FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE UN SISTEMA CRIPTOGRÁFICO A TRAVÉS DE ALGORITMOS AVANZADOS DE ENCRIPTACIÓN PARA MEJORAR LA SEGURIDAD PERIMETRAL DE UNA RED INFORMÁTICA

PARA OPTAR POR EL TÍTULO DE INGENIEROS DE SISTEMAS

AUTORES:

Guevara Tinoco Roberto Carlos

López López Willy Lleison

Pimentel, Febrero del 2016

“IMPLEMENTACIÓN DE UN SISTEMA CRIPTOGRÁFICO A TRAVÉS DE ALGORITMOS AVANZADOS DE ENCRIPTACIÓN PARA MEJORAR LA SEGURIDAD PERIMETRAL DE UNA RED INFORMÁTICA”

Aprobación de la Tesis

Guevara Tinoco Roberto Carlos
Autor

López López Willy Lleison
Autor

Mg. Ing. Christian Dios Castillo
Asesor Metodológico

Ing. Juan Elías Villegas Cubas
Asesor

Ing. Alex Coronado Navarro
Presidente

Ing. Carlos Rojas Ortiz
Secretario

Ing. Juan Elías Villegas Cubas
Vocal

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DEDICATORIA

A mi esposa Kelly, por estar siempre ahí brindándome su comprensión, paciencia, cariño y amor.

A mi hija Maritza Valentina quien es mi motivación de cada día para seguir adelante, para nunca rendirme en esta meta alcanzada y ser un ejemplo para ella.

A mi querido padre Severo, que en paz descanse, a mi madre Valentina porque son parte esencial de mi formación y quienes siempre estaban dándome aliento a seguir adelante en cumplir con mis metas.

A Dios fuente de amor y sabiduría, por haberme dado fuerzas en los momentos más difíciles y porque gracias a Él he logrado ser lo que soy.

Guevara Tinoco Roberto Carlos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DEDICATORIA

Dedico este proyecto de tesis a Dios, porque ha estado conmigo en cada paso que doy, cuidándome y dándome fortaleza para continuar y cumplir mis metas trazadas.

A mi esposa Nathaly Rivera Vega, por su amor, paciencia, comprensión, bondad, fuerza, y apoyo incondicional en todos los momentos que vivimos.

A mi hijo William Jesús López Rivera por darle sentido a mi vida, ser mi motivo para salir adelante siempre y ser tu ejemplo.

A mis padres, hermanas y tío Ricardo por confiar en mí y apoyarme incondicionalmente.

Es por ellos, que soy lo que soy ahora. Los amo con mi vida.

López López Willy Lleison

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

AGRADECIMIENTO

Un agradecimiento especial a la **Universidad Señor de Sipán**, a la plana docente por sus conocimientos y experiencias transmitidas durante el transcurso de toda mi vida universitaria, de igual forma a nuestros asesores y jurados de tesis, los cuales nos ayudan a ver nuestros errores y a pulir nuestras ideas.

Finalmente a mis compañeros de la Universidad, con quienes he compartido años de aprendizaje, mereciendo mi gratitud por su apoyo en los buenos y malos momentos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE DE CONTENIDO

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE DE FIGURAS

ÍNDICE DE DIAGRAMAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

RESUMEN

Históricamente, la autentificación de paquetes se ha manejado a través de firmas digitales basadas en certificados, usualmente emitidos por una entidad neutral a la comunicación y de confianza de todas las partes. Sin embargo, esta solución no siempre es posible de implementar, debido a factores como los costos, el tiempo limitado de vigencia de los certificados, la necesidad de depositar la confianza en un tercero, y por último el poder, usualmente limitado, de procesamiento de las máquinas.

El tema de esta tesis es desarrollar una alternativa de sistema de seguridad para la red informática. El sistema utiliza algoritmos avanzados para la encriptación y desencriptación de los paquetes de información enviados en la entidad de estudio para la protección de datos privados del usuario. El sistema debe poder extenderse para poder incorporar encriptación basada en más algoritmos de este tipo.

El desarrollo de este trabajo consiste en un estudio de las componentes a usar, tanto de hardware como de software, incluyendo los conceptos básicos necesarios para su diseño y operación, así como los estándares y metodologías que siguen.

Palabras Clave:

Sistema criptográfico, Algoritmos avanzados, Encriptación, Desencriptación, Seguridad perimetral.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ABSTRACT

Historically, the identification of packages has been handled via digital signatures based on certificates, usually issued by a neutral entity communication and confidence of all parties. However, this solution is not always possible to implement, due to factors such as cost, time-limited validity of certificates, the need for reliance on a third, and finally the power, usually limited, processing machines.

The subject of this thesis is to develop an alternative security system for the computer network. The system uses advanced algorithms for encryption and decryption of packets of information sent in the entity of study for the protection of user's private data. The system must be able to be extended to be able to incorporate encryption algorithms based on more of this type.

The development of this work is a study of the components to use, both hardware and software, including the basic concepts necessary for their design and operation, as well as the standards and methodologies that remain.

Key words:

Cryptographic system, advanced algorithms, encryption, decryption, perimeter security.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INTRODUCCIÓN

Hoy en día estamos ante una novedosa forma de comunicación en un entorno globalizado debido al desarrollo de la Internet. Por ello, se ha hecho indispensable el aumento de la infraestructura tecnológica dentro de las empresas, tanto en la red convencional como en la red inalámbrica. Sin embargo, muchas empresas no toman en cuenta que dicha infraestructura está en peligro por las vulnerabilidades que presenta, por lo que es necesario implementar un sistema de control de acceso a la red que permita proteger la información de posibles ataques de personas ajenas a ella mediante suplantación de identidad, lo cual podría provocar pérdidas financieras o espionaje corporativo.

Para evitarlo se cuenta con estándares, protocolos y equipos que permiten construir soluciones de seguridad robustas.

La presente tesis busca diseñar e implementar sistema criptográfico a través de algoritmos avanzados de encriptación que sea capaz de

mejorar la seguridad perimetral de la red informática del Instituto Superior Tecnológico ABACO utilizando la metodología CISCO.

El presente proyecto se conformó por seis (6) capítulos, cuyo contenido es brevemente descrito a continuación:

Capítulo I: Problema de la Investigación.

En este capítulo se explica el por qué se realizó la investigación planteando el problema, en donde se identificaron los objetivos generales y específicos, igualmente se delimita el alcance del estudio, así como también se justifica la realización de la investigación.

Capítulo II: Marco Teórico.

Aquí se explica los antecedentes que guardan relación con la investigación, las bases teóricas, el estado del arte y las bases legales sobre las cuales opera el sistema.

Capítulo III: Marco Metodológico.

Se describen el tipo y nivel de investigación los cuales caracterizan a este proyecto, así como también la población y muestra que fue objeto de estudio, las distintas técnicas utilizadas para la recolección de datos, las técnicas de análisis de los datos y además el diseño operativo utilizado.

Capítulo IV: Resultados.

Contiene a los resultados de la contratación de la hipótesis, así como también la descripción del cumplimiento de los indicadores y la discusión de resultados e interpretación de los mismos.

Capítulo V: Propuesta de la Investigación.

Aquí se muestran cada una de las actividades planteadas para el logro de los objetivos propuestos en la investigación, siguiendo la metodología de desarrollo de software RUP, así como el análisis de costo Beneficio del proyecto.

Capítulo VI: Conclusiones y Recomendaciones.

Contiene a las conclusiones y recomendaciones realizadas para el éxito de la investigación.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.1 Situación Problemática

1.1.1 Contexto Internacional

Pablo Ramos, coordinador del Laboratorio de ESET Latinoamérica, señala que el 50% del total de información que se filtra a nivel mundial corresponde a datos de empresas financieras.

En cuanto a seguridad informática, una de las tendencias más fuertes es el robo de información en el sector corporativo, afirmaron especialistas en el I Foro Regional de Seguridad Informática: Malware y Cibercrimen en América Latina, organizado por ESET.

“Según algunos registros, prácticamente el 50% de la información que se filtra en las empresas corresponden a empresas que se dedican a finanzas, entidades que tienen registros de compra, información de tarjetas de crédito y cuentas bancarias”, señaló Pablo Ramos, coordinador del Laboratorio de ESET Latinoamérica.

Durante el 2014, se registraron menos ataques que en los dos años anteriores (2012 representó un pico), pero se ha robado mucha más información.

Más allá de los ataques, es ver cuánta información recopilaron, por cuánto tiempo, de qué manera crecieron. Este año (los cibercriminales) fueron más eficientes. En solo seis meses, se

robaron 500 millones de registros de usuarios. Más no es siempre mejor, sostuvo Ramos.(Bárbara Salas , 2014).

Evitar el espionaje es el objetivo de muchas aplicaciones y servicios que surgen cada vez con más frecuencia, a pesar de que la falta de una curaduría de parte de expertos hace difícil saber cuál es infalible.

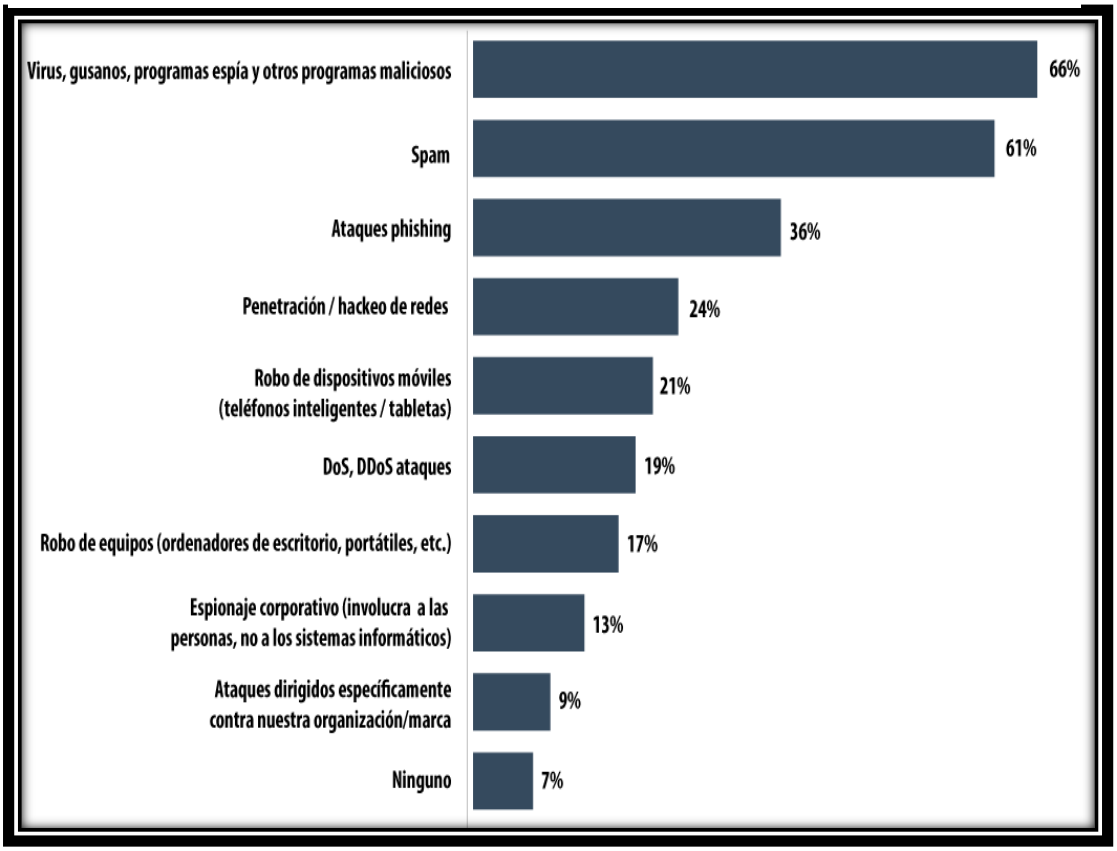
A muy poco estuvo el abogado y columnista del diario británico The Guardian, Glenn Greenwald, de perderse la primicia de su vida y todo por no tener un software de encriptación de datos. Cuando el ex funcionario de la Agencia de Seguridad Nacional (NSA) Edward Snowden decidió arriesgar su libertad al filtrar documentos secretos, eligió a Greenwald para que se encargue de publicarlos. Bajo el seudónimo de Cincinnatus, Snowden le pidió al periodista que instalara un programa que codifique los datos como condición necesaria para brindarle la información que escandalizó al mundo. (Cromo Uruguay, 2014).

En los dos últimos años la cantidad de ataques informáticos graves detectados ha crecido tanto, que cada nuevo ataque ya no suele causar sorpresa. Los informes de las compañías antivirus sobre el descubrimiento de una nueva botnet o un nuevo refinado ejemplar de malware que roba datos aparecen con regularidad.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Con cada vez más frecuencia las compañías comerciales se convierten en víctimas potenciales de los ataques informáticos. Según los resultados de una encuesta realizada por Kaspersky Lab y la compañía analítica B2B International, el 91% de las empresas encuestadas en todo el mundo fueron víctimas de por lo menos un ataque al año y el 9% de las compañías fueron víctimas de ataques selectivos.(Vitaly Kamluk, 2013)

Figura 1: Porcentajes de ataques



Fuente:(Vitaly Kamluk, 2013)

1.1.2 Contexto Nacional

A menudo, cuando escuchamos el término Criptografía nos viene a la mente la idea de algo complejo y quizá, por qué no decirlo, aburrido. En definitiva, nos evoca a algo sofisticado y seguro; pero a la vez, en muchas ocasiones, a algo complicado de entender.

Si buceamos en la red, veremos que el término Criptografía**,** cuyo nacimiento data de la Grecia Clásica, se traduce como “escritura oculta” y es que tenemos que considerar que desde el inicio de los tiempos han existido tensiones entre los creadores de sistemas y algoritmos criptográficos (criptógrafos) y sus destructores (cripto-analistas)

Desde esta época hasta nuestros días, con la irrupción de la informática y las comunicaciones electrónicas, la evolución del término y sus aplicaciones se han ampliado y perfeccionado enormemente, sobre todo durante los 10 últimos años, donde la criptografía se ha convertido en sinónimo de comunicaciones digitales seguras en los ámbitos gubernamentales, bancarios, industriales, etc. Por lo tanto, la tecnología criptográfica nació ante la necesidad de proteger la información en las comunicaciones sin que fuese interceptada por terceros.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En base a todo esto, tenemos que tener en cuenta que para que un sistema de seguridad informática sea de verdad seguro, valga la redundancia, debe estar basado en tecnología criptográfica. Puesto que la Criptografía es la única disciplina capaz de desarrollar robustos sistemas de seguridad informática.

Y en este ámbito de desarrollo del Gobierno Electrónico, la Criptografía juega un papel clave, puesto que permite a los ciudadanos llevar a cabo sus gestiones con las instituciones públicas de un modo rápido, eficiente y sin ningún tipo de riesgo de seguridad. Beneficios que, a su vez, son compartidos por las propias instituciones. (Realsec Peru, 2014).

El 67% de las instituciones financieras en Perú han experimentado incidentes de seguridad o privacidad en el último año, afirmó un estudio realizado por Deloitte. Con este resultado, Perú tiene el segundo más alto porcentaje en la región, ubicándose solo después de Colombia (100%). Por el otro lado, las naciones con menos entidades financieras afectadas por estos problemas son Guatemala (13%) y México (0%).

El reporte, realizado a 41 entidades de la industria financiera pertenecientes a siete países de la región, muestra que la seguridad de información se ha vuelto una prioridad para las empresas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Más del 50% de las instituciones encuestadas afirmaron que su presupuesto destinado para este rubro aumentó a medida que se van generando nuevos marcos regulatorios. (Comercio., 2014).

1.1.3 Contexto Local

Debido a razones de confidencialidad en esta investigación no se mencionara detalles de la red sobre la entidad en estudio.

1.2 Formulación del Problema

¿De qué manera se mejorará la seguridad perimetral de una red informática?

Objeto Estudio: Mejorar la seguridad perimetral de la red informática del instituto “ABACO”.

Campo de Acción: Instituto Superior Tecnológico Privado “ABACO”.

1.3 Delimitación de la investigación

La presente investigación se desarrollara utilizando algoritmos avanzados de encriptación, teniendo como base a los existentes tales como: DES, 3DE, AES. También HASH, HMAC, MDE5 protocolo RDA, DH, IKE para intercambiar llaves en Internet de forma segura. Utilizando HA y ESP para la confiabilidad,

integridad y autentificación, y con failover en la red perimetral. También se utilizara la metodología CISCO para definir las actividades necesarias en cada fase del ciclo de vida de la red y ayudar a asegurar el continuo funcionamiento de los servicios informáticos.

1.4 Justificación e importancia de la Investigación

La propuesta de esta investigación tubo por finalidad ayudar y promover el desarrollo en los siguientes aspectos:

1.4.1 Impacto Social

La sociedad se verá beneficiada de la siguiente manera:

1. Planteamiento de un modelo académicamente elaborado de sistema criptográfico a través de algoritmos avanzados de encriptación basado en nuestra realidad regional, que puede ser replicado en otras instituciones del mismo rubro o incluso adaptarlo para su desarrollo en otros campos.
2. Aprovechamiento de las tecnologías informáticas para fortalecer la toma de decisiones en la planificación de la seguridad.

1.4.2 Impacto Económico

La presente investigación permitió tener una significante reducción en los recursos utilizados como: costos de mantenimiento, costos de energía y de equipos de cómputo en cuanto a la mejora de la red perimetral con la implementación de la misma.

1.4.3 Impacto Tecnológico

En estos tiempos el uso de la tecnología a nivel mundial es casi inevitable, la presente investigación se usarán teorías relacionadas con un sistema criptográfico a través de algoritmos avanzados de encriptación: Metodología Cisco (Cisco, 2013) y la seguridad perimetral de una red informática: Defensa en profundidad (Microsoft, 2015).

1.4.4 Impacto Académico

La presente investigación permitió hacer uso de todos los conocimientos obtenidos en mi formación como profesional, ahondar con profundidad en la información sobre la problemática y la posible solución; demostrando así a la sociedad en general las capacidades y competencias de los futuros egresados de la Escuela de Ingeniería de Sistemas de la Universidad Señor de Sipán.

1.5 Limitaciones de la Investigación

El desarrollo del presente proyecto tuvo limitaciones propias de una investigación de Pregrado Universitario como es el tiempo académico para el desarrollo total del producto, además de recursos económicos que se requiere en el proceso de desarrollo de la investigación.

1.6 Objetivos de la Investigación

1.6.1 Objetivo General

Implementar un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática.

1.6.2 Objetivos Específicos

a) Diagnosticar el estado actual de la seguridad perimetral de una red informática.

b) Identificar los factores influyentes en la seguridad perimetral de una red informática.

c) Diseñar un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática.

d) Estimar los resultados que generará la implantación un sistema criptográfico a través de algoritmos avanzados de encriptación en la seguridad perimetral de una red informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO II: MARCO TEÓRICO

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.1 Antecedentes de Estudios

2.1.1 A nivel Internacional

Según (Jose Baltazar, 2011) en su tesis titulada “Diseño e Implementación de un esquema de seguridad perimetral para redes de datos caso práctico: dirección general del colegio de ciencias y humanidades“. Cuyo objetivo es diseñar un esquema de seguridad perimetral para la Dirección General del Colegio de Ciencias y Humanidades, que permita minimizar los riesgos contra los ataques más frecuentes. Los resultados obtenidos fueron implementar el primer esquema de seguridad de red perimetral para la institución, esperando que las perspectivas de seguridad plasmadas en este documento presente al lector la importancia de la seguridad de la información, procedimientos, buenas prácticas y mecanismos que permitan llevar a cabo un ciclo de mejora continua. La tesis concluye en que para garantizar la seguridad de la información dentro de la institución, no sólo se requiere de la implementación de los diferentes mecanismos de control, ya que no serán suficientes si no se cuenta con el personal adecuado que garantice su operación.

Como responsables de seguridad siempre debemos considerar la capacitación constante, que nos permita responder a futuros incidentes.

Según (Soto, 2010) en su tesis titulada “Algoritmos de encriptación simétricos que procesa bloques de 192 bits, con llaves de cifrado de 192 bits, empleando los teoremas factorial y JV“. Cuyo objetivo es diseñar e implementar en software un algoritmo de encriptación simétrico que procese bloques de 192 bits, utilizando llaves de cifrado de 192 bits empleando los teoremas factorial y JV con objeto de operar números del orden de los 10 en la construcción de permutaciones variables en lugar de números de orden 10 y así reducir el número de operaciones de computo buscando aumentar la seguridad en el cifrado de datos. Los resultados obtenidos fueron lograr cifrar y descifrar mensajes mezclando la información con tres operaciones básicas: operaciones XOR, permutaciones variables usando los teoremas JV y factorial así como sustituciones no lineales haciendo uso de la caja-S del propio algoritmo AES. La tesis recomienda realizar una implementación de este algoritmo utilizando programación paralela para reducir aun mes el número de operaciones bit que se llevan a cabo de manera secuencial.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.1.2 A nivel Nacional

Según (Katia, 2005), en su tesis titulada “Encriptación RSA de archivos de texto” en este trabajo se presentará el método desarrollado en 1978 por R. L. Rivest, A. Shamir y L. Adleman y que es conocido como sistema criptográfico RSA por las iniciales de sus autores. Basa su seguridad en la dificultad de factorizar números primos muy grandes aunque como todo sistema de encriptación de clave pública, el RSA puede estar sujeto a ataques con el fin de obtener el mensaje original o descubrir la clave privada.

(Valenzuela, 2012) En su tesis titulada “Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña“. En el trabajo realizado se presenta una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. Se muestra además una simulación del diseño propuesto en un ambiente de pruebas controlado.

2.2 Estado de Arte

2.2.1 En Cuanto a la integración de Algoritmos Criptográficos:

En el en el artículo de (Cabrera Aldaya & Cabrera Sarmiento, 2014) titulado “Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA”, señala que debido al creciente aumento de la complejidad de los sistemas empotrados y la posibilidad de comunicación a través de redes de comunicaciones, la seguridad de las mismas se convierte en un aspecto a tener en cuenta y en donde entran a jugar protocolos criptográficos que solamente habían sido utilizados en sistemas basados en dispositivos de computo tradicionales, como computadoras personales, servidores, etc. con capacidades de procesamiento muy superiores a las que se pueden desarrollar en un sistema empotrado. Esto conlleva a la implementación de estos algoritmos en arquitecturas no convencionales y con diferentes potencialidades, por ejemplo, tanto en micro controladores de 8 bits basados en arquitectura 8051 de Intel, como en sistemas empotrados basados en el procesador Micro-Blaze de Xilinx, haciendo esta tarea no homogénea y dependiente de la arquitectura y de los recursos del sistema de procesamiento.

Un aspecto muy importante a tener en cuenta en la implementación de algoritmos criptográficos es la cantidad de recursos de cómputo que puede ser necesario destinar a la ejecución de los mismos, los cuales en algunos casos no son despreciables. Esto da lugar a que sea necesario acelerar mediante hardware dedicado la ejecución de aquellos algoritmos cuyo tiempo de procesamiento es considerable en un procesador empotrado, permitiendo así reducir la carga del procesador y con ello destinar sus recursos a la ejecución de las aplicaciones principales del sistema. Por ejemplo, en sistemas empotrados donde sea necesario garantizar la seguridad de la comunicación entre diferentes dispositivos conectados a través de una red TCP/IP, es necesario implementar algoritmos criptográficos.

Esta tarea no es la principal que debe llevar a cabo este sistema, por lo que la cantidad de tiempo de procesamiento utilizada por la misma debe ser reducida para asegurar que las aplicaciones principales del sistema tengan a su disposición la mayor capacidad de cómputo posible, situación que conlleva a la necesidad de la implementación hardware de los algoritmos criptográficos.

En este trabajo se implementaron algoritmos criptográficos utilizando la lógica reconfigurable de los FPGA de Xilinx para luego ser integrados en un sistema empotrado donde el procesador Micro-Blaze es la unidad central de procesamiento. El objetivo de esta

integración fue evaluar el impacto de la aceleración de estos algoritmos durante su utilización en protocolos seguros de comunicaciones basados en TCP/IP. Adicionalmente se dio la integración de implementaciones hardware de algoritmos criptográficos a la biblioteca Open-SSL la cual es utilizada por aplicaciones sobre el sistema operativo Linux para asegurar redes TCP/IP.

Los algoritmos implementados fueron el AES y las funciones resumen SHA-1 y SHA-256. Estos algoritmos son implementados como coprocesadores del procesador Micro-Blaze utilizando interfaces FSL para el intercambio de datos entre ellos. Estos coprocesadores son integrados dentro de la biblioteca Open-SSL considerando la naturaleza multitarea del sistema operativo Linux, por lo que se selecciona un mecanismo de sincronización para controlar el acceso a estos dispositivos.

Esta investigación permitió determinar que el coprocesador AES consume pocos recursos del FPGA, lo que permite su utilización en sistemas empotrados basados en FPGA de bajo y mediano coste, que los coprocesadores de las funciones resumen SHA-1 y SHA-256 poseen un consumo de recursos mayor en comparación con el del algoritmo AES, pero aun así pueden ser considerados apropiados para ser incluidos en sistemas empotrados en FPGA de

bajo a mediano costo y que es posible aumentar la seguridad, utilizando algoritmos avanzados sin comprometer el rendimiento del sistema.

2.2.2 En cuanto a Seguridad Perimetral de una Red

Según (Check Point, en la seguridad perimetral de RBA, 2014), esta quiere adaptarse a los tiempos que corren, en los que las nuevas tecnologías como Internet han transformado los modelos de negocio, y por ello ha decidido transformar su infraestructura de seguridad.

Para esto abordaron dos aspectos clave en su proyecto, de una parte, mejorar el rendimiento, ya que su negocio depende mucho de Internet y es fundamental para ellos dar un buen servicio tanto a nivel de transferencia de contenidos con colaboradores y clientes, como en el uso interno del propio personal, en segundo lugar, era primordial saber qué estaba pasando en su red en todo momento, esto es, de una amplia capacidad de análisis, algo que la soluciones anteriores no cubrían.

A la hora de concebir el proyecto, RBC quería una plataforma homogénea, segura, con un rendimiento óptimo, fácilmente gestionable y con capacidades de reporting. Además, confío las tareas de análisis, diseño e implementación necesarias a Dimension Data.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

La implantación consistió en 2 appliances de nueva generación 4800 en la sede central en Barcelona (acompañado de la protección completa del software blade Threat Prevention), el appliance 2200 para la sede en Madrid con los mismos complementos y 4 equipos 1140 con Threat Prevention y WiFi en las delegaciones pequeñas, más la consola de gestión Smart Event.

RBA ha logrado dar un salto cualitativo a nivel tecnológico en su infraestructura, reducir los riesgos de las comunicaciones tanto internas como externas y lograr una gestión mejorada y simplificada para su departamento TI. “La nueva plataforma de Check Point aumenta la seguridad perimetral, y además goza de una gestión interna más sencilla, lo que ofrece un excelente control de la red. Ahora tienen una visibilidad completa y en tiempo real del tráfico de nuestros datos, lo podemos analizar de forma muy sencilla y ahorramos, por ejemplo, muchísimo tiempo en la resolución de incidencias.

Actualmente, tras la implantación de las soluciones de Check Point, cada firewall central gestiona unas 5000 conexiones concurrentes en momentos puntuales del día y un through put aproximado de 100 Mb por segundo. Por otra parte, el tiempo en la resolución de incidencias por parte del departamento TI ha descendido drásticamente.

Desde el punto de vista técnico, gracias al feed back y a las herramientas de reporting ahora se tiene un control excelente del uso de recursos.

