intrusos informáticos.



Conclusiones y recomendaciones de la investigación de campo.

2.4.1 Conclusiones.

a. Se determinó que el 97% de los encuestados conocen el riesgo en que están expuestos los sistemas informáticos de la Universidad Francisco Gavidia.

b. El 87% de los empleados encuestados de la Dirección de Tecnología y Comunicaciones aseguran que falta más control de monitoreo periódico en los servicios que están instalados en los servidores y que desconocen con que periodicidad son expuestos ante un ataque informático.

c. El 47% de los empleados de la Dirección de Tecnología y Comunicaciones afirma desconocer si existe un sistema de seguridad y monitoreo en servidores públicos.

d. Se determinó que el 93% de los encuestados afirmó desconocer el sistema Honeynet Virtuales como herramientas de seguridad en los servidores.

e. Se determinó que el 100% de los encuestados están dispuestos en conocer e implementar un sistema de seguridad con herramientas gratuitas como lo es la Honeynet con Vmware

f. Se concluyó que la Dirección de Tecnología y Comunicaciones está 100% interesada en una propuesta de solución utilizando Honeynet Virtual con Vmware.

2.4.2 Recomendaciones.

Con fundamento en las conclusiones expuestas se considera necesario formular las siguientes recomendaciones.

a. Elaborar una propuesta de solución de Honeynet Virtuales utilizando vmware que permita el monitoreo y detección de intrusos informáticos.

b. Se recomienda a la Dirección de Tecnología y Comunicaciones adquirir nuevos conocimientos sobre seguridad informática y de las repercusiones legales que amparen la seguridad de la información de manera que se encuentren actualizados.

c. Aplicar la propuesta de Honeynet Virtuales utilizando vmware, para contar con un sistema de seguridad que permitirá que los servidores públicos en producción estén más seguros contra ataques informáticos

d. Contar con un sistema de seguridad como Honeynet Virtuales utilizando vmware, ya que permitirá garantizar la protección de la información de la Universidad.