Los appliances Check Point (4800, 2200 y 1140), piezas angulares de esta implantación, son dispositivos indicados para empresas con escenarios de servicio muy exigentes y que requieren appliances con más puertos y mayor rendimiento. Ofrecen alta disponibilidad, balanceo de carga, enrutamiento dinámico, así como aceleración a velocidades multi-gigabit para bloquear las amenazas a nivel de aplicación.

2.3 Base Teórico Científicas

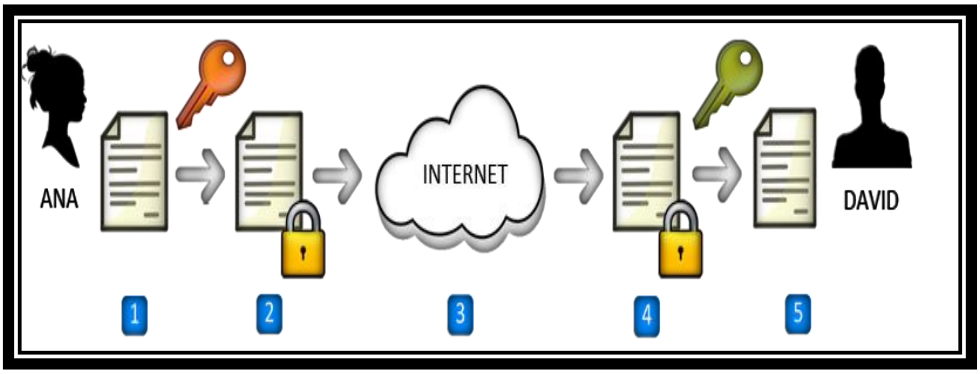
El uso de nuevas tecnologías hoy en día es muy frecuente, en especial en los procesos de que involucra la protección de una red de datos; ya que ello permite garantizar la protección de la información que se maneja dentro de la entidad que la utiliza.

2.3.1 Criptografía

Según (Meavilla, 2009), señala que la criptografía es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados (en griego kriptos significa secreto y gráphos, escritura).

La criptografía es una disciplina muy antigua, sus orígenes se remontan al nacimiento de nuestra civilización. En origen, su único objetivo era el proteger la confidencialidad de informaciones militares y políticas. Sin embargo, en la actualidad es una ciencia interesante no sólo en esos campos, sino para cualquier otro que esté interesado en la confidencialidad de unos determinados datos.

Figura 2: Criptografía Asimétrica



Fuente:(Criptografía asimétrica, 2013)

2.3.2 Encriptación de Datos

Según (Ramió, 2009), la encriptación corresponde a una tecnología que permite la transmisión segura de información, al codificar los datos transmitidos usando una fórmula matemática que "desmenuza" los datos. Asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos.

La encriptación de datos funciona utilizando la criptografía. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o enviada a través de una red insegura (como Internet) y aun así permanecer secreta.

Luego, los datos pueden desencriptarse a su formato original para lo cual utilizan un algoritmo criptográfico, usado en los procesos de encriptación y desencriptación. Un algoritmo criptográfico trabaja en combinación con una llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos. Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada llave posible.

El resultado de este cálculo son los datos encriptados. Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados.

La mayoría de los algoritmos modernos del cifrado se basan en una de las siguientes dos categorías de procesos:

a) Problemas matemáticos que son simples pero que tienen una inversa que se cree (pero no se prueba) que es complicada
b) Secuencias o permutaciones que son en parte definidos por los datos de entradas.

Consultoría de Seguridad y Gestión del Riesgo

Dentro de esta línea están los servicios de consultoría dedicados a la definición de planes directores de seguridad, políticas y planes de seguridad preventiva y planes de contingencia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Arquitecturas de Seguridad

Línea dedicada al diseño e integración de soluciones corporativas de seguridad perimetral, de infraestructuras y de sistemas. Entre otras soluciones, en esta línea se encuentran las plataformas de seguridad perimetral (cortafuegos, redes privadas virtuales, etc.), de contenidos, de detección y prevención de intrusiones, de análisis y gestión de vulnerabilidades.

Certificación y Firma Electrónica

Esta línea de nuestra oferta se ocupa del despliegue de Infraestructuras de Certificación (PKI) corporativas, desde la definición de Políticas y Prácticas de Certificación hasta el despliegue de servicios avanzados como el Sellado de Tiempo o la Validación. Se incluyen los trabajos de integración de las Tecnologías de Certificación (firma, cifrado, autenticación) en los Sistemas de Información.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Gestión de Identidades

Son sistemas de gestión de seguridad corporativa efectivos y alineados con la realidad del negocio. Entre las soluciones de gestión de identidades se pueden destacar los sistemas de gestión de información de seguridad y control de fraude, los Directorios.

La encriptación de datos se basa en métodos llamados Métodos de encriptación:

Para poder Encriptar un dato, se pueden utilizar procesos matemáticos diferentes:

a) **Algoritmo HASH:** Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC. es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor. se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo. Entre los algoritmos de hash más comunes están:SHA-1: algoritmo de hash seguro. Algoritmo de síntesis que genera un hash de 60 bits. Se utiliza, por ejemplo, como algoritmo para la firma digital. MD2 está optimizado para computadoras de 8 bits. El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el ordenador (128 bits o 16 bytes) y añadiéndole un checksum. Para el cálculo real, se utiliza un bloque auxiliar 48 bytes y una tabla de 256 bytes que contiene dígitos al azar del número pi.

b) MD4: Es un algoritmo de resumen del mensaje (el cuarto en la serie) diseñado por el profesor Ronald Rivest del MIT. Implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes. La longitud del resumen es de 128 bits.

c) MD5: Utiliza el esquema de hash de hash de 128 bits muy utilizado para autenticación cifrada. Gracias al MD5 se consigue, por ejemplo, que un usuario demuestre que conoce una contraseña sin necesidad de enviar la contraseña a través de la red.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Algoritmos Simétricos: Utilizan una clave con la cual se encriptan y desencriptan el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. En este modelo, el mensaje original es convertido en un mensaje cifrado que aparentemente es aleatorio y sin sentido. El proceso de encriptación está formado por dos componentes, un algoritmo y una clave. La clave es un valor que es independiente del texto o mensaje a cifrar.

El algoritmo va a producir una salida diferente para el mismo texto de entrada dependiendo de la clave utilizada. Una vez cifrado, el mensaje puede ser transmitido. El mensaje original puede ser recuperado a través de un algoritmo de desencriptación y la clave usada para la encriptación.

Algoritmos Asimétricos (RSA): Requieren dos Claves, una Privada, única y personal, solo conocida por su dueño y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Los pasos del proceso de encriptación con clave pública son los siguientes:

1) Cada sistema genera un par de claves para ser usadas en la encriptación y desencriptación de los mensajes que envíen y reciban.
2) Cada sistema publica su clave de encriptación (clave pública). La clave de desencriptación relacionada (clave privada) se mantiene en privado.
3) Si Alice desea enviar un mensaje a Bob, encripta el mensaje utilizando la clave pública de Bob.
4) Cuando Bob recibe un mensaje lo desencripta usando su clave privada. Nadie puede desencriptar el mensaje porque solo Bob conoce su clave privada.

Algoritmo de encriptación RC4: Es un algoritmo de Cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 usando remailers anónimos en un grupo de news: sci.crypt. Es usado por diversos programas comerciales como Netscape y Lotus Notes.

Firma Digital:

La firma digital permite garantizar algunos conceptos de seguridad que son importantes al utilizar documentos en formato digital, tales como Identidad o autenticidad, integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas.

Ventajas Ofrecidas por la Firma Digital

a) Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, el receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.

b) Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.

c) No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Diferencias hay entre los algoritmos simétricos y los asimétricos

Los algoritmos simétricos encriptan y desencriptan con la misma llave. Las principales ventajas de los algoritmos simétricos son su seguridad y su velocidad. Los algoritmos asimétricos encriptan y desencriptan con diferentes llaves. Los datos se encriptan con una llave pública y se desencriptan con una privada, siendo ésta su principal ventaja.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Los algoritmos asimétricos, también conocidos como algoritmos de llave pública, necesitan al menos una llave de 3.000 bits para alcanzar un nivel de seguridad similar al de uno simétrico de 128 bits. Y son increíblemente lentos, tanto que no pueden ser utilizados para encriptar grandes cantidades de información.

Los algoritmos simétricos son aproximadamente 1.000 veces más rápidos que los asimétricos.

Otros

El protocolo SSL, protege los datos transferidos mediante conexión http, es decir navegación web, utilizando encriptación provista por un Servidor Web de Seguridad. Una llave pública es empleada para encriptar los datos, y una llave privada se utiliza para descifrar o desencriptar la información.

Crypto Forge le proporciona cuatro robustos algoritmos de encriptación para proteger sus datos:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

a) Blowfish (llave de 448 bits) es un algoritmo de encriptación rápido y fuerte. Su creador es Bruce Schneier, uno de los más prestigiosos criptógrafos en el mundo.

b) Rijndael (llave de 256 bits) es un algoritmo seguro y eficiente. Sus creadores son Joan Daemen y Vincent Rijmen (Bélgica). Ha sido elegido como el nuevo Estándar Avanzado de Encriptación (AES) por el Instituto Nacional de Estándares y Tecnología (NIST) de los EEUU.

c) Triple DES (llave de 168 bits) es un algoritmo desarrollado por el gobierno de EEUU y ha sido evaluado durante años sin descubrírsele debilidades. Es una configuración de encriptación en la cual el algoritmo DES es usado tres veces con tres llaves diferentes.

d) Gost (llave de 256 bits) es un algoritmo de Rusia y podría ser considerado el análogo ruso al DES. Tiene un diseño conservador y no ha podido ser vulnerado, a pesar de haber sido uno de los más estudiados, durante años, por los mejores expertos en criptoanálisis.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

La importancia de tener nuestros datos a salvo de miradas extrañas o tener un mínimo de privacidad se ha convertido en un tema muy importante. Los PDAs son muchas veces usados como pequeñas oficinas portátiles donde se guardan datos de gran valor y donde es de gran importancia tener estos datos protegidos.

Muchos usuarios de PDAs por comodidad no protegen el acceso de inicio con una clave, imagínense en caso de pérdida del aparato o descuido poder dejar estos datos confidenciales en manos ajenas a las nuestras. Para solucionar este problema o tener un cierto grado de seguridad, es muy importante poder encriptar nuestros datos.

Cifrado

Según (Hernández Orallo, 2013), el cifrado es el proceso por el que un texto es transformado en otro texto cifrado usando una función matemática (también denominado algoritmo de encriptación) y una clave.

El cifrado es necesario entre otras funciones para:

1. Proteger la información almacenada en un ordenador
2. Proteger la información transmitida desde un ordenador a otro.
3. Asegurar la integridad de un fichero.

El cifrado también tiene sus límites ya que no puede prevenir el borrado de información, el acceso al documento antes de su cifrado, por lo que un plan de seguridad no se puede basar simplemente en el cifrado de la información.

No todas las formas de cifrado tienen la misma seguridad. Hay cifrados muy simples que son fáciles de romper (se denomina romper un cifrado a la obtención del mensaje cifrado o la clave) y otros muchos más complejos que requieren de técnicas muy complejas para su descifrado.

Hay que comentar que no existen mecanismos de cifrado totalmente seguros, ya que con un ordenador lo suficientemente potente, o muchos a la vez y el tiempo necesario siempre será posible romper el cifrado. Por lo tanto, el objetivo de la criptografía es obtener mecanismos de cifrado que sean lo suficientemente complejos para evitar su descifrado usando la tecnología actual.

Hay dos tipos básicos de algoritmos de encriptación:

Clave secreta o clave simétrica: utiliza la misma clave para cifrar y descifrar un mensaje. Estos métodos de cifrado se usan principalmente para proteger información que se almacena en un disco duro o para transmisión de datos entre ordenadores. El algoritmo de encriptación más usado de este tipo es el DES (Data Encryption Standard) que usa una clave de 56-bits. Un mensaje cifrado con este algoritmo es bastante seguro aunque ya puede ser descifrado con máquinas muy potentes en menos de un día, por lo que su uso está restringido a ámbitos civiles. Otros algoritmos comúnmente usados son el RC2, RC4, RC5 e IDEA. La mayoría de estos algoritmos tienen patente, aunque su uso público está permitido.

Clave pública (o clave asimétrica): que utiliza una clave pública para cifrar el mensaje y una clave privada para descifrarlo De esta forma cualquiera puede cifrar un mensaje pero solo quien tenga la clave privada puede descifrarlo. Esto sirve para poder enviar un mensaje a un determinado destino sin que otro pueda descifrarlo. El objeto de estos métodos es la de asegurar la integridad y la autentificación del origen de los datos, por ejemplo, usando firmas digitales. RSA es el algoritmo de encriptación más conocido de clave pública. RSA utiliza una clave pública que es

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

usada para cifrar el mensaje y una clave privada que es usada para descifrar el mensaje.

Estos dos métodos de encriptación funcionan mu-chas veces conjuntamente. Por ejemplo, el protocolo SSL que se utiliza como conexión segura en Internet (el que usa el navegador cuando está en modo seguro y en la URL nos sale https), utiliza primero una clave pública para enviar de forma cifrada la clave secreta DES que posteriormente utilizarán en la comunicación.

De esta forma la clave DES utilizada sólo la podrá descifrar el destino. Este método en general se denomina OTP (*One Time Password*) ya que para cada sesión se genera un nueva clave DES.

2.3.3 Seguridad Perimetral

Según (García Felipe, 2010), la seguridad perimetral es un método de defensa de red, que se basa en el establecimiento de recursos de seguridad en el perímetro de la red y a diferentes niveles, permitiendo definir niveles de confianza, el acceso de usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de suportación (auto soportados, soportados, enterrados, detección visual, etc.).

También cabe destacar la clasificación dependiendo del medio de detección. En esta se clasificarían en:

a) **Sistemas Perimetrales Abiertos:** Los que dependen de las condiciones ambientales para detectar. Como ejemplo de estos son la video vigilancia, las barreras infrarrojas, las barreras de microondas. Esta característica provoca falsas alarmas o falta de sensibilidad en condiciones ambientales adversas.

b) **Sistemas Perimetrales Cerrados:** Los que no dependen del medio ambiente y controlan exclusivamente el parámetro de control. Como ejemplo de estos son los antiguos cables microfónicos, la fibra óptica y los piezasensores. Este tipo de sensores suelen ser de un coste más elevado.

Su aplicación destaca principalmente en Seguridad Nacional (instalaciones militares y gubernamentales, fronteras, aeropuertos,

etc.) e instalaciones privadas de alto riesgo (centrales nucleares, sedes corporativas, residencias VIP, etc.).

Objetivos de la seguridad perimetral.

a) Rechazar conexiones a servicios comprometidos.
b) Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico) o entre ciertos nodos.
c) Proporcionar un único punto de interconexión con el exterior.
d) Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet.
e) Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
f) Auditar el tráfico entre el exterior y el interior.
g) Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

Perímetro de la red.

Se conoce como perímetro de la red a la “frontera” entre el exterior y las computadoras y servidores internas. Este se forma por los equipos que brindan conexión a Internet a las computadoras de la red, así como aquellos que las protegen de accesos externos.

Equipos como los gateways, proxys y firewalls forman parte de este perímetro.

Contar con protección antivirus a este nivel es importante dado que brinda una capa adicional de protección a las que nombramos en series anteriores, protegiendo a nivel de servidores varias de las entradas más comunes de los virus informáticos, antes de que puedan ingresar en la red interna.

2.3.4 Metodología de Desarrollo CISCO

Según (METODOLOGÍA DEL DESARROLLO CON CISCO, 2014), Cisco, el mayor fabricante de equipos de red, describe las múltiples fases por las una red atraviesa utilizando el llamado ciclo de vida de redes PDIOO (Planificación –Diseño –Implementación –Operación –Optimización).

a) **Fase de planificación**: Los requerimientos detallados de red son identificados y la red existente es revisada.

b) **Fase de diseño:** La red es diseñada de acuerdo a los requerimientos iniciales y datos adicionales recogidos durante el análisis de la red existente. El diseño es refinado con el cliente.

c) **Fase de implementación:** La red es construida de acuerdo al diseño aprobado

d) **Fase de operación:** La red es puesta en operación y es monitoreada. Esta fase es la prueba máxima del diseño.

e) **Fase de optimización:** Durante esta fase, los errores son detectados y corregidos, sea antes que los problemas surjan o, si no se encuentran problemas, después de que ocurra una falla. Si existen demasiados problemas, puede ser necesario rediseñar la red.

FASE I:

Se presenta una descripción de las problemáticas bien detalladas y la propuesta del grupo de proyecto sobre cómo pueden trabajar contra la problemática por la que va pasando la empresa.

FASE II:

a) Se comienzan a recopilar todos los requerimientos de la empresa.

b) Se hace el subneteo.

c) Se asignan los Ip's para las computadoras de la empresa.

FASE III:

a) Se hace el diseño físico de la red

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

b) Configuración de las VLAN'S y asignación de puertos a las VLAN'S.

c) Configuración de los servidores.

d) Modelo de red: Basado en servidor.

e) Configuración de los clientes de la red.

f) Distribución del cableado.

FASE IV:

a) Diseño físico y lógico de la red. Representado en el simulador Packet Trace.

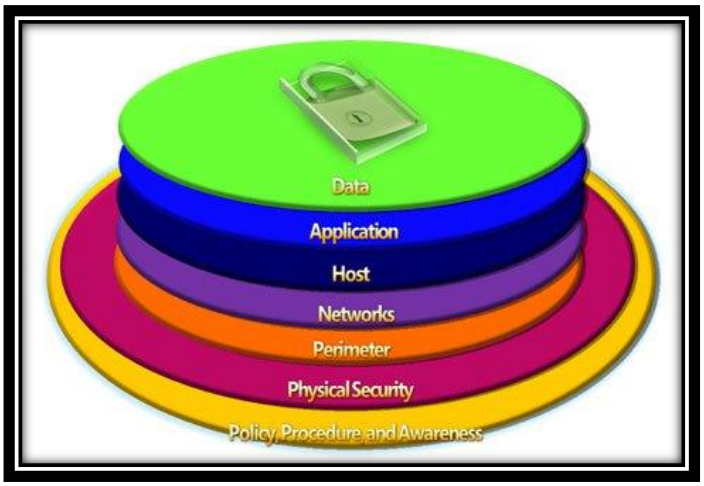
b) Diseño de la red LAN y VLAN.

2.3.5 Metodología de defensa en profundidad de Microsoft

Según (Microsoft, 2015) Este concepto de defensa en niveles enseña principalmente que la seguridad es un aspecto transversal, que abarca desde la información misma (los datos) hasta las dependencias físicas donde se encuentra la información, pasando por un conjunto de capas sucesivas y relacionadas. Pero quizá lo más destacable del modelo de defensa en profundidad es que todas estas capas están rodeadas por el aspecto humano: una solución de seguridad que no tenga considerado el aprendizaje del tema por parte de los usuarios está condenado al fracaso.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 3: Descripción del Modelo Defensa en profundidad de Microsoft



Fuente: (Microsoft, 2015)

Descripción del modelo de defensa en profundidad:

Capa 1: Políticas, Procedimientos y Conciencia

Establecer algunas políticas y prácticas escritas de seguridad, como una Política de uso aceptable de una compañía.

Capa 2: Seguridad física

Es una capa donde debemos de tener en cuenta a cosas como vigilancia por video IP y candados magnéticos y doble puerta de seguridad, etc.

Capa 3: Seguridad del perímetro

Se recomienda implementar servidores de seguridad, sistemas de cuarentena en VPN.

Capa 4: Seguridad de la red

Una de las mejores maneras de hacer esto es utilizar una tecnología conocida como IPSec. IPSec es simplemente un mecanismo que permite al sistema operativo una seguridad mediante un canal cifrado. Básicamente, IPSec tiene dos modos: Modo transporte, utilizado para conexiones de extremo a extremo y Modo túnel, utilizado para conexiones portal a portal. Al utilizar IPSec, podemos garantizar que sólo computadoras específicas, que utilicen la misma clave de cifrado, puedan conectarse entre sí.

Capa 5: Seguridad del host

Aquí se pueden realizar acciones como emplear un refuerzo del sistema operativo, autenticaciones, etc.

Capa 6: Seguridad de las aplicaciones

Se puede realizar refuerzo de la seguridad de las aplicaciones, antivirus, etc.

Capa 7: Seguridad de los datos

Se recomienda el uso de listas de control de acceso, texto cifrado, etc.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.3.6 Administración de Proyectos

Según(Reyes & Reyes, 2007), un proyecto es una serie de actividades y tareas con un objetivo específico, iniciando y terminando fechas y recursos. Los recursos consumidos por el proyecto incluyen el tiempo, dinero, personal y equipo. La administración del proyecto incluye:

a) Las metas específicas y objetivos
b) Al desempeño deseado o nivel de tecnología
c) Restricciones de tiempo y costo
d) Recursos dispuestos

Los elementos de un proyecto de administración son:

a) Planeación: Aquí se decide qué hacer
b) Programación: Aquí se decide cuándo hacerlo
c) Control: Aquí se asegura que los resultados deseados sean obtenidos.

La administración de proyectos es aplicable a proyectos que abarca el diámetro de tareas simples en un ambiente estático a tareas complejas en un ambiente dinámico.

Los beneficios de la administración de un proyecto incluyen:

1) Identificación de tiempos límites para programación.
2) Disposición de responsabilidades de función para asegurar que todas las actividades están contabilizadas.
3) Selección de una metodología para el análisis.
4) Minimizar la necesidad de reporte continuo.
5) Medición de cumplimiento contra planes.
6) Identificación temprana de problemas.
7) Saber cuándo los objetivos no pueden ser cumplidos o serán excesivos.
8) Capacidad estimada mejorada para planeación futura.

Los proyectos son administrados en las siguientes cuatro categorías:

a) Justificación del proyecto y técnicas de prioridad.
b) Planeación y estimación del proyecto.
c) Monitoreo y medición de la actividad del proyecto.
d) Documentación del proyecto y procedimientos relacionados.

Técnicas de priorización y justificación del proyecto:

Análisis costo – beneficio

a) Retorno de inversión (ROI por sus siglas en inglés)

b) Retorno en activos (ROA por sus siglas en inglés)

c) Valor presente neto (VPN por sus siglas en inglés)

d) Tasa interna de retorno (TIR por sus siglas en inglés)

e) Periodo de pago.

Análisis de decisión y análisis de portafolio aplicados como a las decisiones del proyecto.

2.3.6.1 Análisis costo – beneficio

El análisis del proyecto costo – beneficio es una comparación para determinar si el proyecto vale o valdrá la pena. El análisis es ejecutado antes de la implementación de los planes del proyecto y está basado en tiempos estimados de costos y valores estimados de beneficios. El análisis costo – beneficio es utilizado como una herramienta administrativa para determinar si se debe aprobar el proyecto para su implementación.

La secuencia para ejecutar un análisis de costo – beneficio es:

a) Identificar los beneficios del proyecto.

b) Expresar los beneficios en monto monetario, de tiempo y de duración.

c) Identificar los factores de costo del proyecto incluyendo materiales, mano de obra y recursos.

d) Estimar los factores de costo en términos de monto monetario y periodo de gastos.

e) Decida si el proyecto debería ser implementado, antes de empezar, o si el proyecto fue benéfico, después de completarlo.

A continuación se detallan cada una de las ecuaciones planteadas para hacer los diferentes cálculos del Costo Beneficio:

Retorno en activos (ROA)

Johnson (1982) da una ecuación para el retorno en activos:

Formula 1: Para Calcular ROA

$$ROA = \frac{Ingresoneto}{Totaldeactivos}$$

Dónde: el ingreso neto para un proyecto es igual a las ganancias esperadas y el total de activos es el valor de los activos aplicados al proyecto.

Retorno de la inversión (ROI)

Formula 2: Para calcular ROI

$$\text{ROI} = \frac{Ingresoneto}{Inversión}$$

Donde el ingreso neto para un proyecto es igual a las ganancias esperadas y la inversión es el valor de la inversión en el proyecto. Existen varios métodos utilizados para evaluar un proyecto basado en el monto de efectivo y periodos de tiempo. Existen tres métodos comunes: valor presente neto (NPV), tasa interna de retorno (IRR), y los métodos de periodo de pago.

Método del valor presente neto (VPN)

Johnson (1982) da una ecuación para el valor presente neto (VPN)

Formula 3: Para calcular VPN

$$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t}$$

Dónde:

n = número de periodos

t = periodo de tiempo

r = costo por periodo de capital para la Organización (también conocido como i si se utiliza tasa de interés anual)

CF = flujo de efectivo en el periodo de tiempo t.

Note que el flujo de efectivo CF_0 en el periodo 0 también se conoce como inversión inicial.

El flujo de efectivo para un periodo dado, CF, es calculado así:

Formula 4: Para calcular Flujo Efectivo

$$CF_t = CF_{B,t} - CF_{C,t}$$

Dónde:

$CF_{B,t} =$ Flujo de efectivo de los beneficios del proyecto en un periodo de tiempo t.

$CF_{C,t} =$ Costos del proyecto en el mismo periodo de tiempo.

La conversión estándar para el flujo de efectivo es positivo (+) para entradas y negativo (-) para salidas.

La conversión de una tasa en porcentaje anual por año (APR) es igual a:

Formula 5: Para calcular la tasa de porcentaje

$$r = (1+i)^{1/m} - 1$$

i = tasa r para un periodo corto de tiempo.

m = periodos por año.

Si el Valor presente neto del proyecto es positivo, para un costo de capital dado, r, el proyecto es aprobado normalmente.

Método de la tasa interna de retorno (TIR)

La tasa interna de retorno (TIR) es el interés o tasa de descuento, i o r, que resulta en una valor presente neto de cero, NPV = 0, para el proyecto. Esto es equivalente a establecer que la carga de entradas en el tiempo es igual a la carga de salidas en el mismo tiempo. La ecuación para la TIR de Johnson es:

Formula 6: Para calcular la Tasa Interna de Retorno

$$NPV = 0 = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t}$$

La tasa interna de retorno es el valor de “r” que resulta para que VPN sea igual a 0. Una vez calculada para el proyecto, la IRR es entonces comparada con otros proyectos y oportunidades de inversión para la Organización. Los proyectos con la mayor IRR son aprobados, hasta que el capital de inversión disponible es asignado.

La mayoría de los proyectos pueden tener una IRR en el rango de 5% a 25% por año. Los gerentes a los que se les da la oportunidad de aceptar un proyecto que tiene valores calculados para IRR mayores que la tasa de retorno de inversión de la compañía (ROI), normalmente lo aprueban, asumiendo que el capital está disponible.

Las ecuaciones de arriba para el valor presente neto y la tasa interna de retorno han ignorado el efecto de los impuestos. Algunas Organizaciones toman decisiones de inversión sin incluir los impuestos, mientras otros buscan resultados después de impuestos. Las ecuaciones para el VPN y la IRR pueden ser utilizadas con impuestos, si el efecto de impuestos sobre el flujo de efectivo es conocido.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Método de periodo de pago

El periodo de pago es la longitud de tiempo necesaria para los beneficios netos de efectivo o entradas igual a los costos netos o salidas de flujo. El método de pago generalmente ignora el valor del dinero en el tiempo, los cálculos deben ser hechos tomando esto en consideración. La principal ventaja del método de pago es la simplicidad para su cálculo.

Una desventaja de este método es que los beneficios en efectivo y los costos más allá del periodo de pago no están incluidos en los cálculos.

2.3.6.2 Análisis de riesgos del proyecto

En adición al análisis costo – beneficio para un proyecto, la decisión para proceder debe incluir una evaluación de los riesgos asociados con el proyecto. Para manejar riesgos del proyecto, primero identifique y evalúe las áreas con riesgo potencial. Áreas con riesgo potencial incluyen:

Riesgos del negocio

a) Cambios tecnológicos

b) Competidores

c) Faltantes de material

d) Cuestiones de seguridad y salud

e) Cuestiones ambientales

Riesgos asegurables

a) Daño a propiedad

b) Pérdida indirecta como consecuencia

c) Responsabilidad legal

d) Personal

Después de que las áreas de riesgo son identificadas, a cada una se le debe asignar una probabilidad de ocurrencia y la consecuencia del riesgo. El factor de riesgo del proyecto entonces es la suma de los productos de probabilidad de ocurrencia y la consecuencia del riesgo.

Formula 7: Para calcular Factores de Riesgo del Proyecto

Factores del Riesgo del Proyecto = ∑(Probabilidad de ocurrencia * consecuencia del riesgo)

Los factores de riesgo para varios proyectos pueden ser comparados, si proyectos alternativos están siendo considerados. Los proyectos con factores de riesgo menores son escogidos en relación a más altos factores de riesgo.

Análisis de portafolio del proyecto

Cuando hay un portafolio de oportunidades del proyecto y recursos limitados, el gerente debe tomar decisiones para aprobar, posponer o rechazar las propuestas del proyecto. Estas decisiones están basadas en el análisis costo – beneficio del proyecto, y la evaluación de los riesgos.

El tomador de decisiones puede aprobar decisiones del proyecto basado en el rastreo del registro del gerente del proyecto, o en intuición por los beneficios no financieros del proyecto y la probabilidad de éxito.

Sin importar el método utilizado para la evaluación del proyecto, cada proyecto debe ser comparado contra los otros proyectos en el portafolio, y contra un criterio de monto establecido por la Organización para esa medición.

2.4 Definición de la Terminología

2.4.1 Algoritmo

Método expresado de manera matemática (código de cómputo) para ejecutar una función u operación específica.

2.4.2 Algoritmo Simétrico

Algoritmo que utiliza la misma clave secreta para cifrar y descifrar.

2.4.3 Amenaza

Cualquier entidad física, lógico y natural que provoque un evento, permitiendo desencadenar un incidente en la organización.

2.4.4 Análisis de Riesgo

Uso sistemático de la información para identificar fuentes y estimar el riesgo que presentan los activos de una organización.

2.4.5 Cifrado Asimétrico

Emplea dos contraseñas diferentes, una para ocultar la información y otra para recuperarla.

2.4.6 Cifrado Simétrico

Emplean una misma contraseña para ocultar y para recuperar la información.

2.4.7 Criptografía

Es la ciencia de cifrar y descifrar información, utilizando técnicas que hagan posible el intercambio de mensajes de manera segura, que sólo pueden ser leídos por las entidades a quien va dirigido.

2.4.8 Cyber-Crimen

Symantec define Cyber-crimen como un crimen que es realizado utilizando una computadora, red o hardware.

2.4.9 Ethernet

Es el estándar de red de área local más ampliamente utilizado, define las características de cableado, señalización de nivel físico y los formatos de trama del nivel del enlace de datos del modelo OSI.

2.4.10 Firewall

Un dispositivo físico o lógico que filtra paquetes entre una red privada y una red pública decide qué información puede ser entregada con base en políticas programadas.

2.4.11 Malware

Denominación que se le recibe cualquier tipo de software malicioso, el término malware incluye virus, gusanos, troyanos, rootkits.

2.4.12 Seguridad de la Información

Preservación de la confidencialidad, integridad y disponibilidad de la información, pueden estar involucradas otras propiedades como la autenticación, responsabilidad, no repudio y confiabilidad.

2.4.13 Servicio de Seguridad

Referido a ofrecer confidencialidad, integridad, no repudio, autenticación, control de acceso, disponibilidad.

2.4.14 Virus

Malware que tiene por objeto alterar el normal funcionamiento de la computadora.

CAPÍTULO III: MARCO METODOLÓGICO

.

3.1 Tipo y Diseño de Investigación

Tipo de Investigación:

Aplicada.- Debido a que aplicará teorías desarrolladas en investigaciones básicas a la presente investigación.

Explicativa.- Debido a que explicará la forma en que la variable independiente influye en la variable dependiente. Esta explicación es el eje fundamental sobre el cual se basa la investigación.

Diseño de la Investigación:

No experimental.- Debido que en nuestra investigación no se pretende variar intencionalmente variables independientes por lo que se observarán los fenómenos tal y como se dan en su contexto. Esto se debe a las limitaciones sobre el costo de implantación y el tiempo prolongado de obtención de resultados.

. **T1** **T2**

N O P RE

Dónde:

N: Es la población que se está observando.

O: Es la observación a desarrollar en la muestra.

P: Es la propuesta de la presente investigación.

T1: Es el tiempo de medición de la Observación.

T2: Es el tiempo de proyección del escenario hipotético.

RE: Son los resultados estimados.

3.2 Población y Muestra

3.2.1 Población:

Esta investigación tomará como población a la cantidad de data enviada y recibida en la red perimetral de la institución “ABACO”, es decir todo el tráfico IP permitido entre la red origen y destino.

3.2.2 Muestra:

Debido a que se tiene acceso a la red perimetral del Instituto Superior Tecnológico Privado “ABACO”, se trabaja con toda la población.

3.3 Hipótesis

El desarrollo de un sistema criptográfico, utilizando algoritmos avanzados de encriptación permitirá mejorar la seguridad perimetral de una red informática.

3.4 Operacionalización de variables

3.4.1 Variable Independiente

Sistema criptográfico.

3.4.2 Variable Dependiente

Mejora de la seguridad perimetral de una red informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 1: Operacionalización de Variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES Y /O INDICADORES	TECNICA E INSTRUMENTO
Variable Independiente Sistema criptográfico	Sistema que se utiliza para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.	Consiste en definir qué tan protegidos se encontrarían los datos encriptados que son enviados dentro de la red de la empresa.	➢ Cantidad de paquetes encapsulados. ➢ Cantidad de paquetes desencapsulados. ➢ Cantidad de paquetes encriptados. ➢ Cantidad de paquetes desencriptados.	**Técnica:** Observación **Instrumento:** Guía de observación de la bitácora sobre datos del sistema criptográfico

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Variable Dependiente Mejora de la seguridad perimetral de una red informática. . .	Es el establecimiento de un perímetro de seguridad el cual protege y aísla la red interna y la red local de servicios de las entradas externas.	Consiste en poder establecer un perímetro de seguridad, apoyándose de algoritmos criptográficos avanzados, para mejorar y controlar el acceso a la data que tiene la empresa dentro de su red informática.	➢ Disminución de datos desencriptados por personal no autorizado. ➢ Cantidad de paquetes protegidos al recibir la información. ➢ Cantidad de paquetes protegidos al enviar información.	. **Técnica:** Observación **Instrumento:** Guía de plan de pruebas del sistema criptográfico

Fuente: Elaboración Propia

Tabla 2: Medición de Indicadores

Indicador	Descripción	Unidad de Medida	Formula	Técnica
Cantidad de paquetes encapsulados.	Es la cantidad de paquetes encapsulados al enviar la información.	Paquetes	**CPEN= TPEN – TPNEN** CPEN= Cantidad de Paquetes encapsulados. TPEN= Total de Paquetes encapsulados. TPNEN= Total de Paquetes no encapsulados.	Observación
Cantidad de paquetes desencapsulados.	Es la cantidad de paquetes Desencapsu-lados al recibir la información.	Paquetes	**CPDE = TPDE – TDNDE** CPDE= Cantidad de Paquetes Desencapsulados. TPDE= Total de paquetes Desencapsulados. TPNDE= Total de Paquetes no Desencapsulados.	

Cantidad de paquetes encriptados.	Es la cantidad de paquetes encriptados al enviar la información.	Paquetes	**CPE= TPE – TPNE** CPE= Cantidad de Paquetes encriptados. TPE= Total de paquetes encriptados. TPNE= Total de Paquetes no encriptados.	
Cantidad de paquetes desencriptados.	Es la cantidad de paquetes desencriptados al recibir la información.	Paquetes	**CPD= TPD – TPND** CPD= Cantidad de Paquetes desencriptados. TPD= Total de paquetes desencriptados. TPND= Total de Paquetes no desencriptados.	

Fuente: Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.5 Métodos, Técnicas e instrumentos de recolección de datos

3.5.1 Métodos de investigación

Análisis: porque se descompuso el objeto de estudio en sus partes para conocer sus riesgos y propiedades. En este caso tenemos que conocer los niveles de seguridad perimetral en el Instituto Superior Tecnológico privado “ABACO”, y así poder determinar los parámetros del desarrollo del Sistema en mención.

Síntesis: porque una vez analizada la situación actual en cuanto a los niveles de seguridad perimetral en el Instituto Superior Tecnológico privado “ABACO”, se planteó una solución: Desarrollo de un Sistema Criptográfico utilizando algoritmos avanzados para la seguridad perimetral de la red.

Deductivo: porque después de haber definido las variables independientes y sus parámetros se infirió la hipótesis para el desarrollo del Sistema.

3.5.2 Instrumento de recolección de datos

Las técnicas e instrumentos de recolección de datos, utilizadas en la presente investigación, son las detalladas a continuación:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 3: Instrumentos y Métodos de recolección de Datos

TÉCNICA	DESCRIPCIÓN	INSTRUMENTO
Observación	• Se observara a los datos almacenados en la bitácora del sistema criptográfico para comprar resultados antes y después de hacerle las pruebas al sistema.	Guía de observación de la bitácora sobre datos del sistema criptográfico
Observación	• Se observarán los procesos de pruebas que se le hacen al sistema para ver si se logró cumplir con el objetivo planteado en la presente investigación, el cual está dado por la mejora de la seguridad perimetral de la red informática de la institución a la cual se le implemente el mencionado sistema.	Guía de plan de pruebas del sistema criptográfico

Fuente: Elaboración Propia

3.6 Procedimiento para la recolección de datos

A continuación se muestra el flujo de proceso para la obtención de datos:

Observación de los datos: A través de formatos impresos en papel bond se pretende realizar la toma de nota sobre los datos observados de la bitácora del sistema criptográfico, de los cuales se obtendrá la información necesaria con respecto al tema de investigación propuesto.

Tabulación: A través de cuadros establecidos bajo los indicadores que la presente investigación presenta, se ha determinado una comparación entre el rendimiento actual y a futuro de dichos indicadores.

3.7 Análisis Estadístico e Interpretación de los datos

La presente investigación tuvo dos enfoques para el análisis de datos los cuales están descritos a continuación:

a) Enfoque cualitativo

Ya que para esta investigación se realizó: guías de observación tanto de la bitácora del sistema como de la información que se obtiene al ejecutar el mismo.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

b) Enfoque cuantitativo

Puesto que los datos que se presentaran serán tomados de la base de datos del Instituto Superior Tecnológico “ABACO”, a través de los cuales se puedo determinar cómo se dan los procesos que involucran la protección de su red informática. En cuanto al encriptamiento y desencriptamiento de los datos que se manejan dentro de la misma.

3.8 Criterios Éticos

Según el (CÓDIGO DEONTOLÓGICO DEL COLEGIO DE INGENIEROS DEL PERÚ, 2012)el proyecto cumplió con los siguientes criterios éticos relacionados al desarrollo del mismo:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 4: Criterios éticos de la Investigación

Criterios	Características éticas del criterio
Medio ambiente	La propuesta de solución propiciará el cuidado del medio ambiente.
Confidencialidad	Se asegurará la protección de la identidad de la institución y las personas que participan como informantes de la investigación.
Objetividad	El análisis de la situación encontrada se basará en criterios técnicos e imparciales.
Originalidad	Se citarán las fuentes bibliográficas de la información mostrada, a fin de demostrar la inexistencia de plagio intelectual.
Veracidad	La información mostrada será verdadera, cuidando la confidencialidad de ésta.
Derechos laborales	La propuesta de solución propiciará el respeto a los derechos laborales en la entidad de estudio.

Fuete: Elaboración propia

3.9 Criterios de rigor científico

Teniendo en cuenta lo presentado por (Alcaraz Moreno & Noreña, 2012), en esta investigación se tuvo en consideración los siguientes criterios de rigor científico en cuanto a:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 5: Criterios de Rigor Científicos aplicados a la investigación

Criterios	Características científicas del criterio
Confiabilidad	Se realizarán cálculos estadísticos para la determinación del nivel de consistencia interna de los instrumentos de recolección de datos.
Validación	Se validarán los instrumentos de recolección de datos y la propuesta de solución a través de Juicio de Expertos.
Contrastación	Se contrastará la hipótesis a través de métodos estadísticos debido al diseño pre experimental.

Fuete: Elaboración propia

CAPÍTULO IV: ANÁLISIS E INTERPRETACION DE LOS RESULTADOS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.1 Resultados en tablas y gráficos

El presente capítulo tiene como objetivo presentar los resultados de la aplicación de los instrumentos de recolección de datos que fueron aplicados al Instituto Superior Tecnológico Privado “ABACO” y estuvieron sujetas a estudio.

También se mostrará el resultado gráfico y tabular de cada instrumento de recolección de datos aplicado en la presente investigación y a continuación su interpretación correspondiente para poder determinar la conclusión final como aporte del trabajo en conjunto.

Cabe mencionar que el Sistema Criptográfico en estudio, se utilizó desde Mayo hasta Junio, meses donde se recopilo la información necesaria, para medir los indicadores de nuestra variable dependiente, los cuales se detallan a continuación:

a) **Cantidad de paquetes encapsulados:** Es la cantidad de paquetes encapsulados al enviar la información

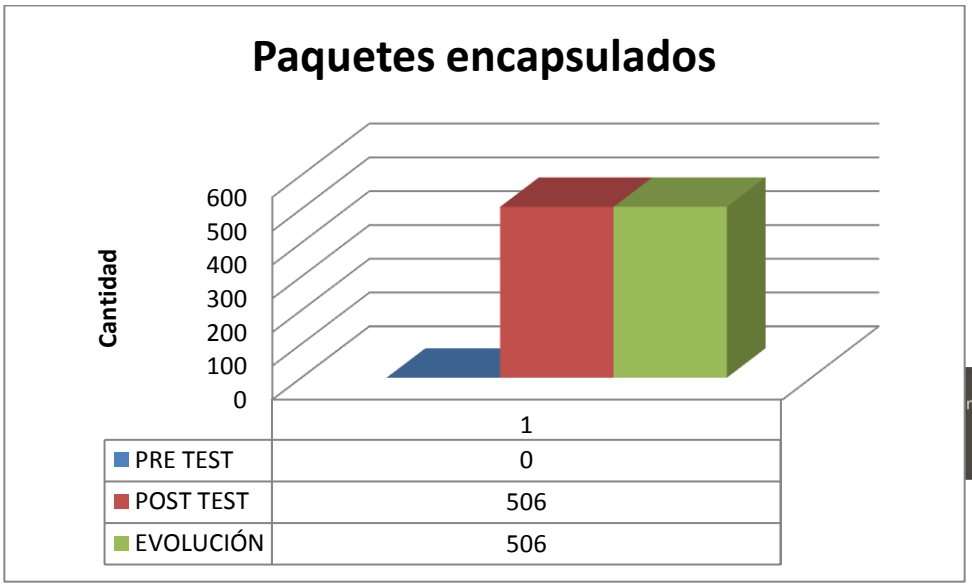
Tabla 6: Cantidad de paquetes encapsulados al enviar la información

INDICADOR	PREGUNTA	TIPO	UNIDAD DE MEDIDA	PRE TEST	POST TEST	EVOLUCIÓN
Cantidad de paquetes encapsulados	¿Cuánto paquetes encapsulados de la base de datos existen?	Cuantitativo. Continuo.	Paquetes	0	506	506

Fuente: Muestra de la investigación

Elaboración: Propia

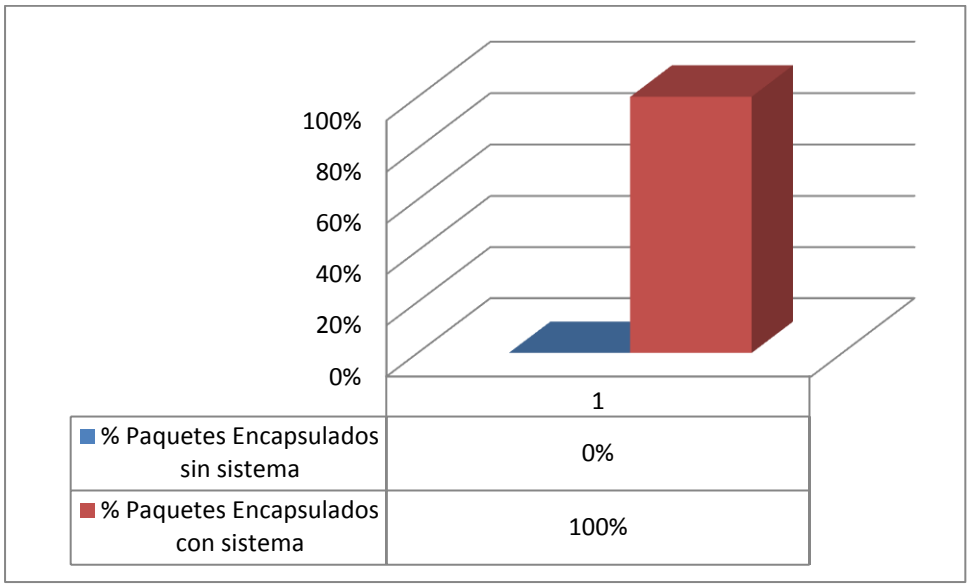
Gráfico 1: Cantidad de paquetes encapsulados al enviar la información



Fuente: Muestra de la investigación

Elaboración: Propia

Gráfico 2: Representación de la cantidad de paquetes encapsulados al enviar la información en porcentajes



Fuente: Muestra de la investigación

Elaboración: Propia

Gráficamente se puede observar que con la utilización del Sistema Criptográfico se pudo aumentar la encapsulación de los paquetes, al enviar información, puesto que se aumentó la encapsulación de 506 paquetes en la ejecución de esta actividad, lo que representa una un aumento de un 100% en la encapsulación general de paquetes tenidos en la base de datos del instituto ABACO.

b) Cantidad de Paquetes desencapsulados: Es la cantidad de paquetes desencapsulados al recibir la información.

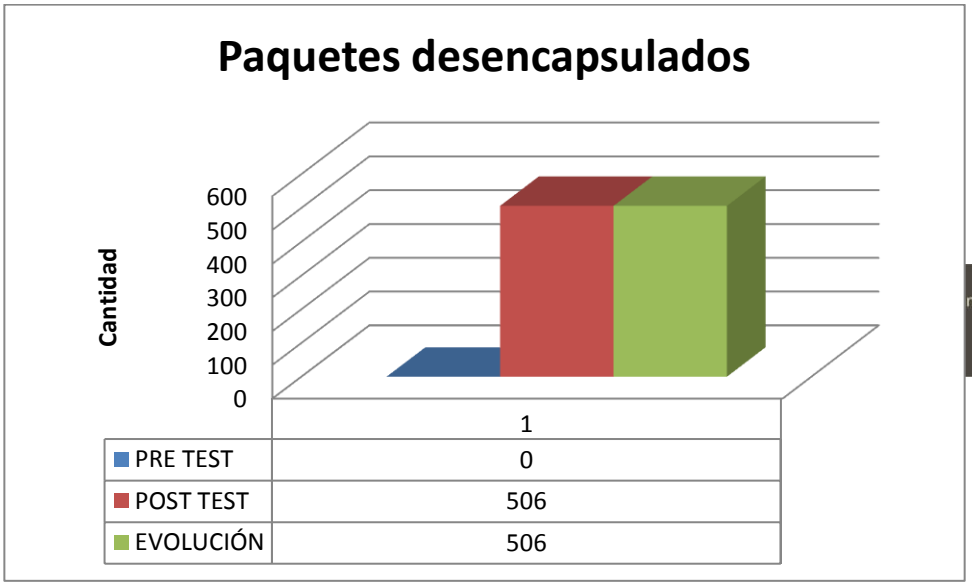
Tabla 7: Cantidad de paquetes desencapsulados al recibir la información

INDICADOR	PREGUNTA	TIPO	UNIDAD DE MEDIDA	PRE TEST	POST TEST	EVOLUCIÓN
Cantidad de paquetes desencapsulados	¿Cuánto paquetes desencapsulados de la base de datos existen?	Cuantitativo. Continuo.	Paquetes	0	506	506

Fuente: Muestra de la investigación

Elaboración: Propia

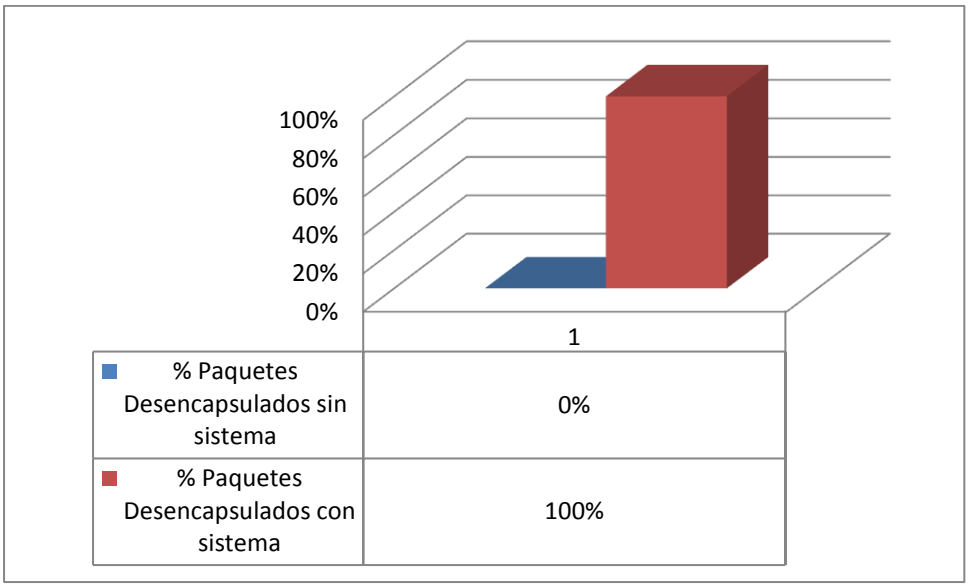
Gráfico 3: Cantidad de paquetes desencapsulados al recibir la información



Fuente: Muestra de la investigación

Elaboración: Propia

Gráfico 4: Representación de la cantidad de paquetes desencapsulados al recibir la enviar en porcentajes



Fuente: Muestra de la investigación

Elaboración: Propia

Gráficamente se puede observar que con la utilización del Sistema Criptográfico se pudo aumentar la protección de los paquetes, al recibir información, puesto que se aumentó la seguridad de 506 paquetes en la ejecución de esta actividad, lo que representa una un aumento de un 100% en la protección general de paquetes tenidos en la base de datos del instituto ABACO.

c) **Cantidad de paquetes encriptados:** Es la cantidad de paquetes en total los cuales se encuentran encriptados al enviar la información.

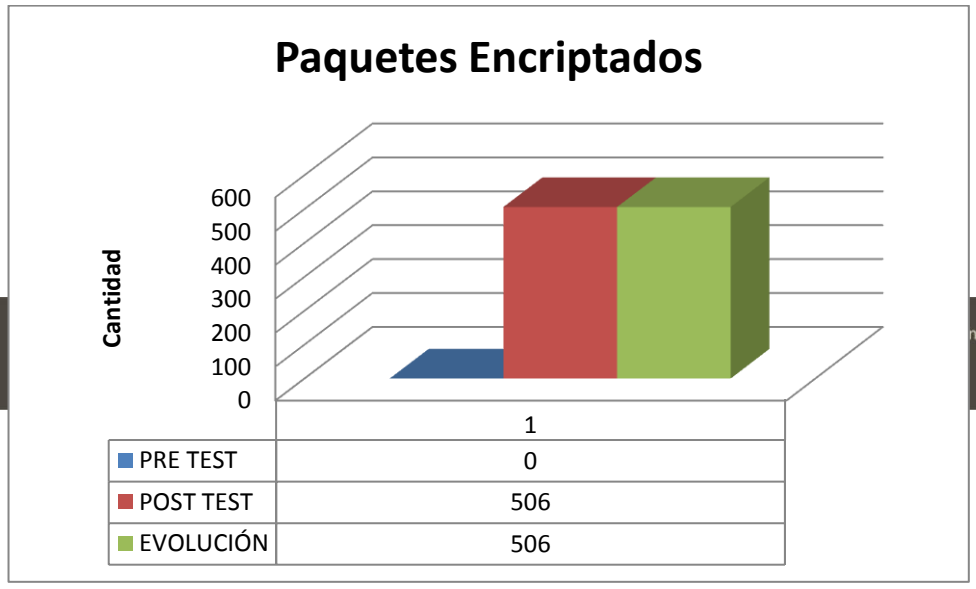
Tabla 8: Cantidad de paquetes encriptados al enviar la información

INDICADOR	PREGUNTA	TIPO	UNIDAD DE MEDIDA	PRE TEST	POST TEST	EVOLUCIÓN
Cantidad de paquetes encriptados	¿Cuánto paquetes encriptados existen dentro de la red informática?	Cuantitativo. Continuo.	Paquetes	0	506	506

Fuente: Muestra de la investigación

Elaboración: Propia

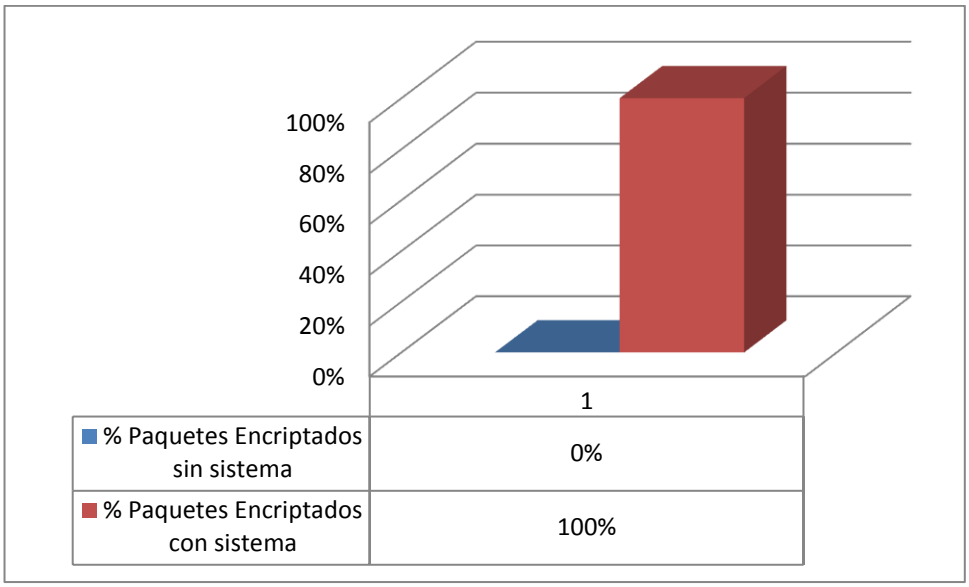
Gráfico 5: Cantidad de paquetes encriptados al enviar información



Fuente: Muestra de la investigación

Elaboración: Propia

Gráfico 6: Representación de la cantidad de paquetes encriptados al enviar la información



Fuente: Muestra de la investigación

Elaboración: Propia

Gráficamente se puede observar que con la utilización del Sistema Criptográfico se pudo aumentar la protección de los paquetes que están dentro de la red informática, puesto que se aumentó la encriptación de los mismos en 506 paquetes en la ejecución de esta actividad, lo que representa una un aumento de un 100% en la protección general de paquetes tenidos en la base de datos del instituto ABACO.

d) Cantidad de paquetes desencriptados: Es la cantidad de paquetes desencriptados al recibir la información.

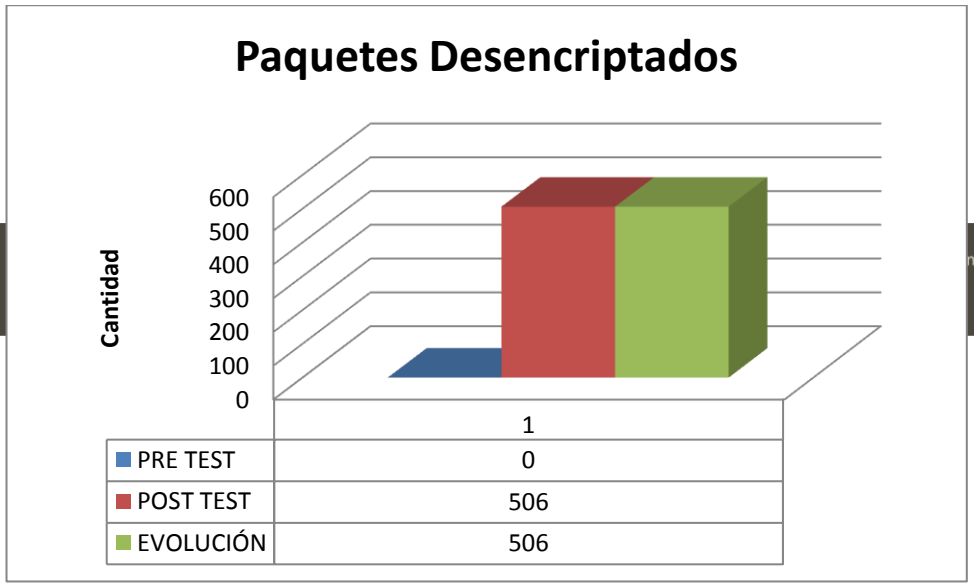
Tabla 9: Cantidad de paquetes desencriptados al recibir la información

INDICADOR	PREGUNTA	TIPO	UNIDAD DE MEDIDA	PRE TEST	POST TEST	EVOLUCIÓN
Cantidad de paquetes desencriptados	¿Cuánto paquetes desencriptados existen dentro de la red informática?	Cuantitativo. Continuo.	Paquetes	0	506	506

Fuente: Muestra de la investigación

Elaboración: Propia

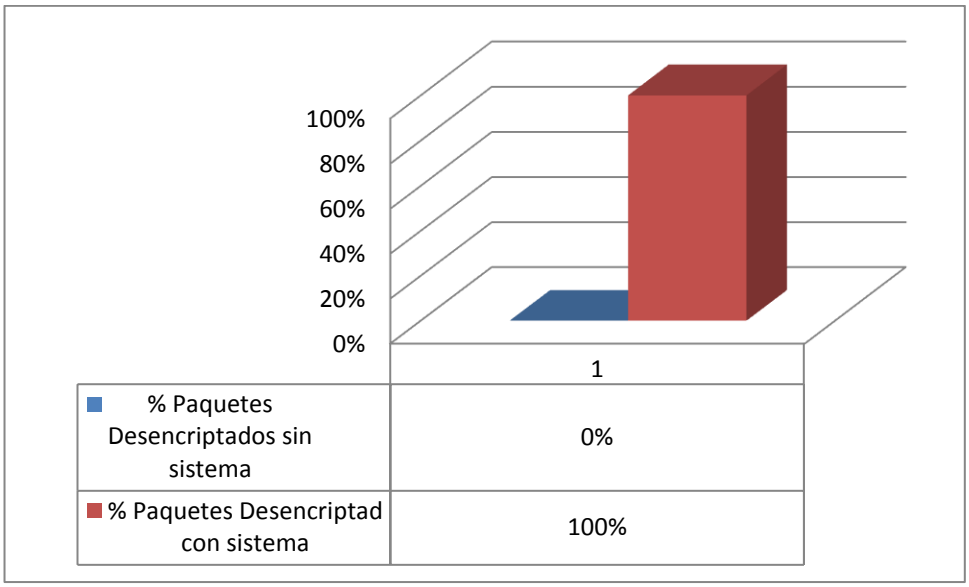
Gráfico 7: Cantidad de paquetes desencriptados al recibir la información



Fuente: Muestra de la investigación

Elaboración: Propia

Gráfico 8: Representación de la cantidad de paquetes desencriptados al recibir la información



Fuente: Muestra de la investigación

Elaboración: Propia

Gráficamente se puede observar que con la utilización del Sistema Criptográfico se pudo aumentar la protección de los paquetes que están dentro de la red informática, puesto que se aumentó la desencriptación de los mismos en 506 paquetes en la ejecución de esta actividad, lo que representa una un aumento de un 100% en la protección general de paquetes al recibir la información de la base de datos del instituto ABACO.

4.2 Discusión de Resultados

A nivel del Sistema Criptográfico

Los resultados obtenidos durante el desarrollo de la presente investigación, han sido satisfactorios ya que con la utilización del Sistema Criptográfico se pudo contrastar la hipótesis planteada anteriormente.

A nivel de Observación de Resultados

Con respecto a la observación de resultados realizados a la base de datos del Instituto Superior Tecnológico Privado “ABACO” , la cual fue tomada como muestra, se pudo determinar que:

a) Se puede proteger la integridad de los datos con la protección contra la modificación de los datos en forma intencional o accidental, que ofrecen los algoritmos avanzados.

b) El sistema criptográfico proporciona la autenticidad del origen del mensaje, garantizándole al receptor que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo.

c) El sistema también proporciona el no repudio del origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN

5.1. Reunir requisitos y expectativas

Ha sido el proceso destinado a recabar información en el Instituto Superior Tecnológico Privado “ABACO”, ayuda a aclarar e identificar cualquier problema de la red actual.

a) Se formuló las siguientes preguntas al reunir la información:
b) Quienes son las personas que utilizan la red.
c) Datos críticos de la organización.
d) Que operaciones han sido declaradas críticas por la organización.
e) Protocolos permitidos en la red.
f) Cuantos hosts son soportados dos y cuáles son los tipos.
g) Quien es el responsable de las direcciones, la denominación, el diseño de topología y la configuración de las LAN.

a) Las personas que utilizan la red

Los beneficiados participaron de una comunicación rápida e integral lo que permitió aumentar la eficiencia y efectividad de todos los trabajadores utilizando los servicios informáticos y facilitó el acceso a todos aquellos que querían conectarse, se logró incrementar la movilidad y flexibilidad en sus coordinaciones reduciendo tiempo y problemas con la correcta y oportuna actualización de la información.

Las entidades involucradas:

- Sede Chiclayo
- Sede Lima

b) Datos críticos de la organización

Los datos críticos se encontraban en el servidor web, el servidor de base de datos, el servidor de correo y servidor de ftp e aplicaciones. Además de la comunicación con la sede Abaco – Lima.

c) Que operaciones han sido declaradas críticas por la organización

Los servicios informáticos que brindamos a través de nuestros servidores y las comunicaciones con la sede Abaco – Lima, porque tenemos que brindar un servicio confiable y seguro.

d) Protocolos permitidos en la red

Los protocolos a usar son los siguientes:

Redes Inalámbricas

- IEEE 802.3
- DHCP
- WPS
- Authentication Method Exted Service Set ID (ESSID)

- Powerover Ethernet

Telefonía IP

- IP
- Compresiones G.711 y G.729
- Session Initiation Protocol (SIP) puerto 5060

Red LAN

- Sistema de nombres de dominio (DNS): TCP/UDP 53.
- Protocolo de transferencia de hipertexto (HTTP), TCP 80.
- Protocolo simple de transferencia de correo (SMTP): TCP 25.
- Protocolo de oficina de correos (POP): UDP 110.
- Telnet: TCP 23.
- Protocolo de configuración dinámica de host (DHCP): UDP 67.
- Protocolo de transferencia de archivos (FTP): TCP 20 y 21.
- Protocolo de transferencia Datos SQL (TCP): TCP 1433.

e) Hosts Soportados

En la sede Chiclayo cuenta con 50 computadoras para administrativos, 4 servidores, 80 computadoras para laboratorios y 10 para aulas multimedia. En la sede Lima cuenta con 10 computadoras para administrativos, 1 para aula multimedia.

f) Responsable de las direcciones, la denominación, el diseño de topología y la configuración de las LAN

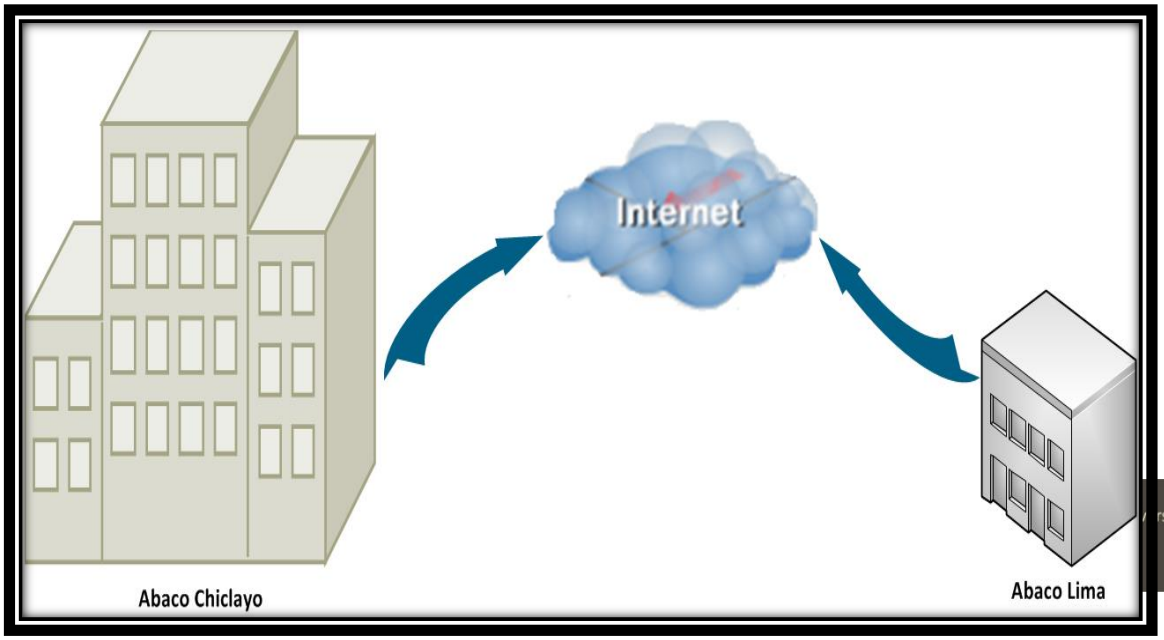
El Jefe de tecnologías de la información y comunicación, el cual desempeña sus funciones en el local de Chiclayo.

5.3. Diseñar la estructura o topología de las Capas 1, 2 y 3 de la LAN

5.3.1. Capa Física

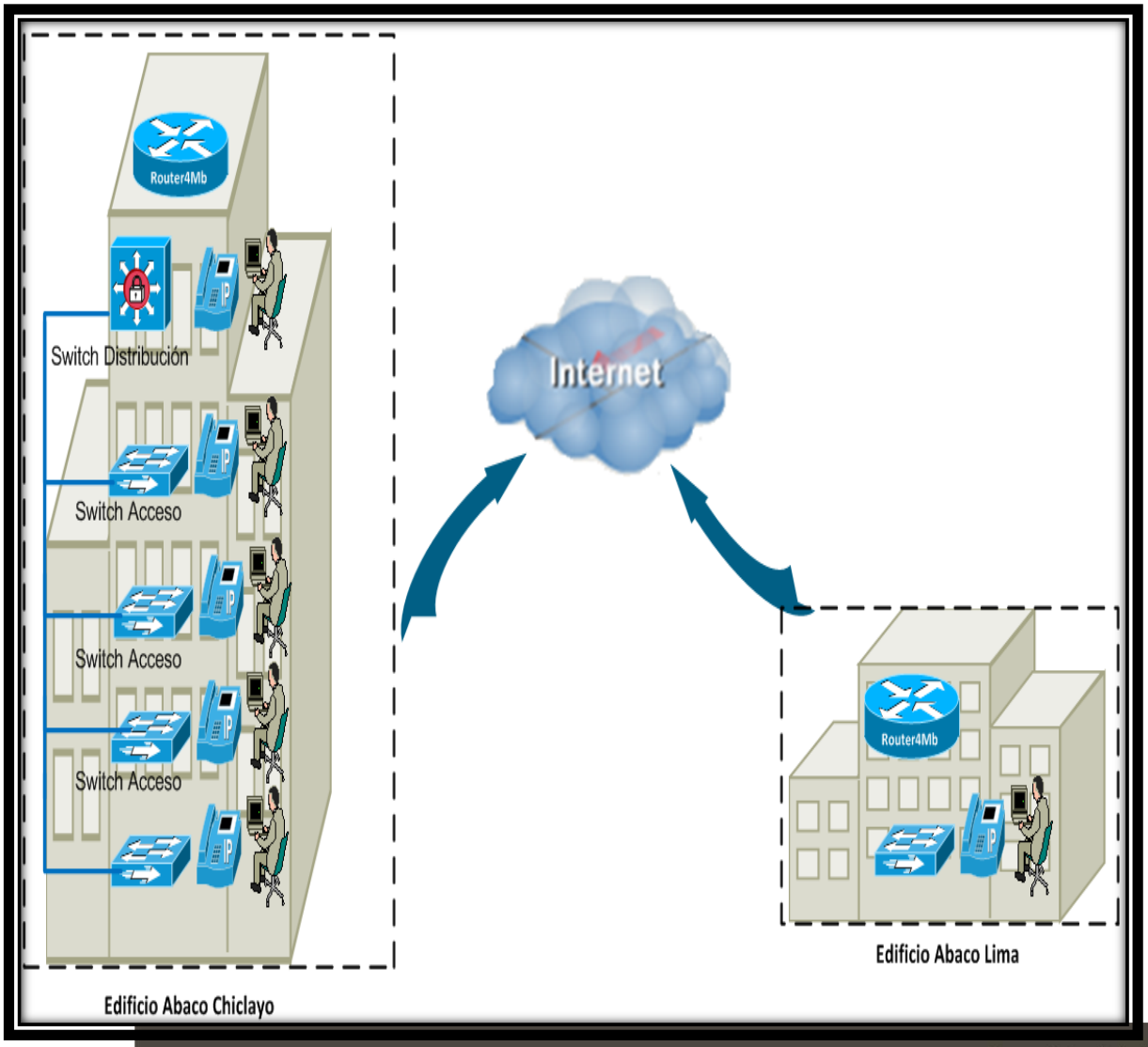
En la capa física se muestra el diseño de red actual y propuesto.

Diagrama 1: Diagrama contextual de la Red



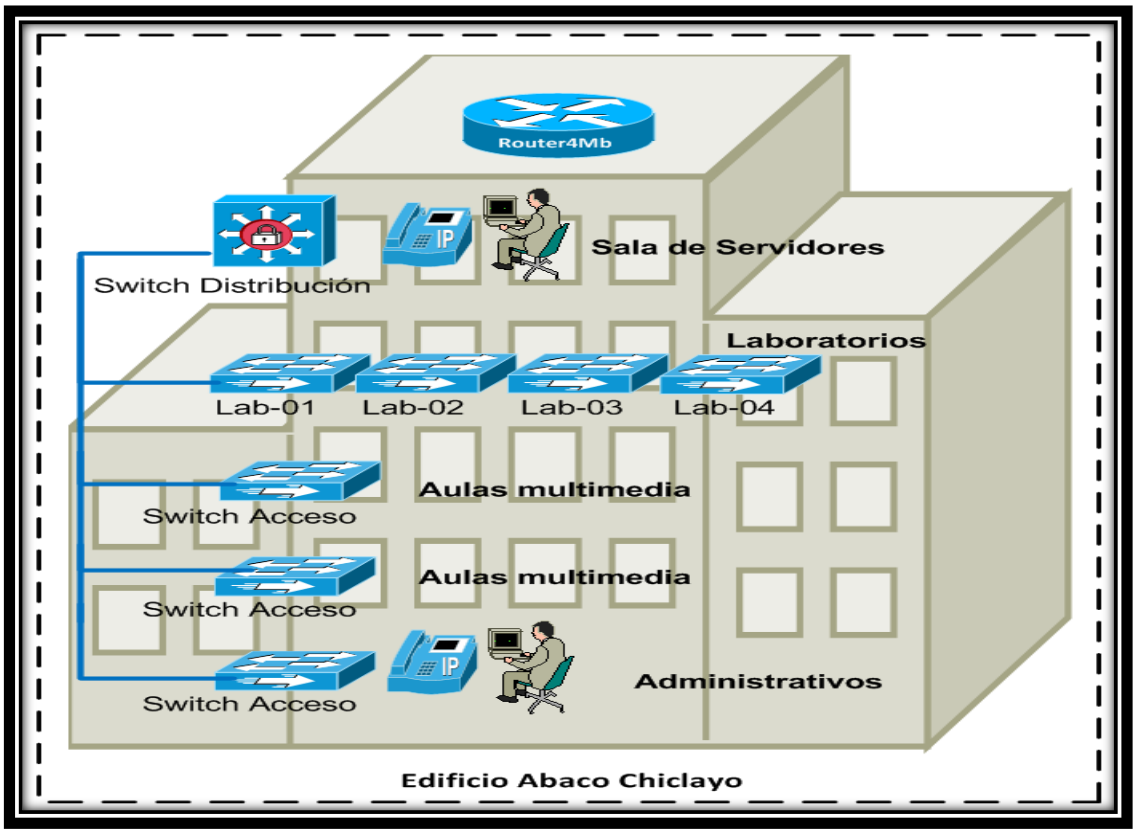
Fuente: Elaboración Propia

Diagrama 2: Diagrama contextual de la Red por Local



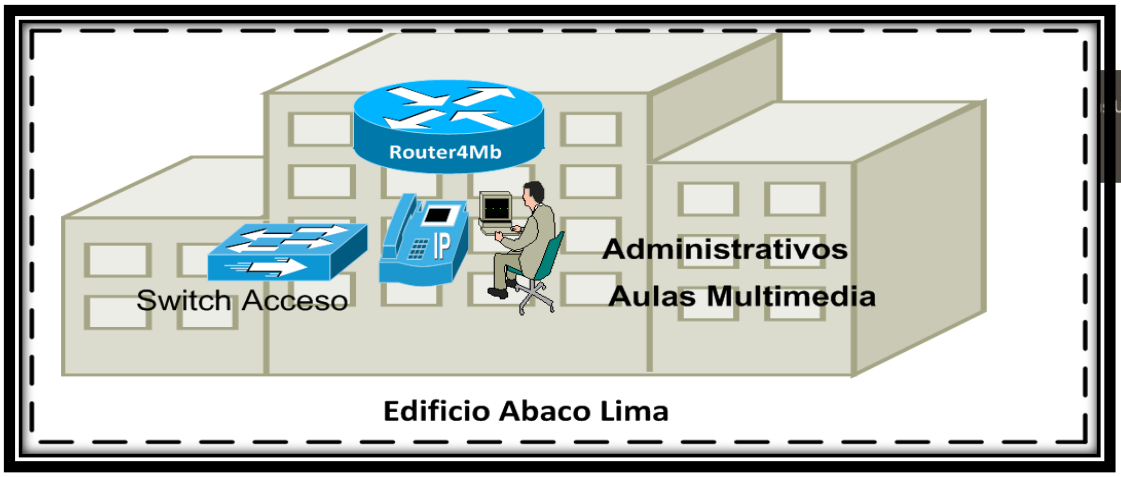
Fuente: Elaboración Propia

Diagrama 3: Diagrama contextual de la Red por Local Chiclayo



Fuente: Elaboración Propia

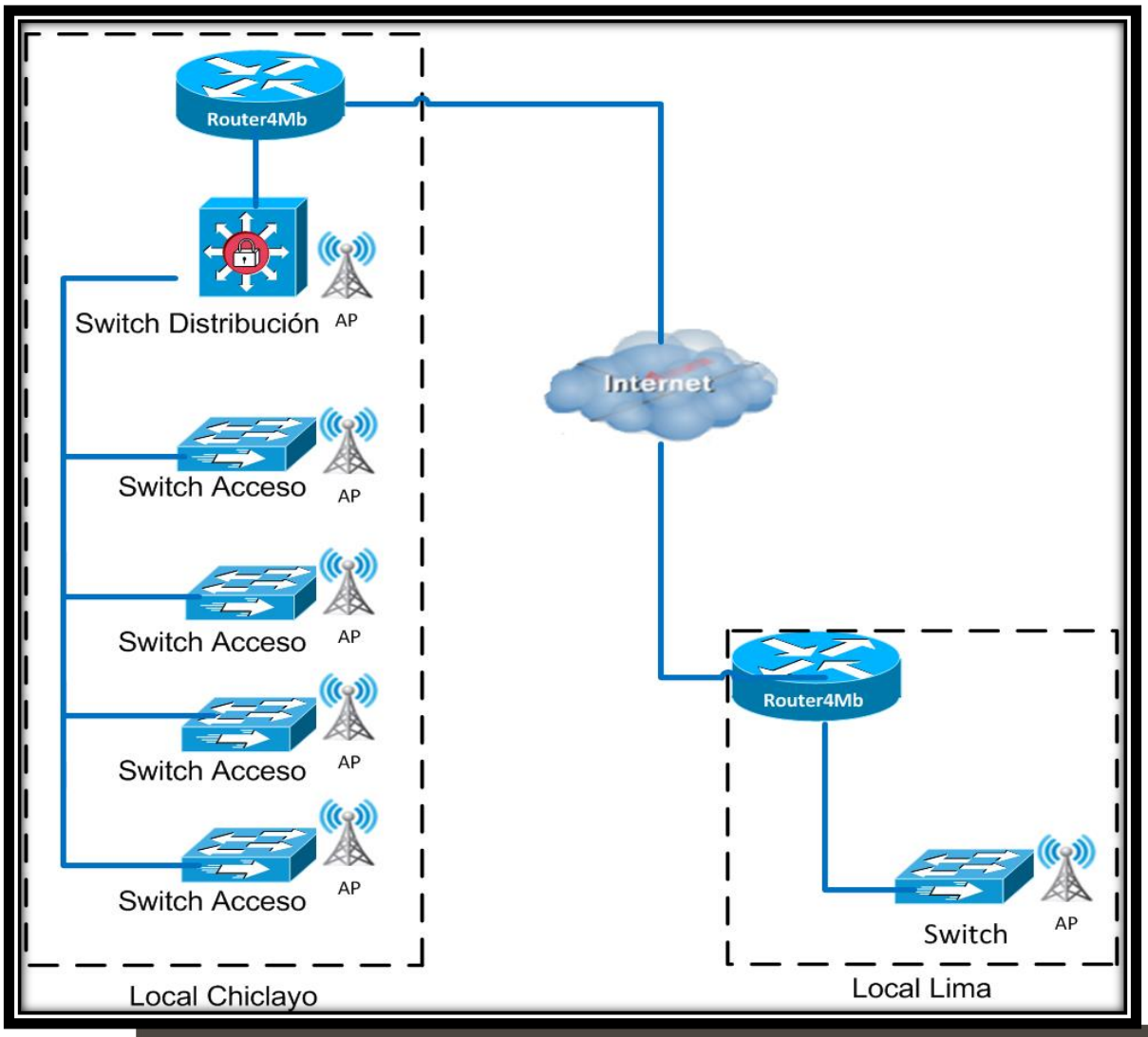
Diagrama 4: Diagrama contextual de la Red por Local Lima



Fuente: Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Diagrama 5: Diagrama Físico Actual



Fuente: Elaboración Propia

5.3.2. Capa Enlace de datos

Se sugirió un modelo jerárquico de capas (núcleo, distribución, acceso). Se hizo la distribución de switchy de su sede. Se distribuyeron sus puertos de cada switch empleado.

Se asignaron y crearon LAN virtuales (VLAN) para crear una segmentación de la red con la finalidad dar seguridad a la red.

Ubicación: Chiclayo
Nombre del Switch: Distribución
Dirección IP: 10.10.10.10
Mascara: 255.255.255.0
Gateway: 10.10.10.1
Modo VTP: Servidor
Dominio VTP: vtpabaco

Tabla 10: LAN virtuales Chiclayo

Tipo/ Puerto/ Número de Interfaz/ Subinterfaz	VLAN	Asignada a
0/1	Trunk	Administración
0/2	Trunk	Administrativos
0/3	Trunk	Wifi
0/14	Trunk	WAN
0/15	Trunk	Red Interna
0/16	Trunk	Red Externa
0/17	Trunk	Laboratorios
0/18	Trunk	Aulas Multimedia

Fuente: Elaboración Propia

Ubicación: Lima

Nombre del Switch: Distribución

Dirección IP: 10.10.10.11

Mascara: 255.255.255.0

Gateway:10.10.10.1

Tabla 11: LAN virtuales Lima

Tipo/ Puerto/ Número de Interfaz/ Subinterfaz	VLAN	Asignada a
0/1	Trunk	Administración
0/2	Trunk	Administrativos
0/3	Trunk	Wifi
0/14	Trunk	Aulas Multimedia
0/15	Trunk	WAN

Fuente: Elaboración Propia

Tabla 12: ID de VLAN

ID de VLAN	*Descripción*
10	Administración
11	Administrativos
12	Wifi
13	WAN
14	Red Interna
15	Red Externa
16	Laboratorios
17	Aulas Multimedia

Fuente: Elaboración Propia

5.3.3. Capa de Red

Se realizó el direccionamiento IP. Según topología propuesta para red perimetral.

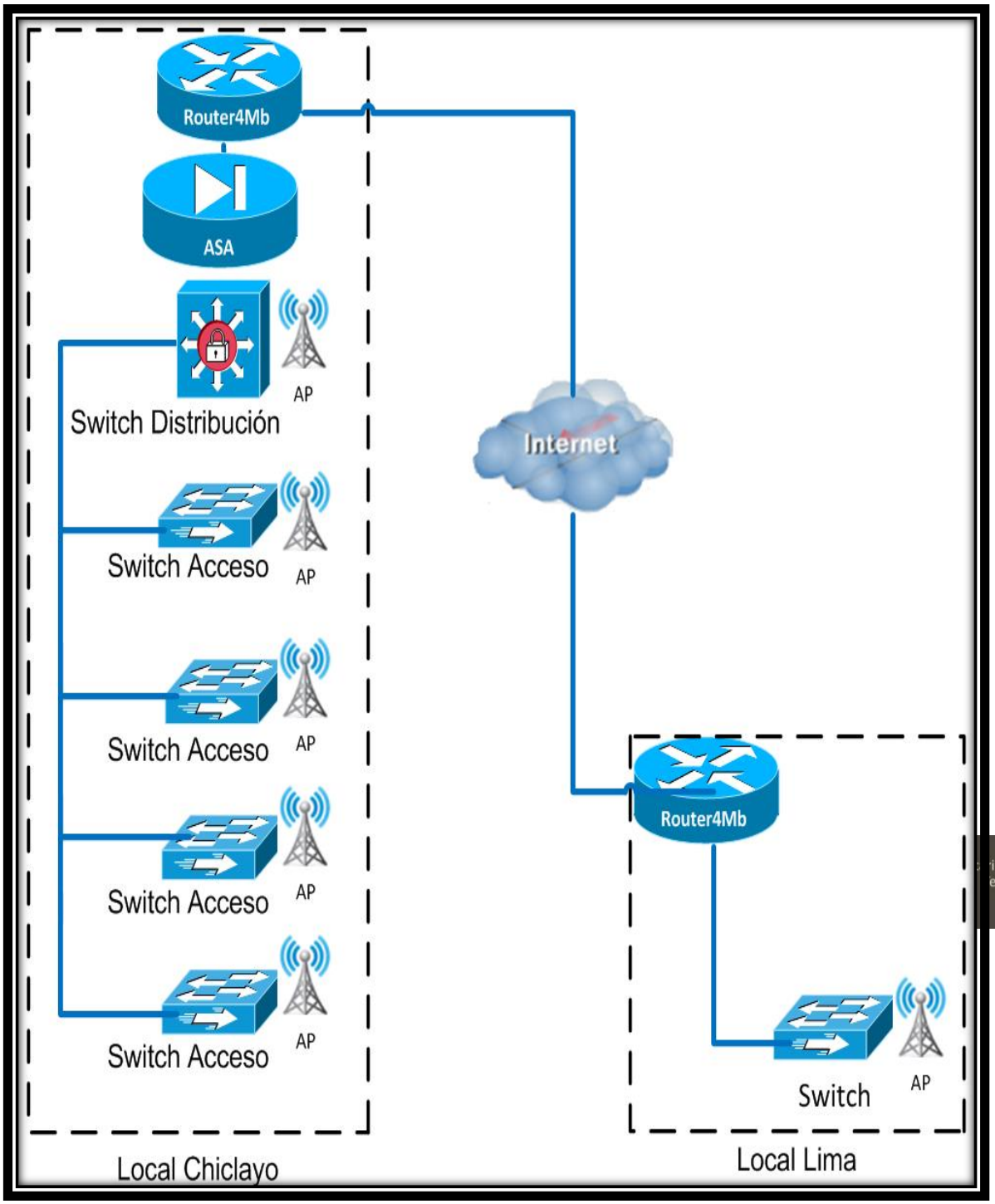
Tabla 13: Direccionamiento IP

ID de VLAN	*Descripción de Asignación*	*Direccionamiento IP*
10	Administración	10.10.10.0/24
11	Administrativos	172.17.1.0/24
12	Wifi	10.20.0.0/24
13	WAN	100.100.1.0/28
14	Red Interna	172.17.2.0/24
15	Red Externa	172.16.1.0/24
16	Laboratorios	10.30.0.0/24
17	Aulas Multimedia	10.40.0.0/24

Fuente: Elaboración Propia

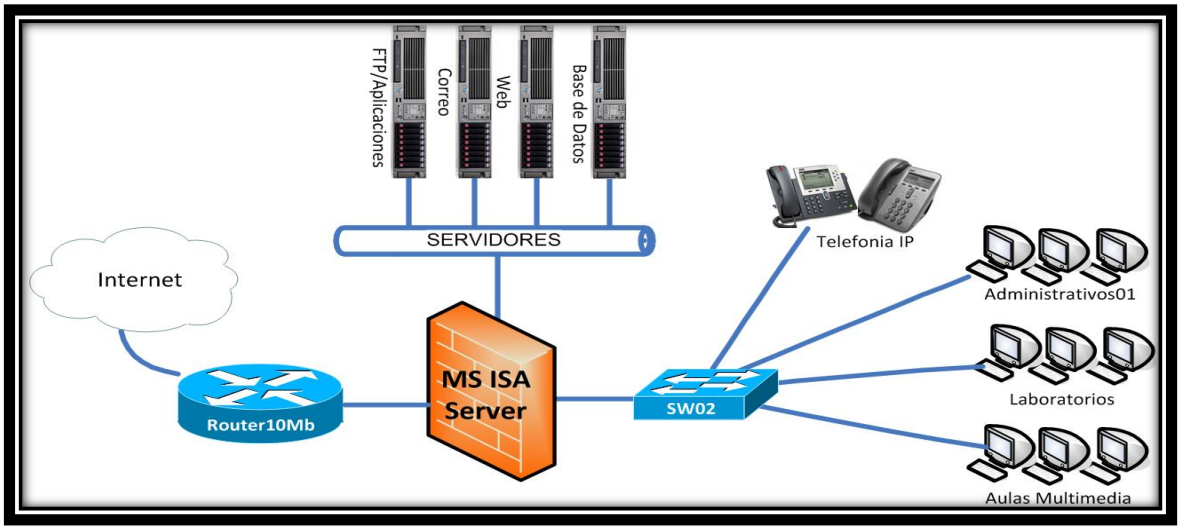
5.4. Diseñar la Físico y Lógico

Diagrama 6: Diagrama Físico Propuesto



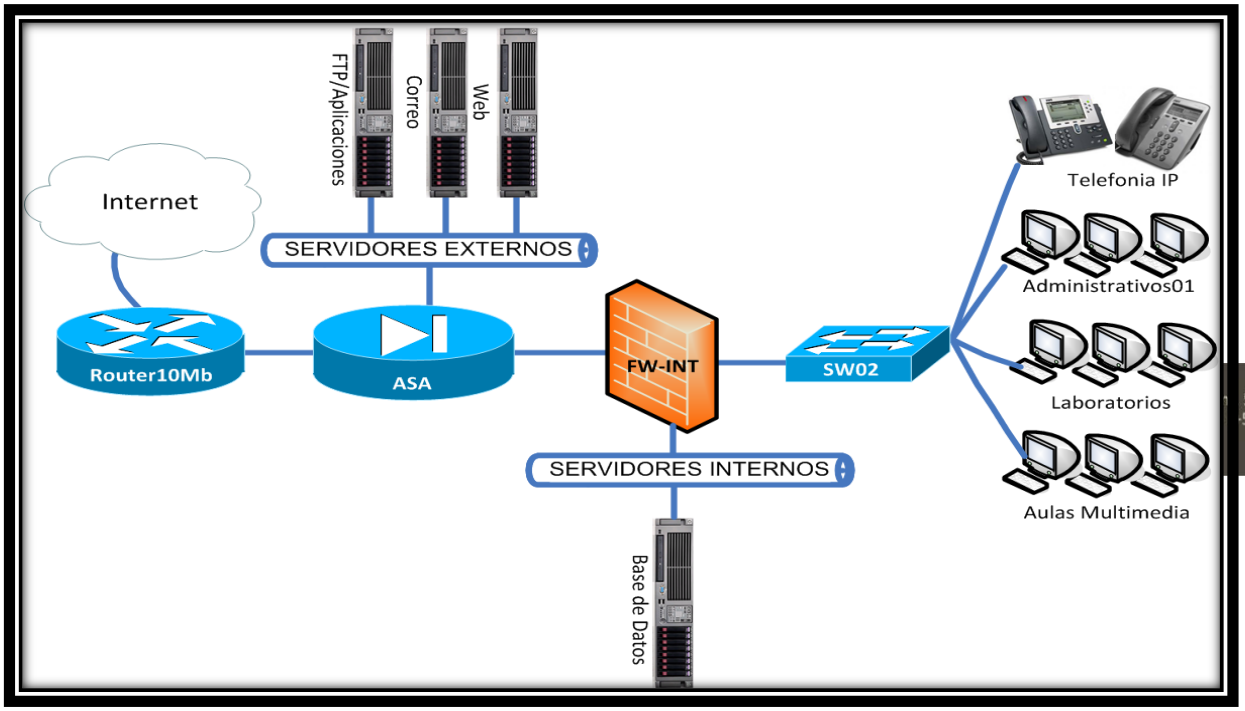
Fuente: Elaboración Propia

Diagrama 7: Diagrama Lógico Actual



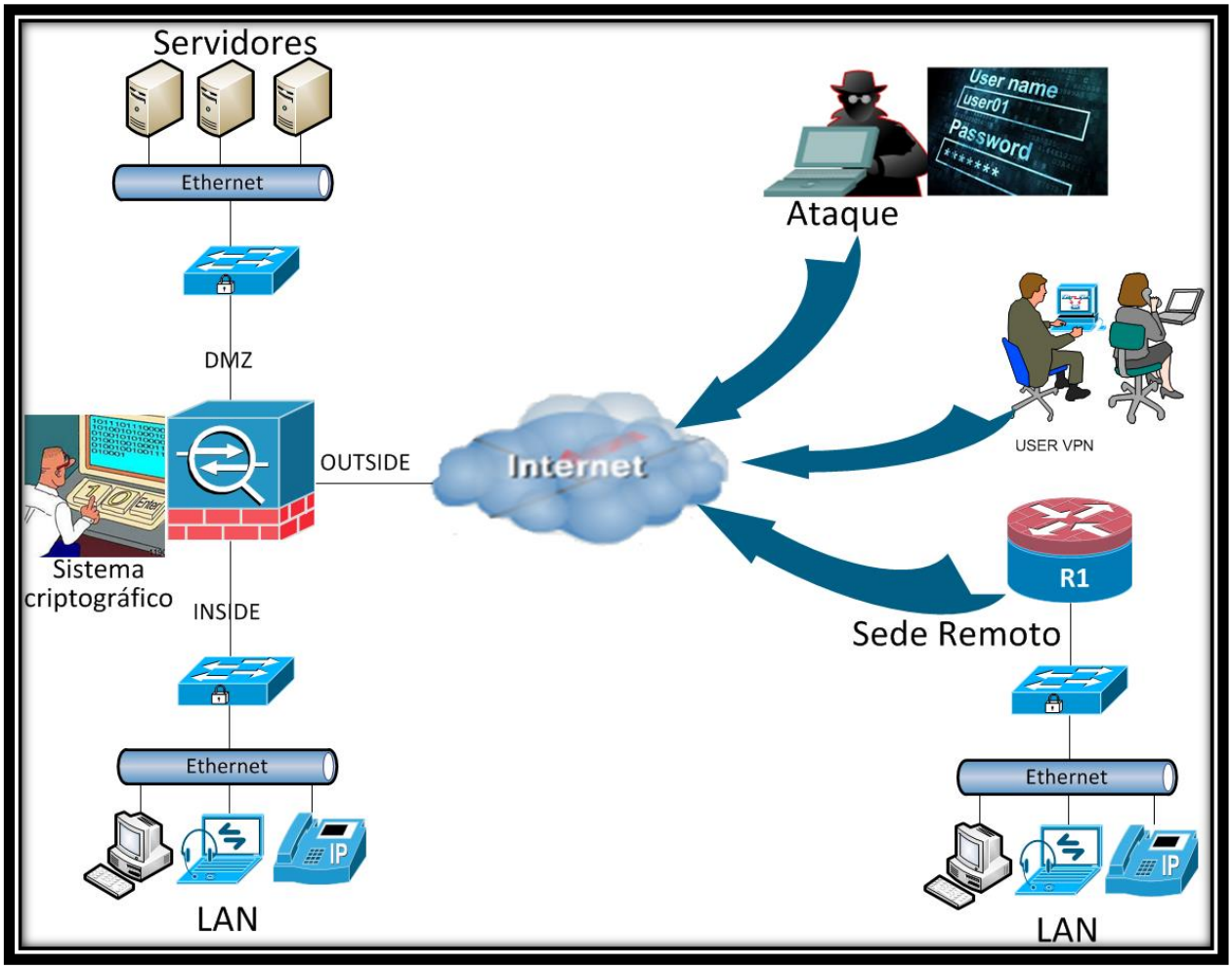
Fuente: Elaboración Propia

Diagrama 8: Diagrama Lógico Propuesto



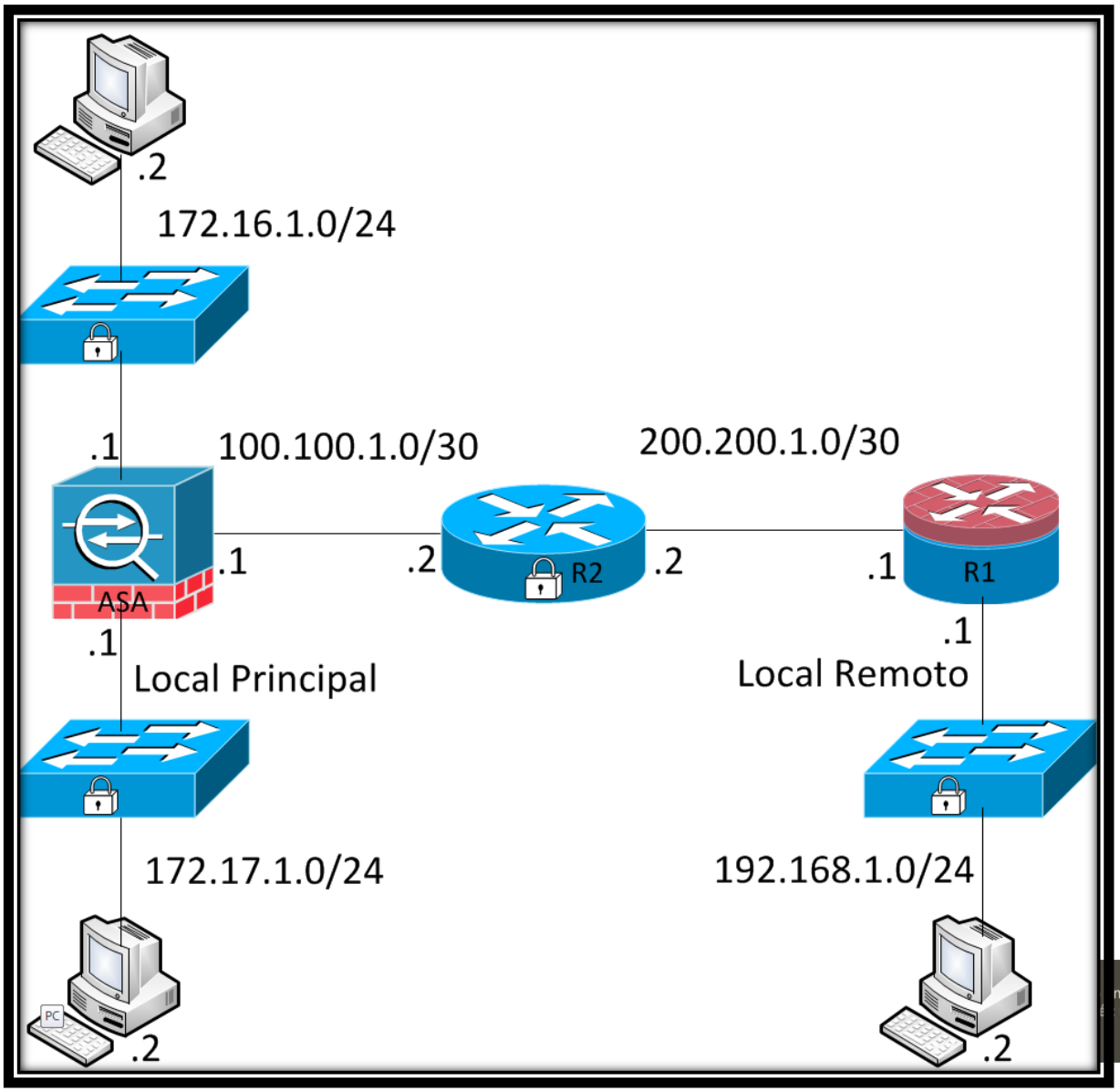
Fuente: Elaboración Propia

Diagrama 9: Diagrama Contextual del Sistema Criptográfico



Fuente: Elaboración Propia

Diagrama 10: Diagrama de topología del Sistema Criptográfico – Prototipo

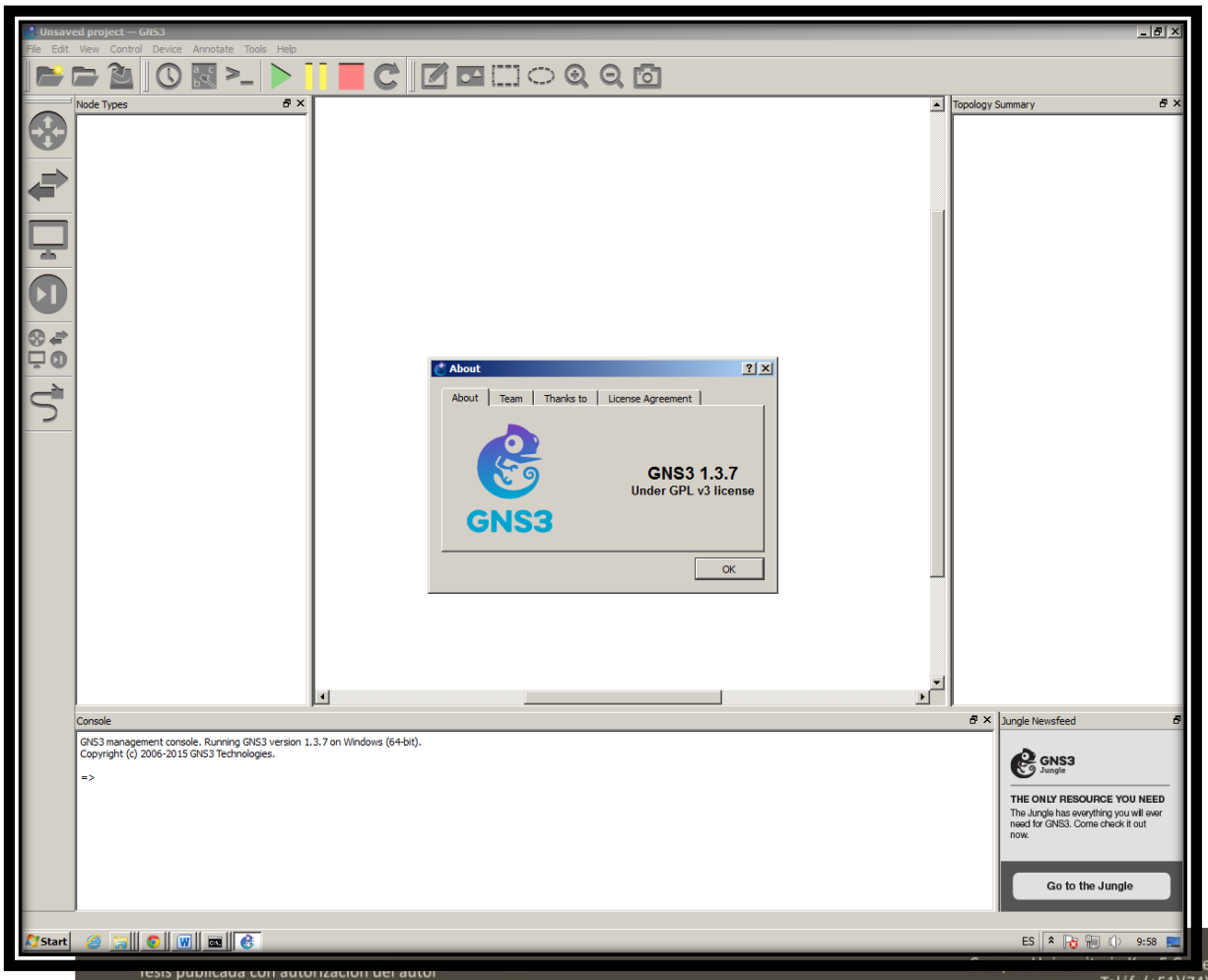


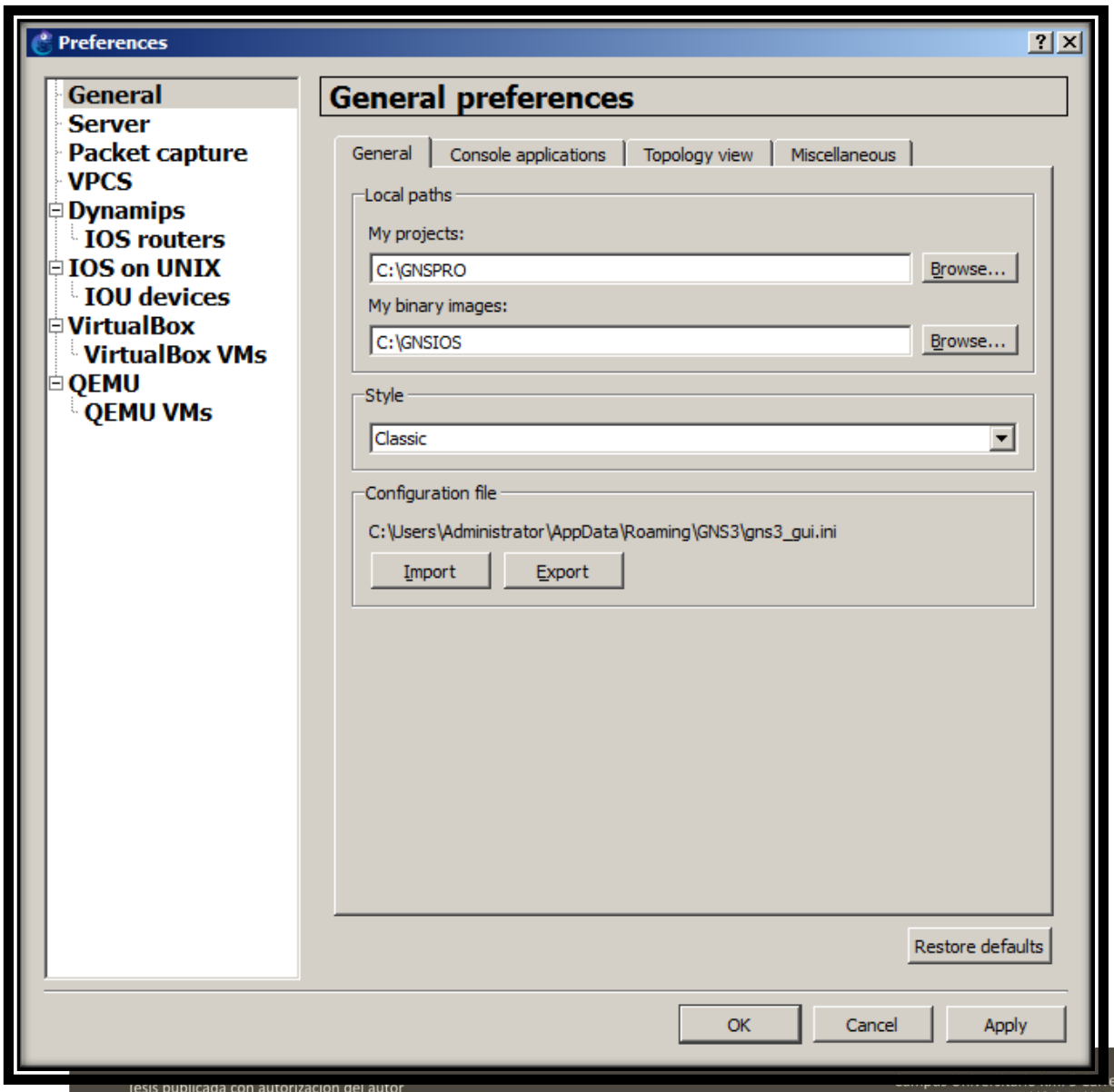
Fuente: Elaboración Propia

5.5 Implementación del Sistema Criptográfico - Prototipo

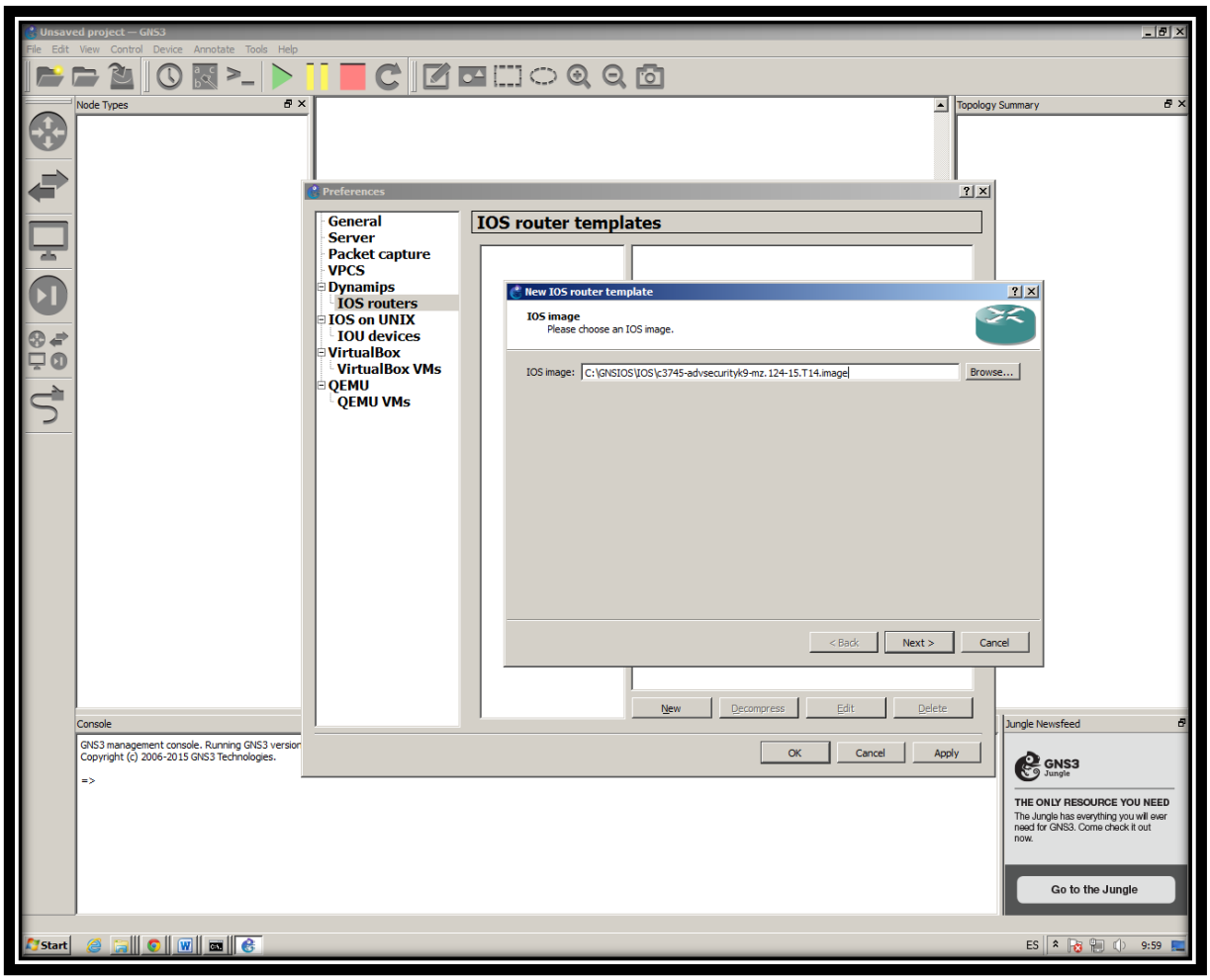
Instalamos el GNS3 1.3.7 y empezamos a configurarlo.

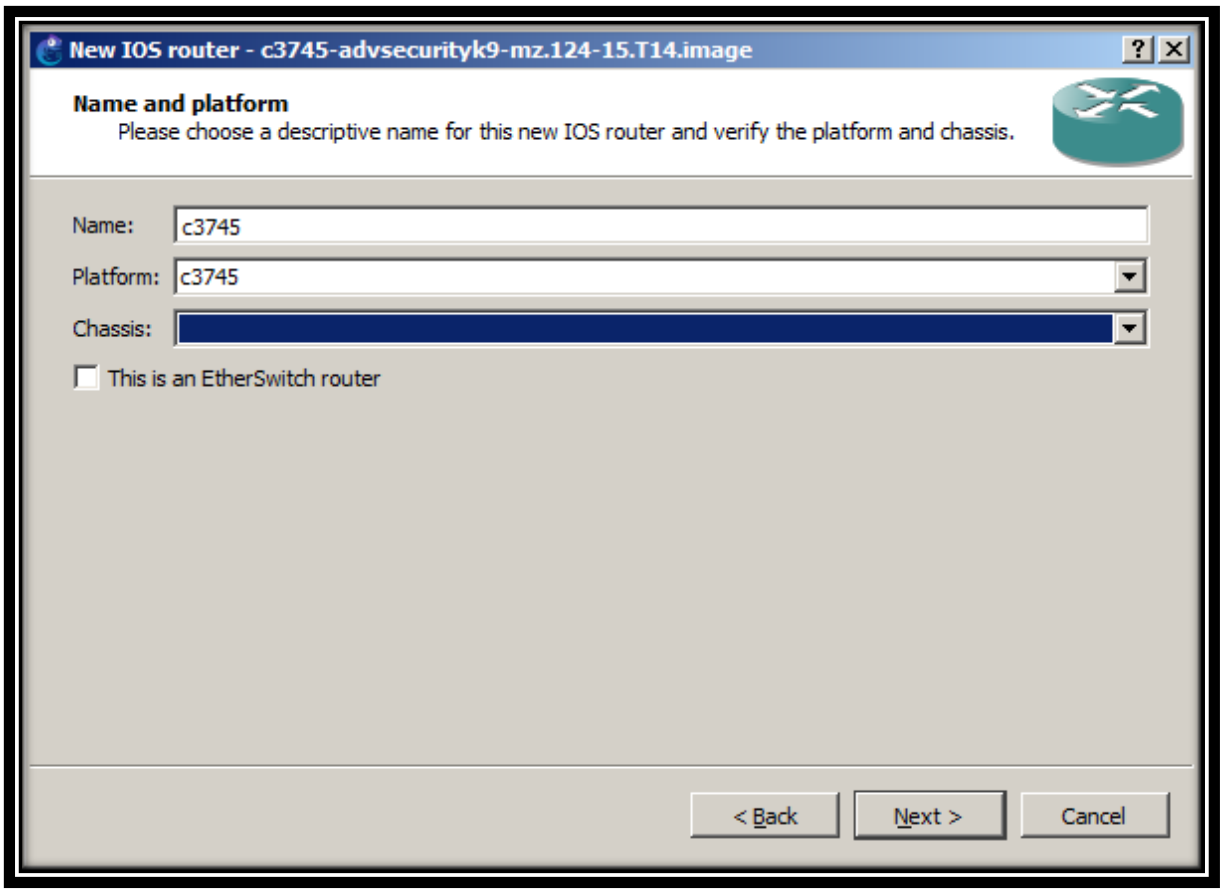
Primero configuramos IOS de Router.





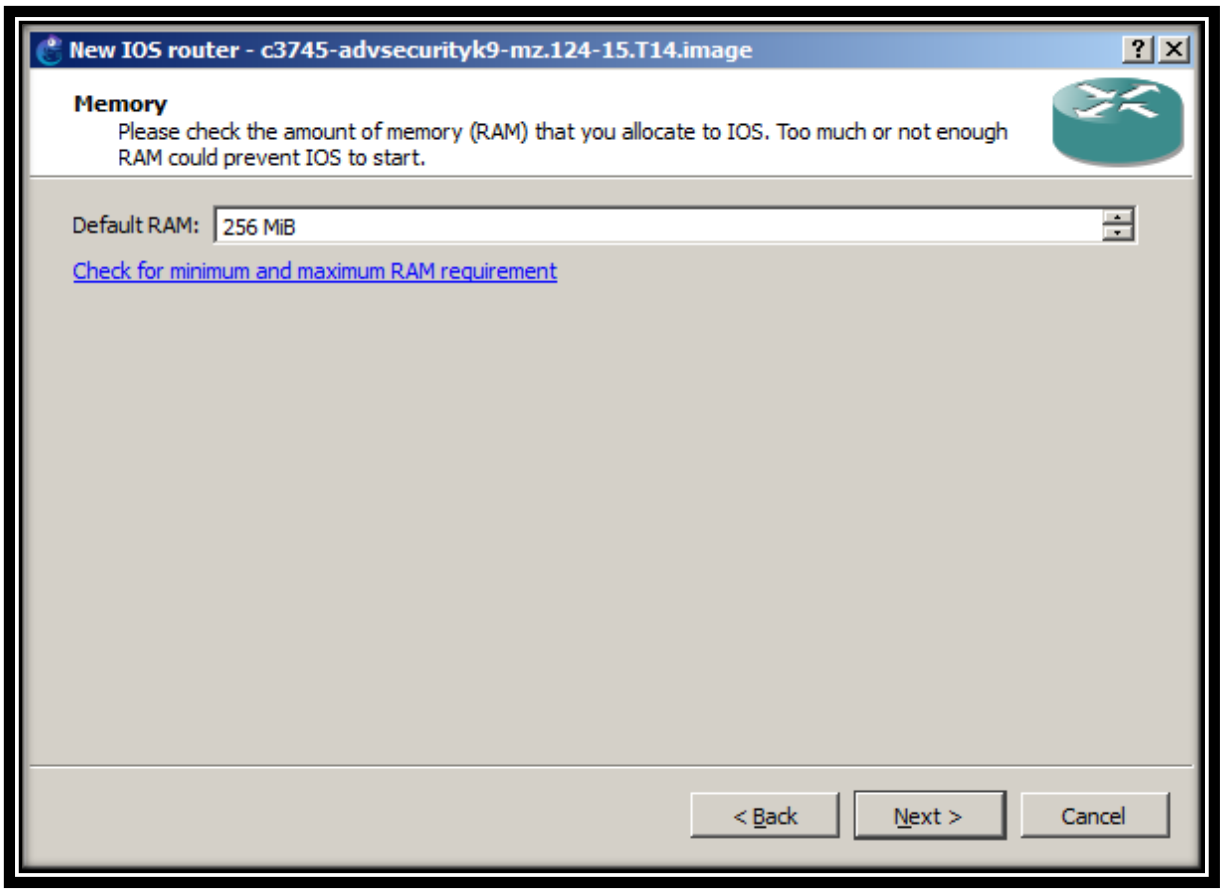
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

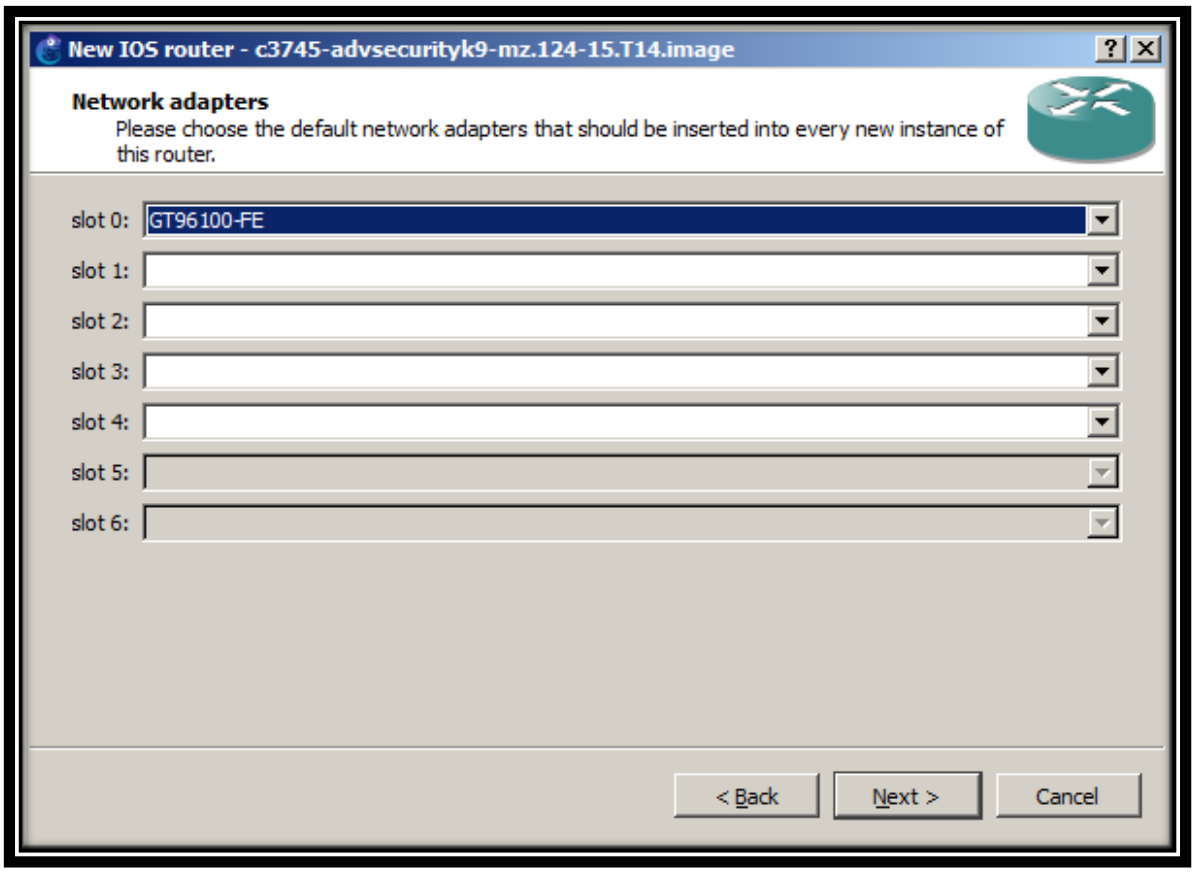


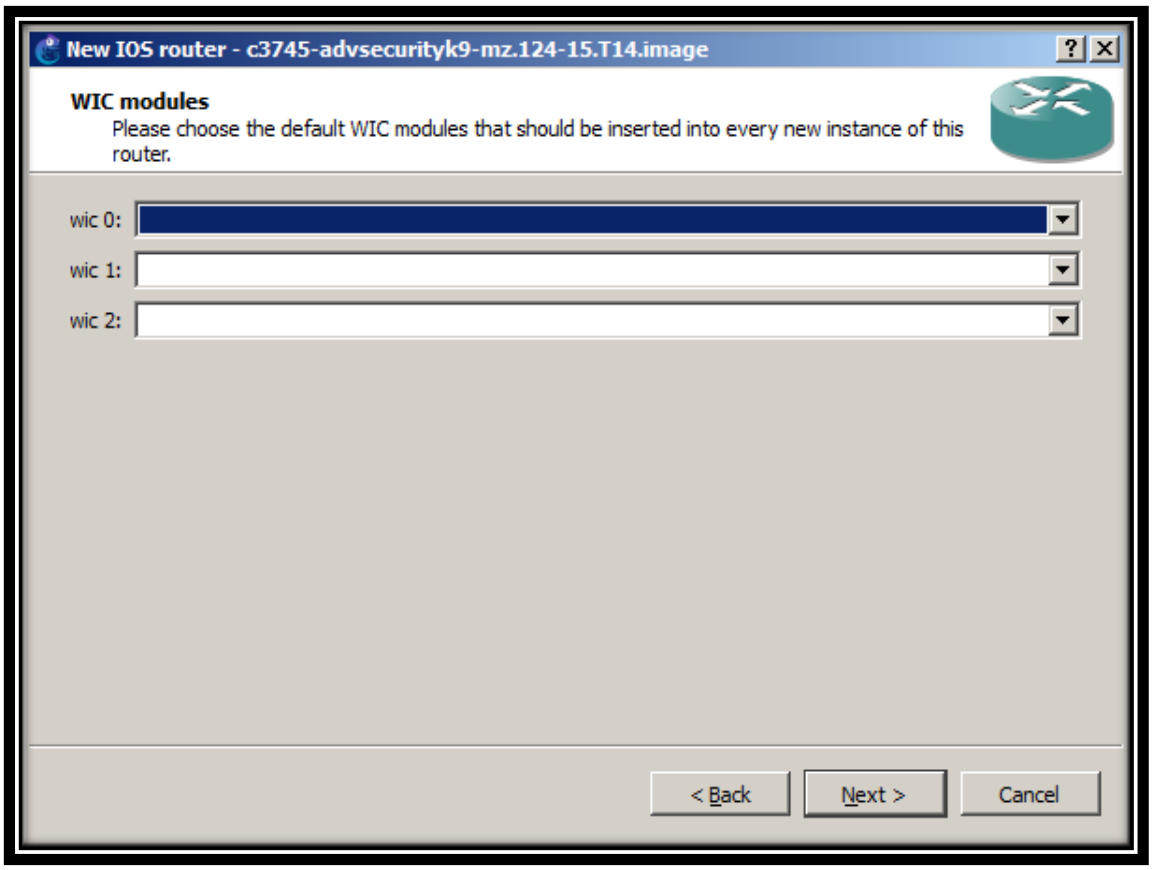


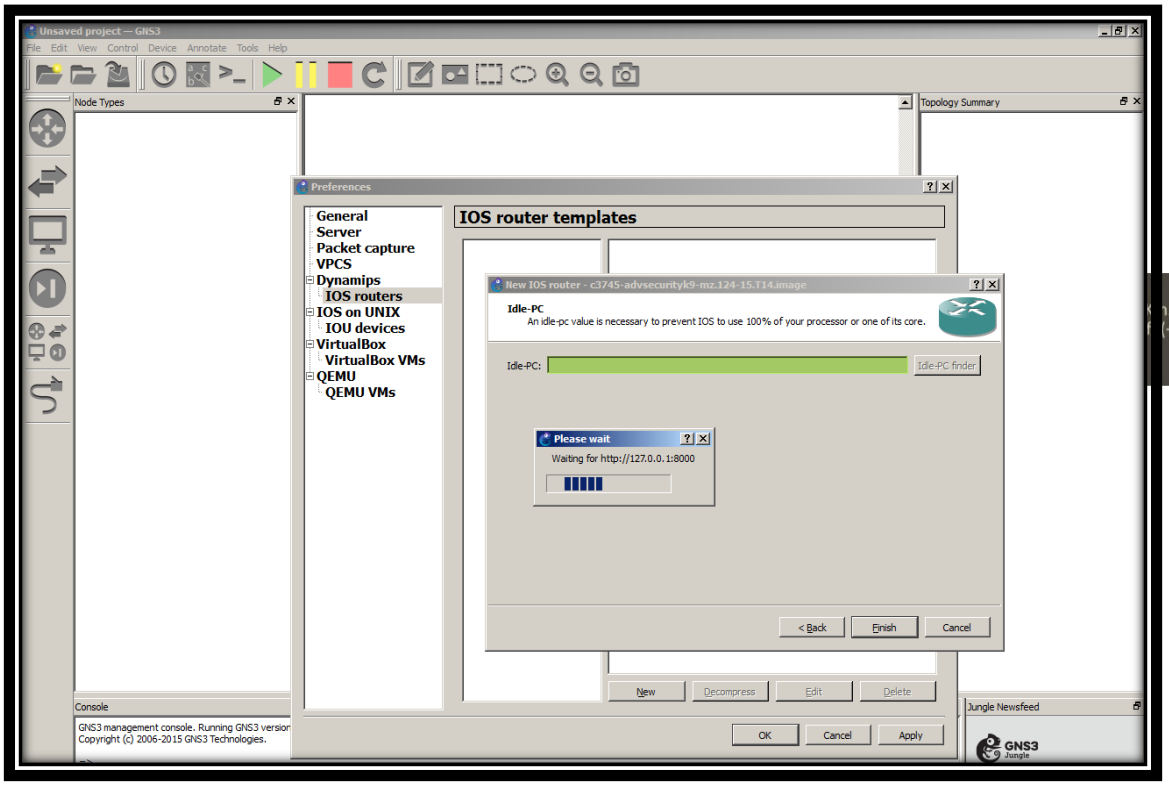
Campus Universitario Km. 5 Carretera a Pi
Teléf: (+51)(74) 481610

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

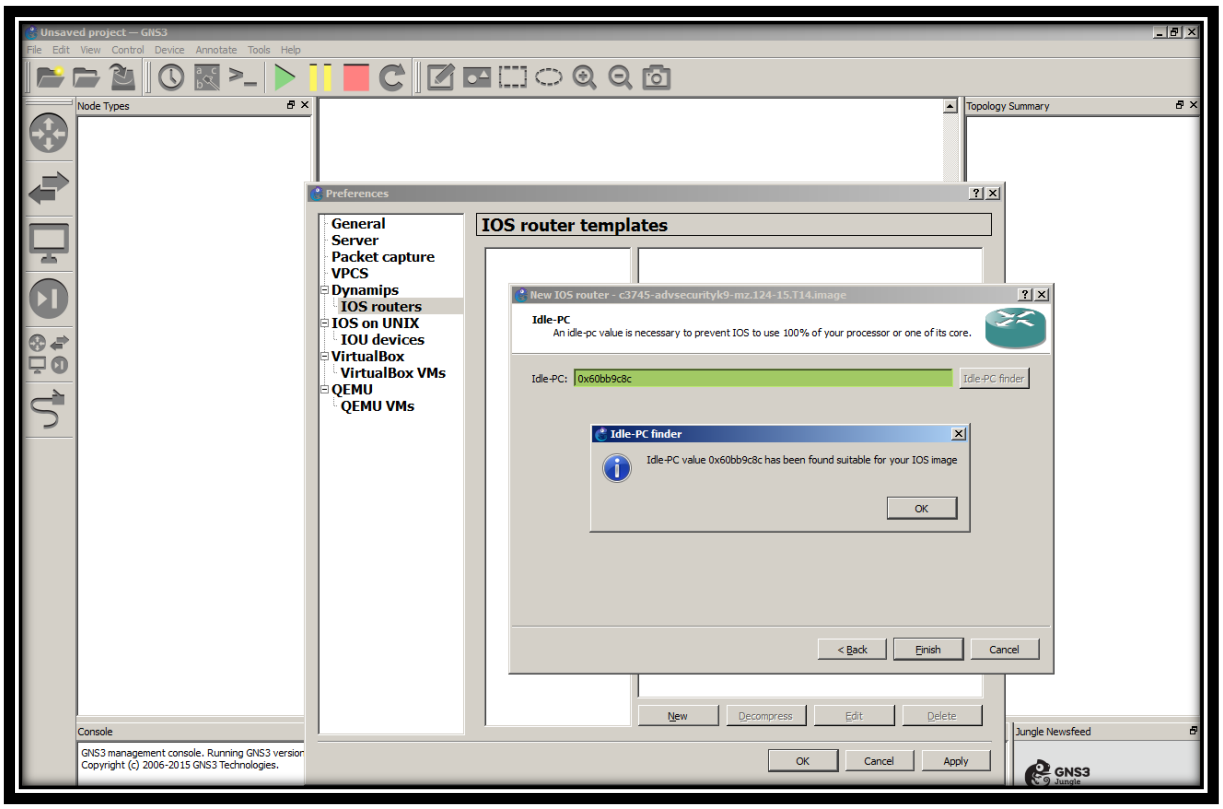


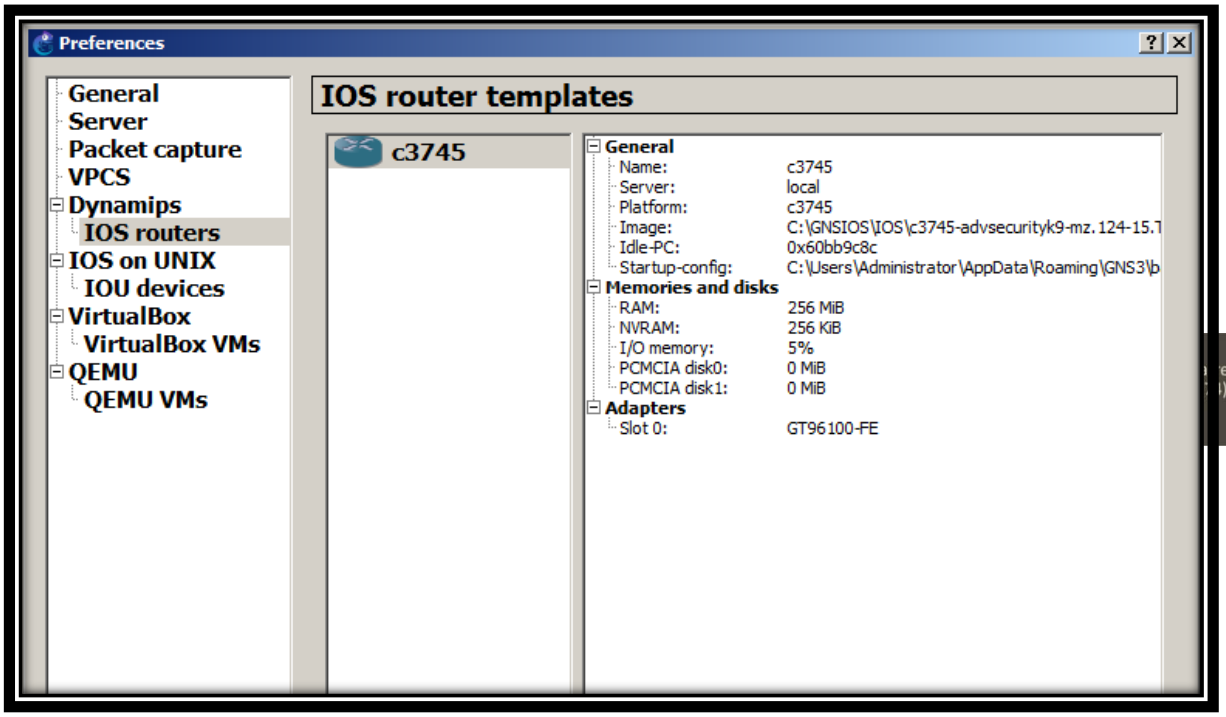




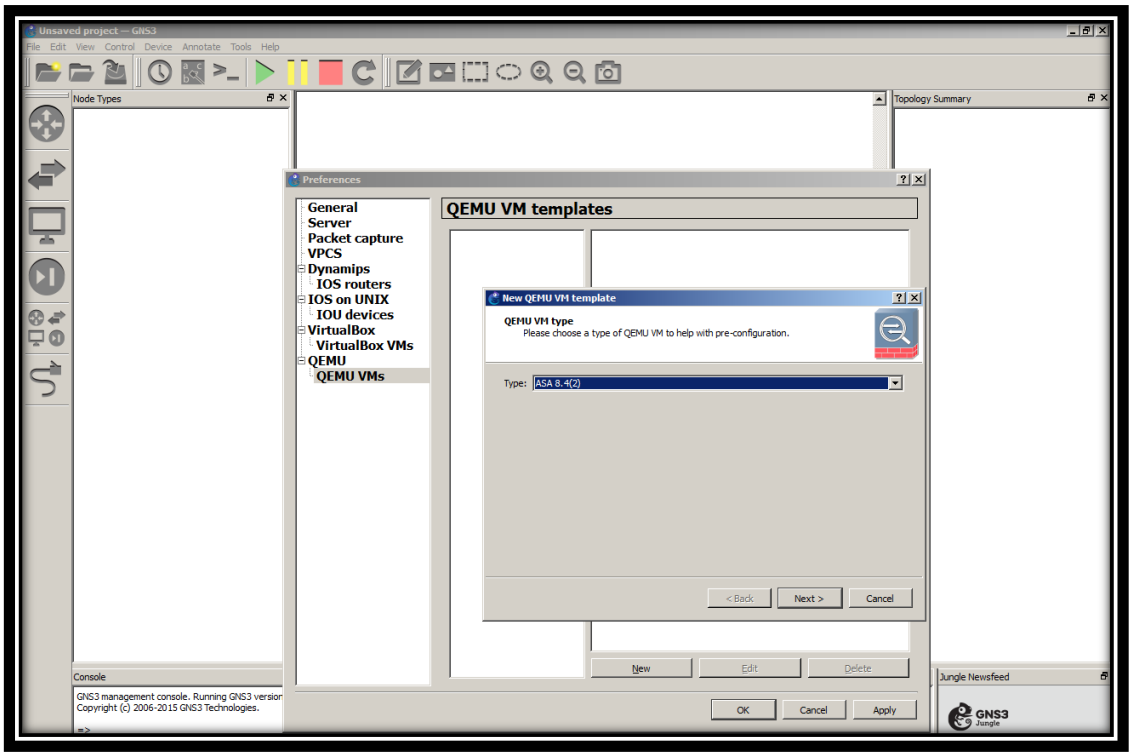


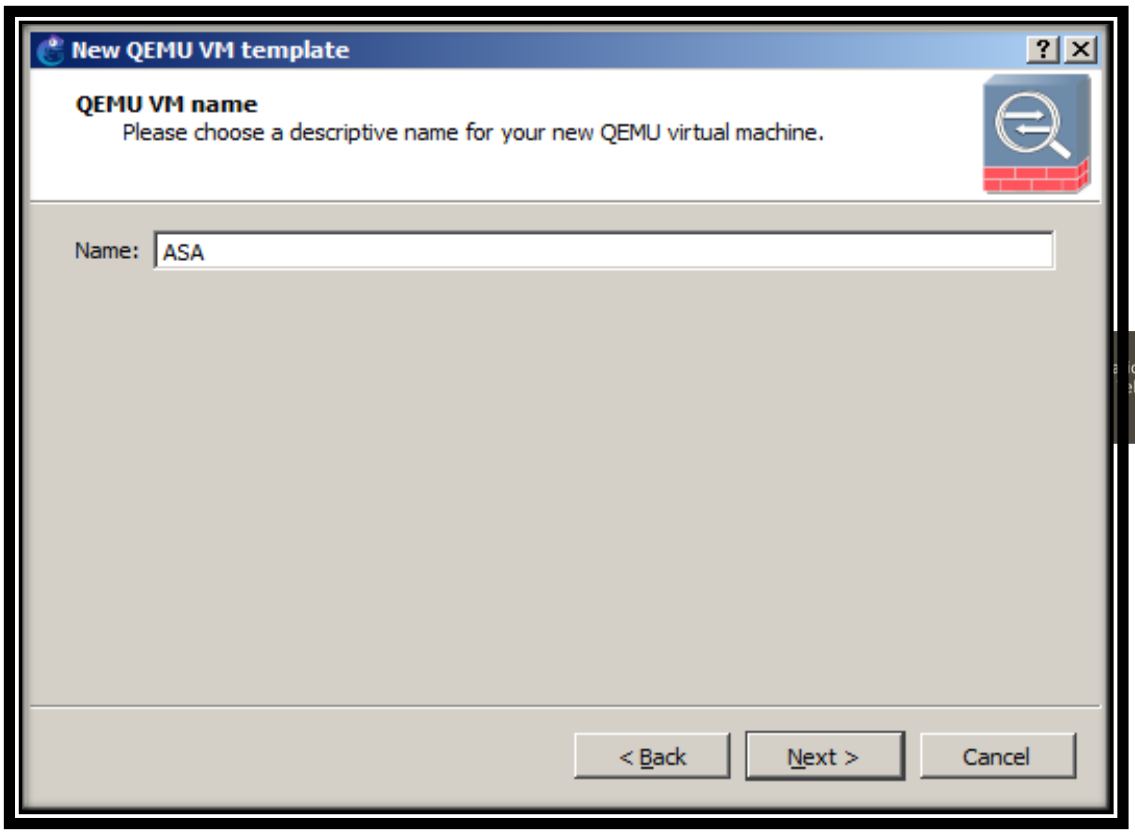
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe



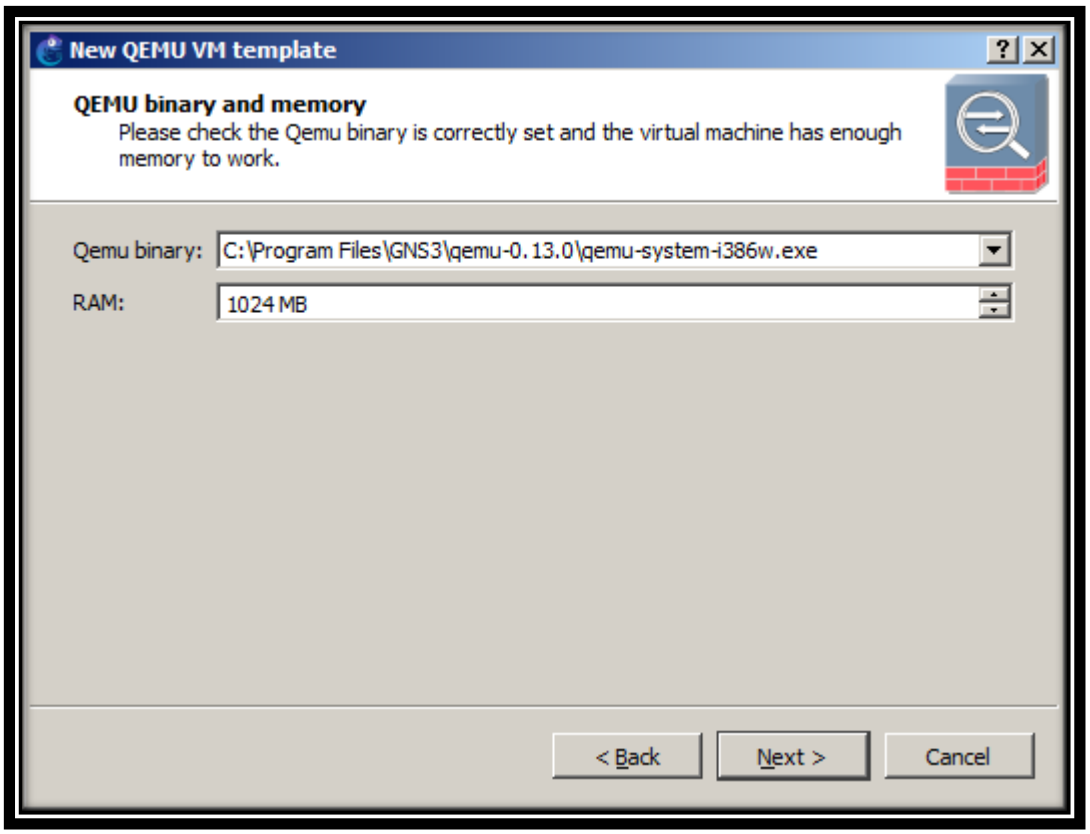


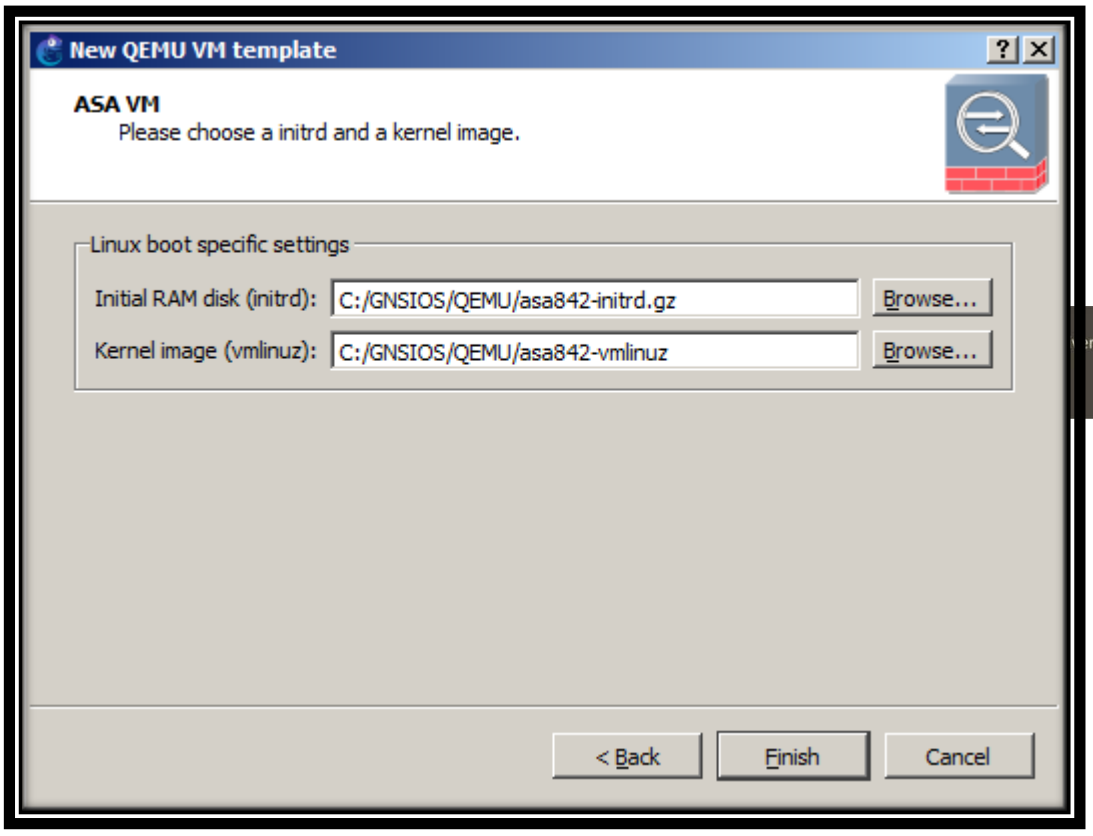
Configuramos IOS de Cisco ASA





Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe





Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Configurando FLASH para Cisco ASA, a través de la consola de Windows.

C:\Users\Administrator>cd..

C:\Users>cd..

C:\>cd "Program Files"

C:\Program Files>cd GNS3

C:\Program Files\GNS3>cd qemu-2.2.0

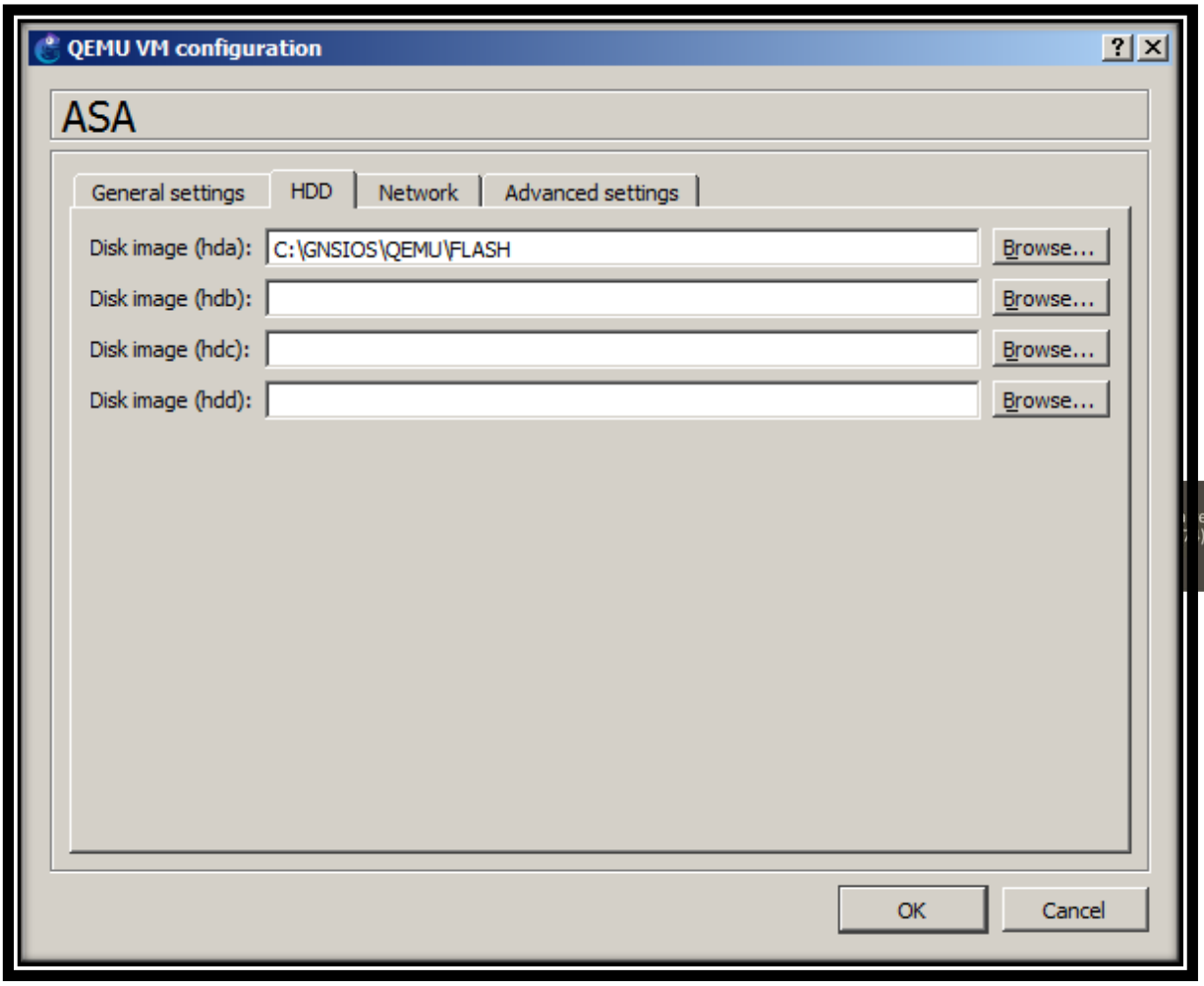
C:\Program Files\GNS3\qemu-2.2.0>qemu-img create FLASH 512M

Formatting 'FLASH', fmt=raw size=536870912

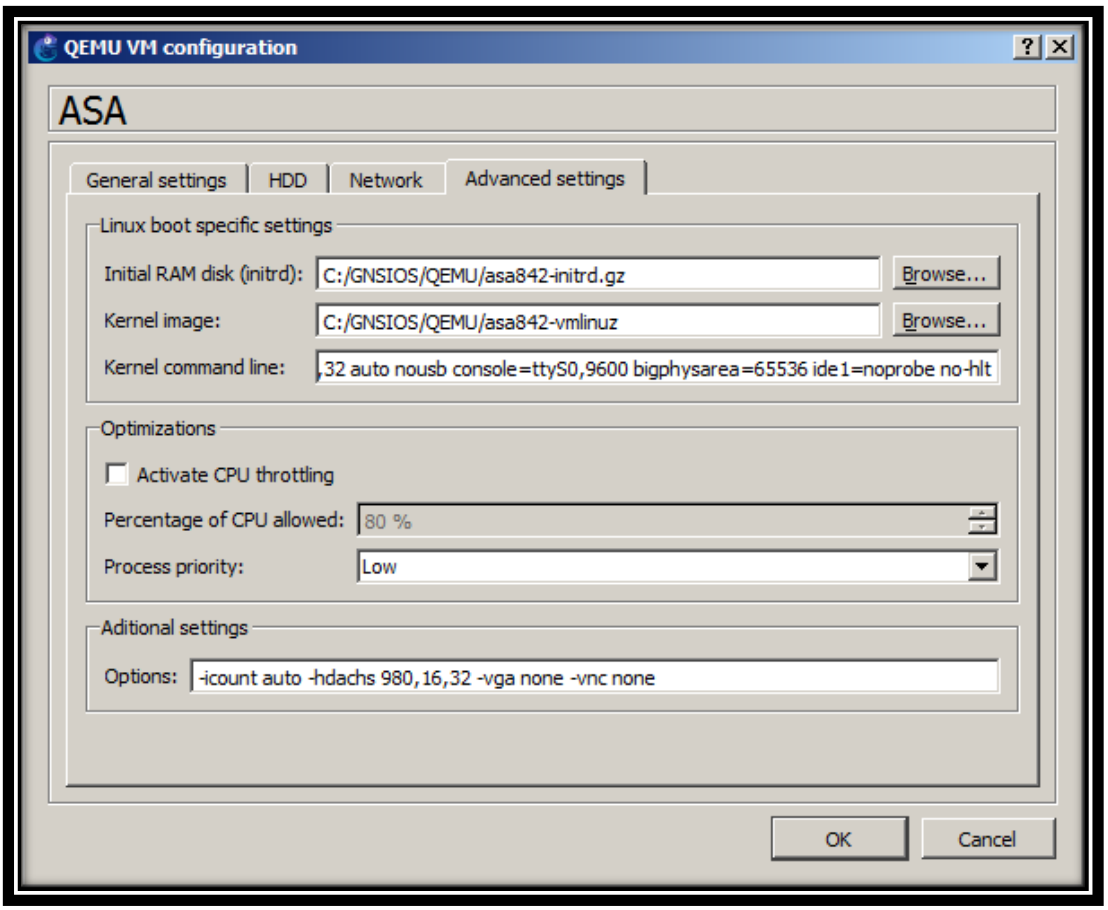
Free space 34406391808

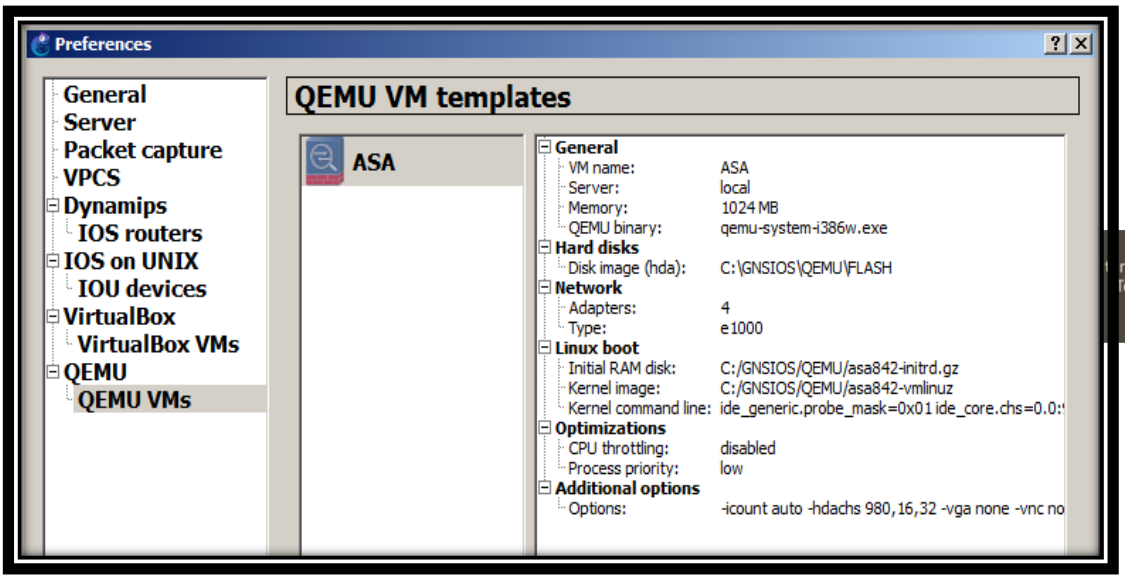
C:\Program Files\GNS3\qemu-2.2.0>

Luego agregamos FLASH creada.



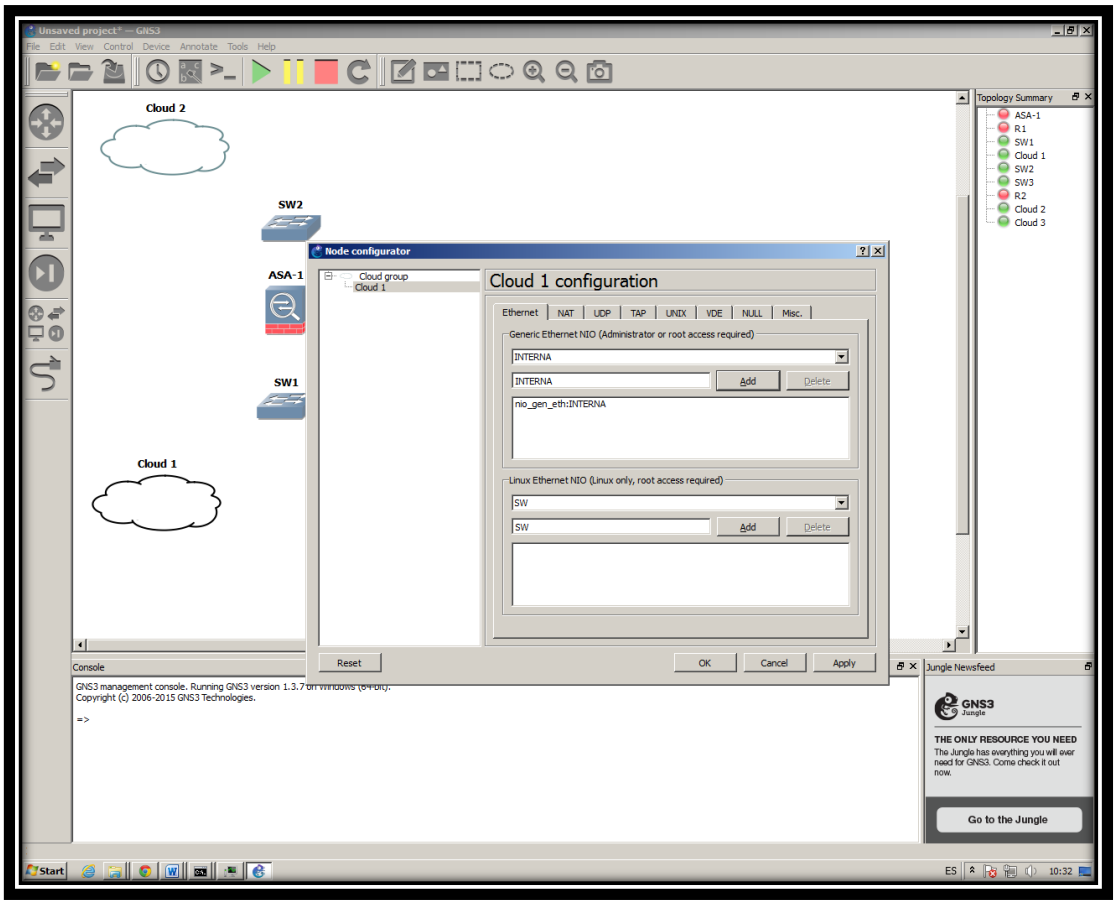
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe





Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Implementation de Topología



Configuración de Cisco ASA

ciscoasa(config)#

ciscoasa(config)# inter gigabit Ethernet 0

ciscoasa(config-if)# ip add 172.17.1.1 255.255.255.0

ciscoasa(config-if)# name if inside

INFO: Security level for "insisde" set to 100 by default.

ciscoasa(config-if)# no shu

ciscoasa(config-if)# exit

ciscoasa(config)# inter gigabit Ethernet 1

ciscoasa(config-if)# ip add 100.100.1.1 255.255.255.0

ciscoasa(config-if)# name if outside

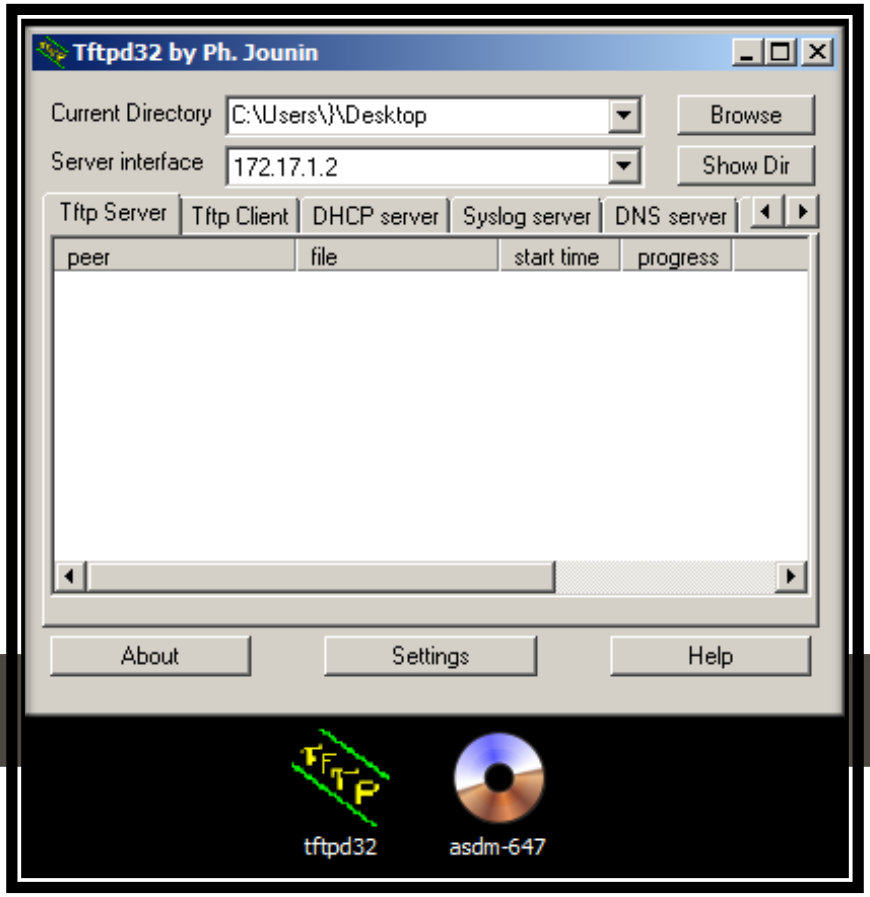
INFO: Security level for "outside" set to 0 by default.

ciscoasa(config-if)# no shut

ciscoasa(config-if)# exit

ciscoasa(config)# exit

Bueno, ahora el siguiente paso es copiar ASDM Firewall. Si ya tiene instalado el servidor TFTP. Sino descargar de http://tftpd32.jounin.net/tftpd32_download.html. También descargar ASDM 6.4(7) de Cisco.



ciscoasa# copy tftp: flash:

Address or name of remote host []? 172.17.1.2

Source filename []?asdm-647.bin

Destination filename [asdm-647.bin]?

Accessing tftp://172.17.1.2/asdm-

647.bin...!!

!!!

!!!!!!!!!!!!!

17902288 bytes copied in 37.870 secs (483845 bytes/sec)

ciscoasa# confter

ciscoasa(config)# asdm image flash:/asdm-647.bin

ciscoasa(config)# http server enable

ciscoasa(config)# http 172.17.1.2 255.255.255.255 inside

ciscoasa(config)# username cisco password cisco privilege 15

ciscoasa(config)# q

ciscoasa# cop run sta

Source filename [running-config]?

Cryptochecksum: b45087c7 7df5271f dd44f740 5d872fa0

2225 bytes copied in 0.450 secs

ciscoasa# cop sta disk0:

Destination filename [startup-config]?

Copy in progress...C

2225 bytes copied in 0.10 secs

ciscoasa# wr

Building configuration...

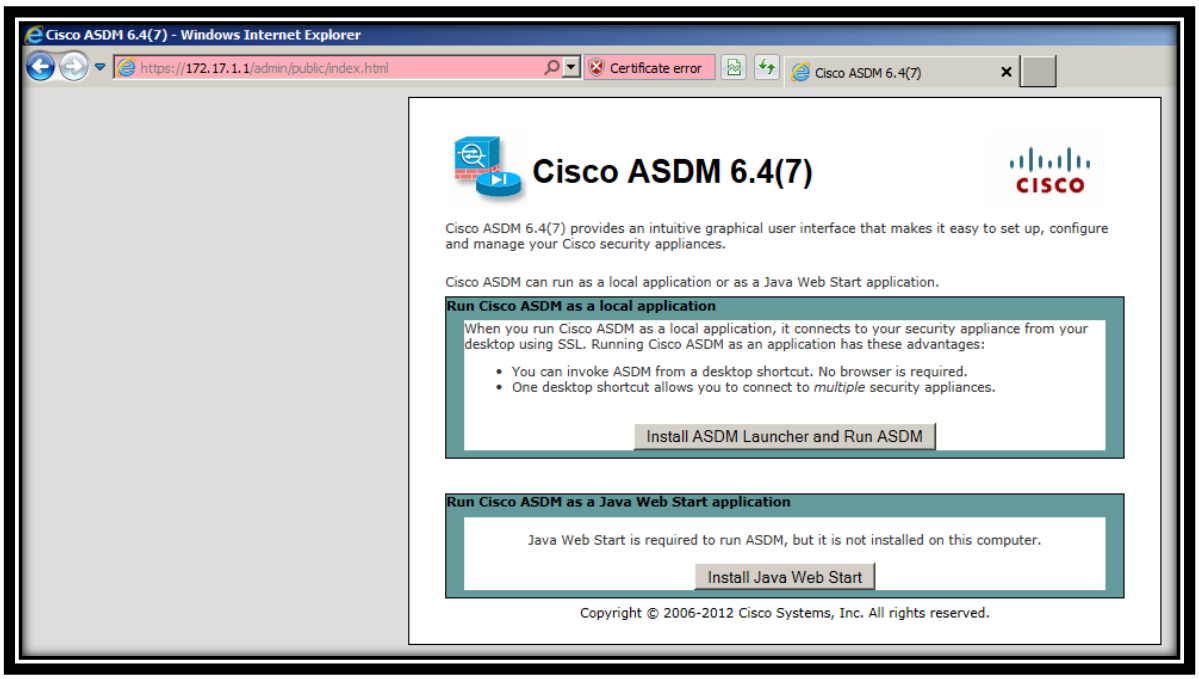
Cryptochecksum: b45087c7 7df5271f dd44f740 5d872fa0

2225 bytes copied in 0.380 secs

[OK]

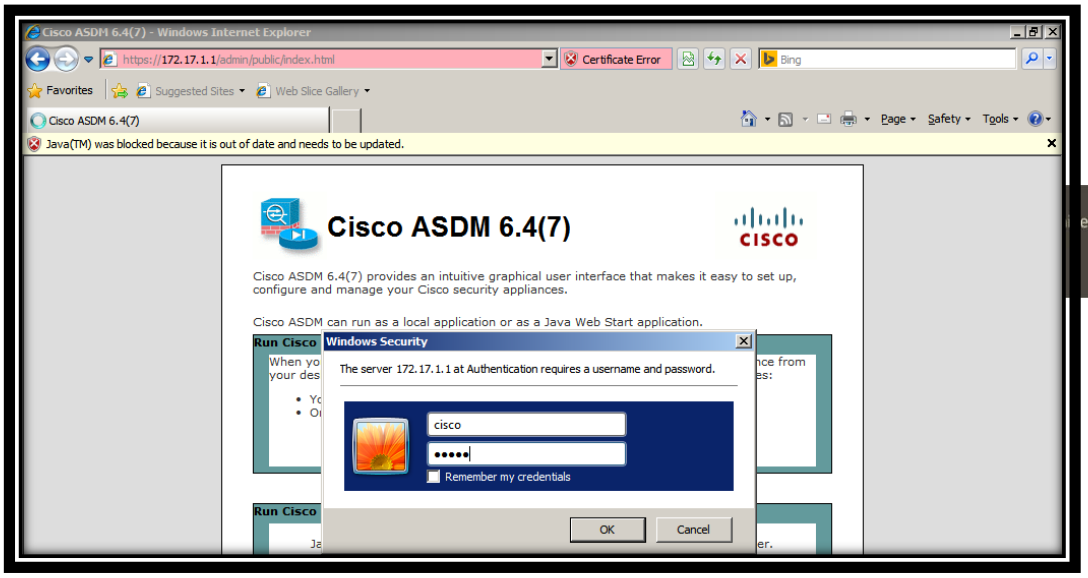
ciscoasa#

Abrimos en navegador https://172.17.1.1 e instalamos el ASDM en nuestra PC

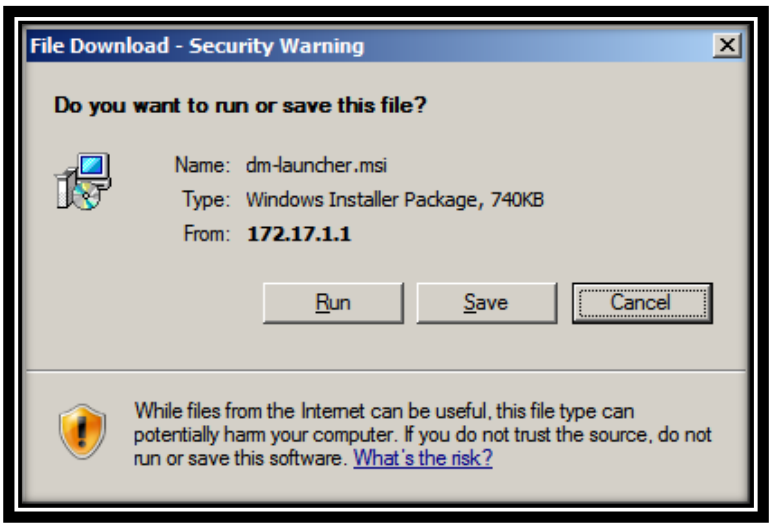


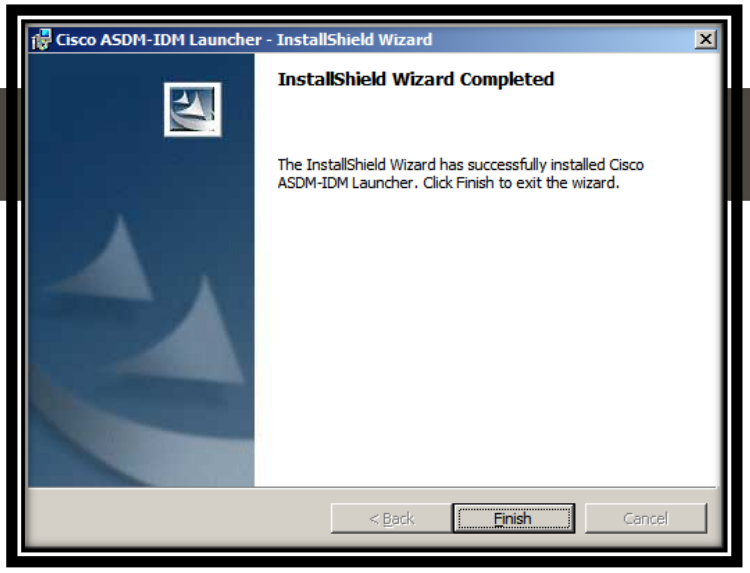
Click en Continue to this website ()

Ingresamos Credenciales: user: **cisco**, pass: **cisco**



Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe



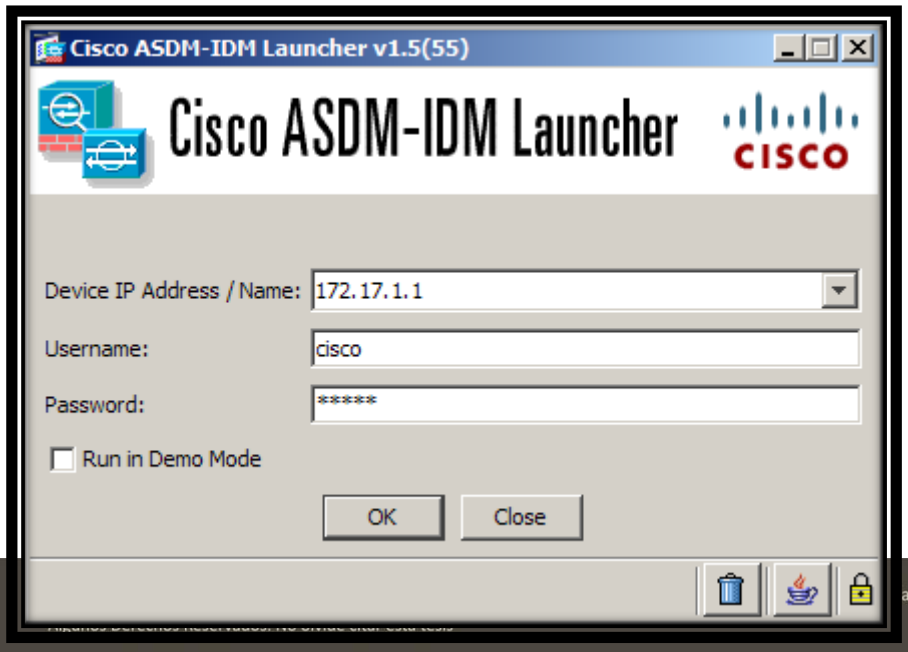


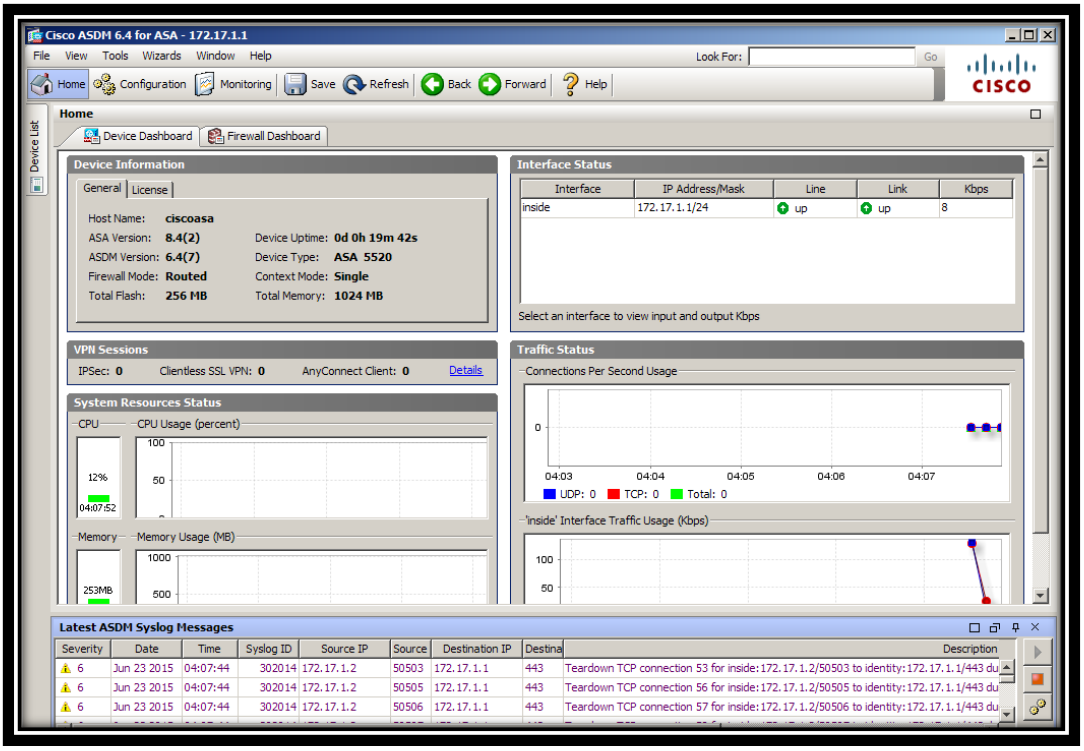
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En el escritorio aparecerá el siguiente icono.

Darle doble Click. Luego Ingresar Dirección IP de Cisco ASA y credenciales.

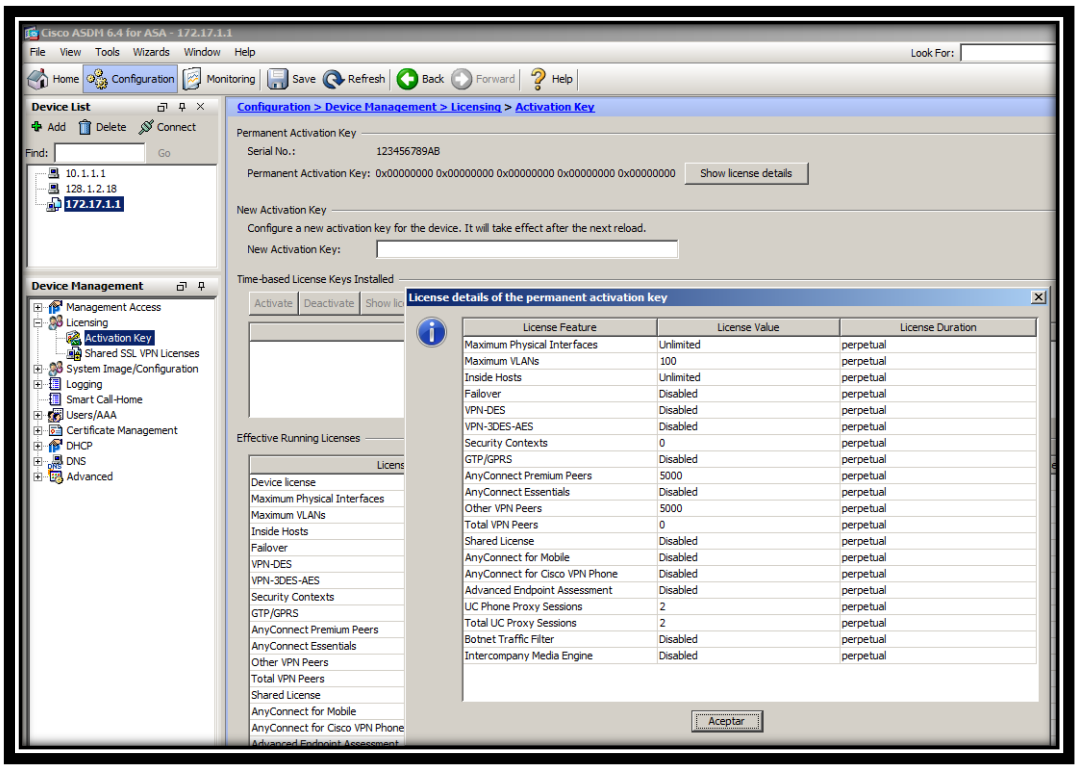
Doble Click. Luego Ingresar Dirección IP de Cisco ASA y credenciales.





Activar las licencias para seguridad como FAILOVER, VPN, ALGORITOOS CRYPTOGRAFICOS, COMUNICACIONES UNIFICADAS, etc.

Antes

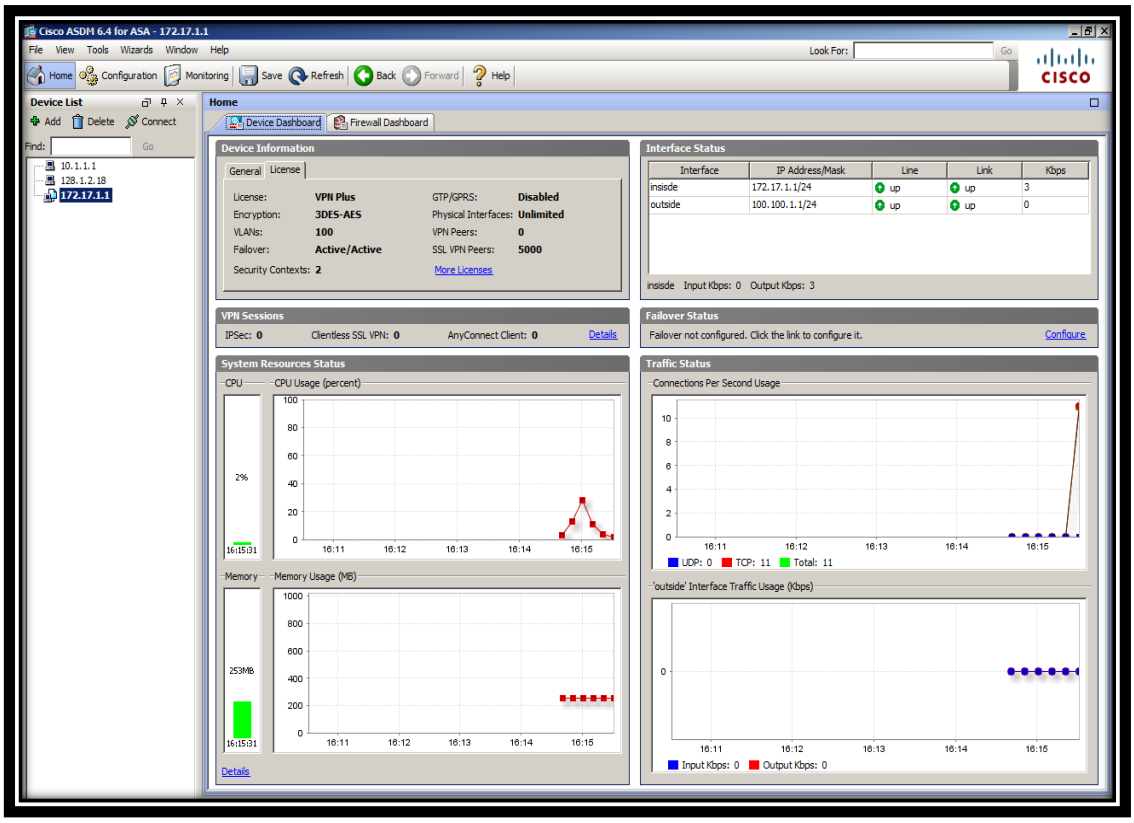


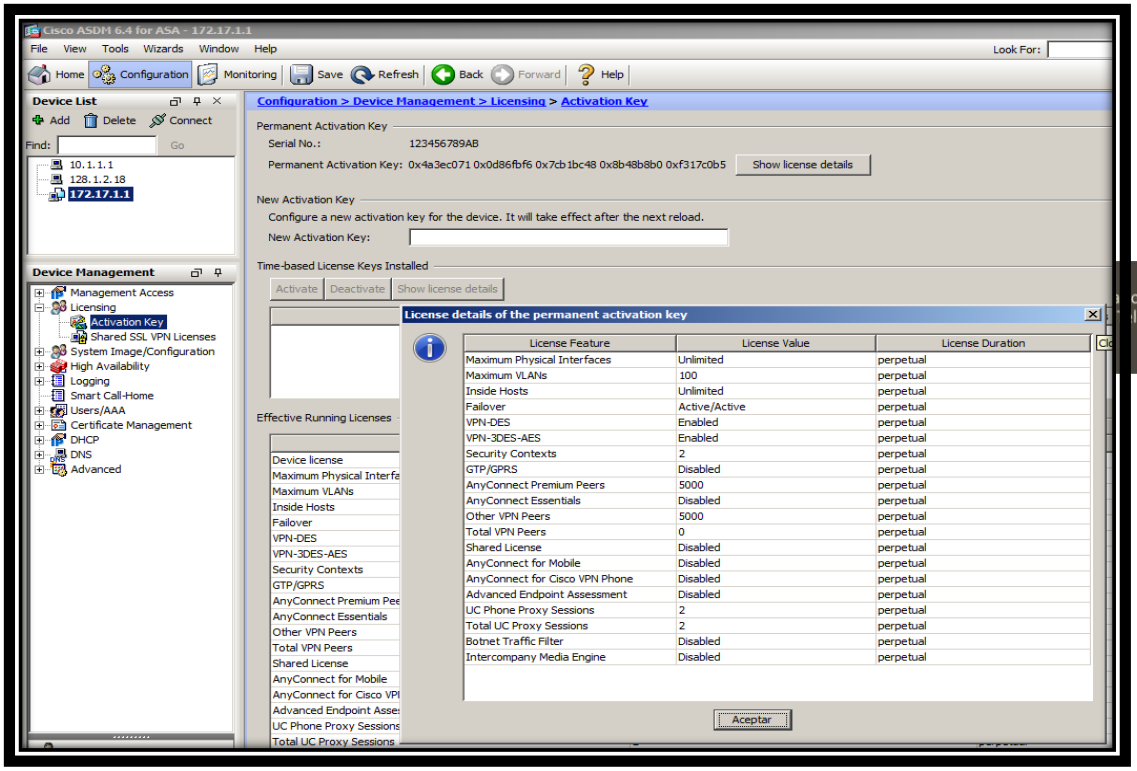
Aplicando las licencias:

```
activation-key 0x4a3ec071 0x0d86fbf6 0x7cb1bc48 0x8b48b8b0 0xf317c0b5

activation-key 0xb23bcf4a 0x1c713b4f 0x7d53bcbc 0xc4f8d09c 0x0e24c6b6
```

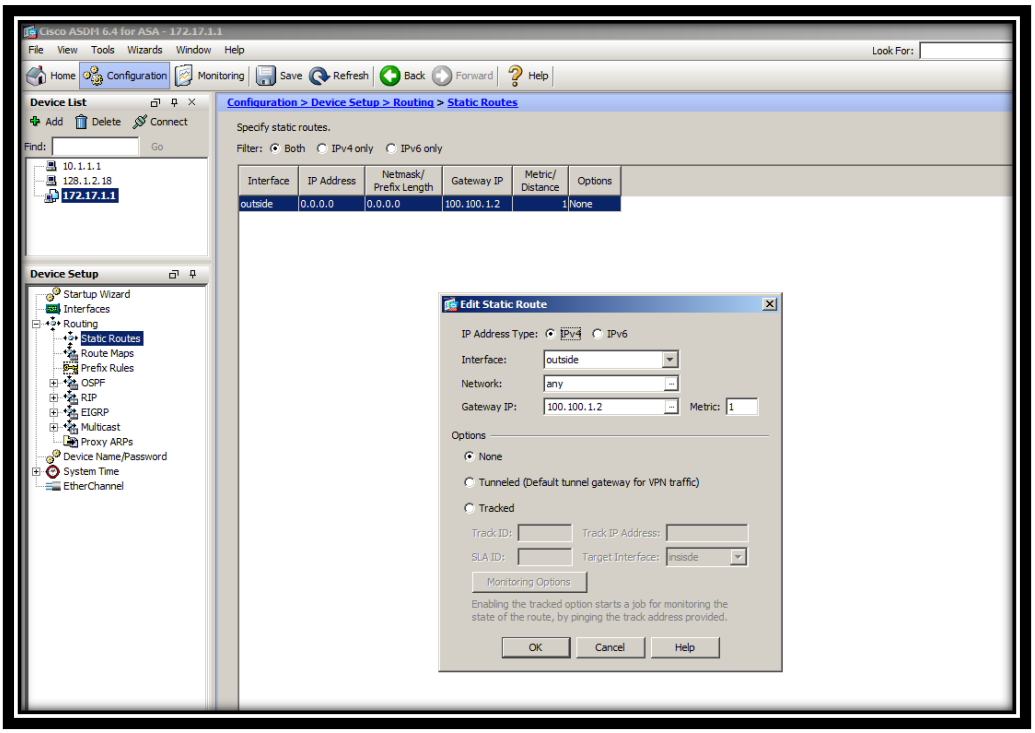
Para instalar la segunda licencia tenemos que esperar 15 minutos a mas, reiniciar el ASA en ambos casos y listo.

Después





Configuración de Ruta estática



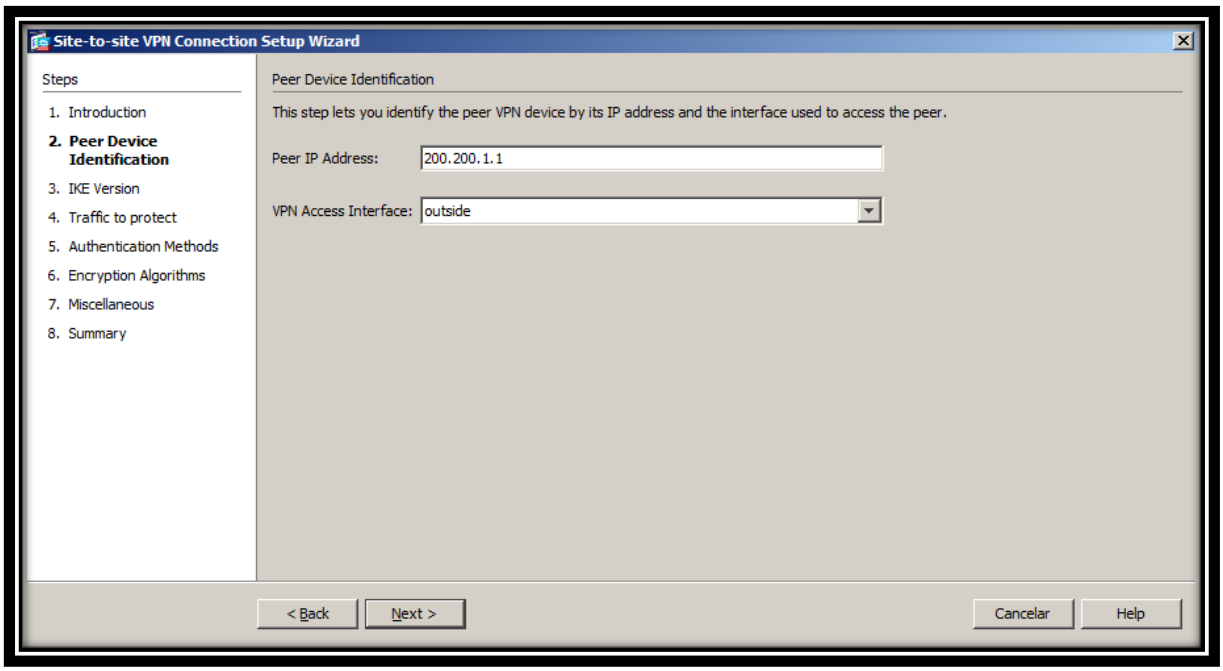
Configuración de Router ISP

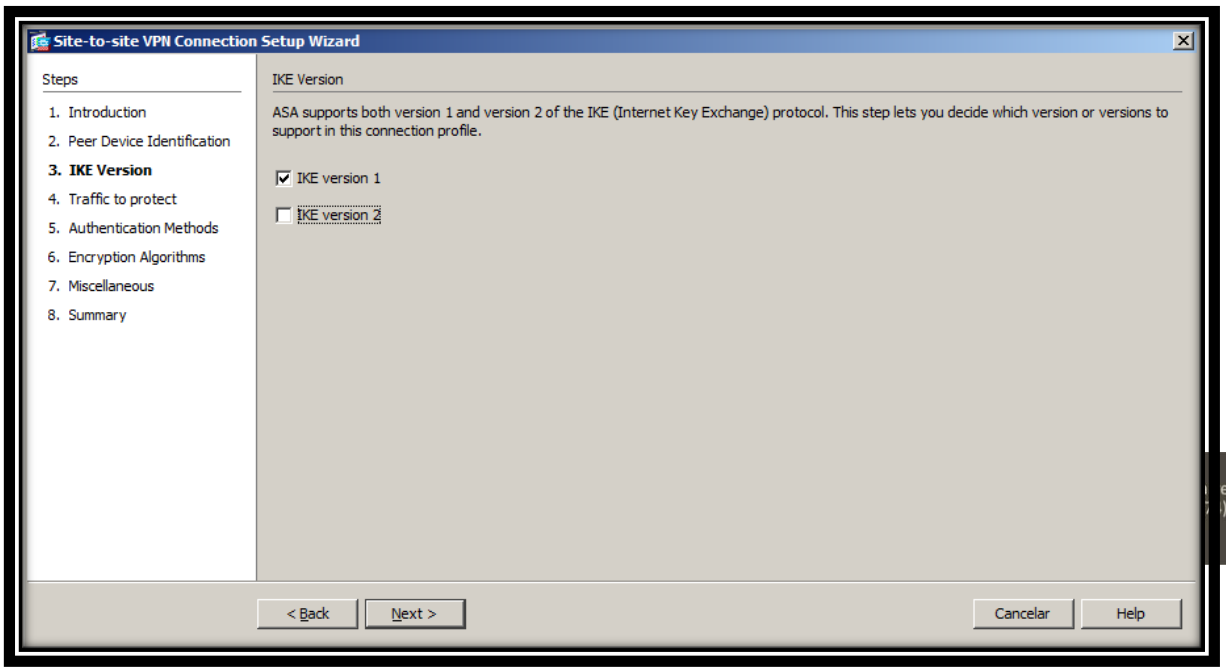
```
ISP#showip inter br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
ISP#confter
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#inter fas 0/0
ISP(config-if)#ip add 100.100.1.2 255.255.255.0
ISP(config-if)#no shu
ISP(config-if)#exit
ISP(config)#inter fas 0/1
ISP(config-if)#ip add 200.200.1.2 255.255.255.0
ISP(config-if)#no shu
ISP(config-if)#
ISP#wr
Building configuration...
changed state to up
ISP#
```

Configuración de Router Remoto R2

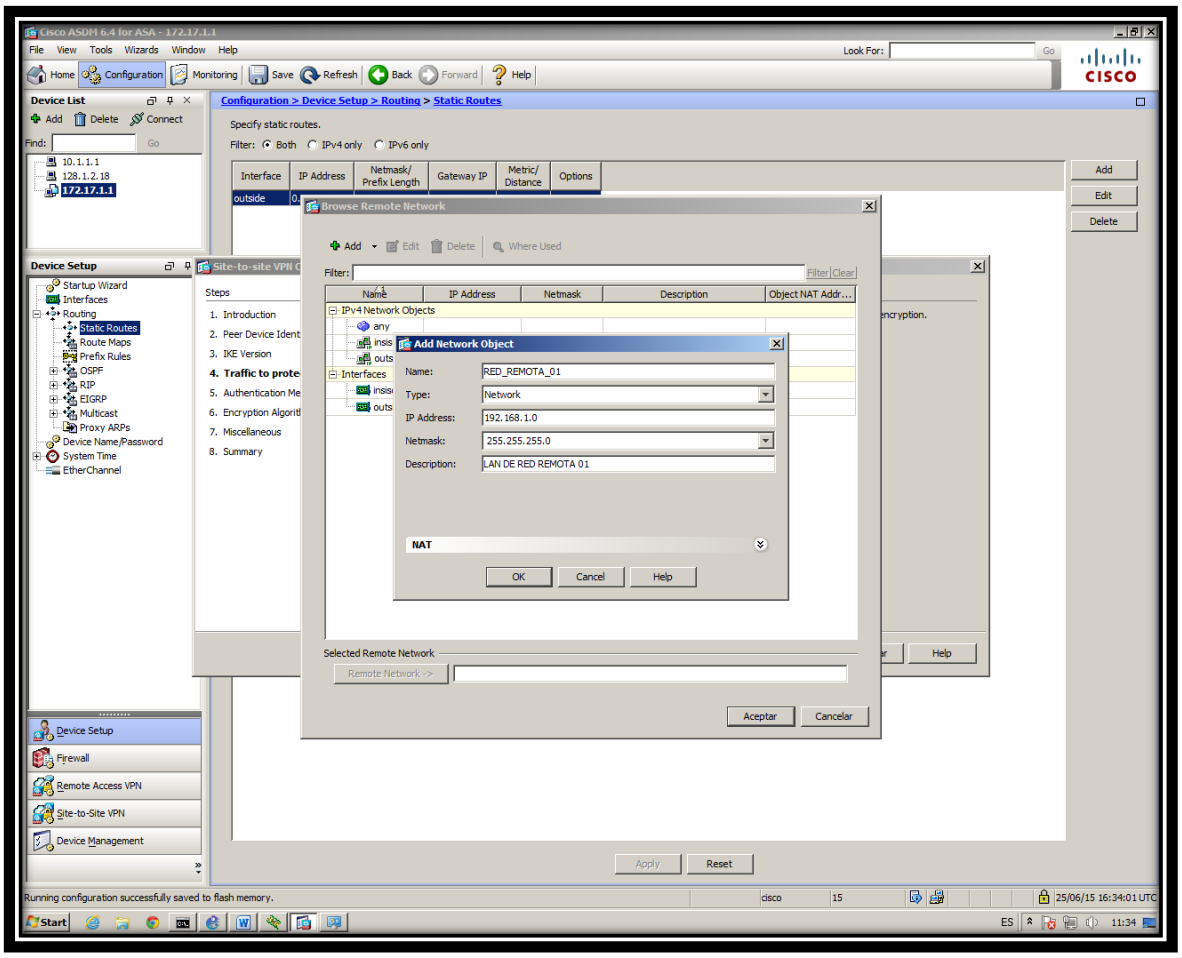
```
R2#show ip inter br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
R2#conf ter
R2(config)#inter fas 0/1
R2(config-if)#ip add 200.200.1.1 255.255.255.0
R2(config-if)#no shu
R2(config-if)#exit
R2(config)#inter fas 0/0
R2(config-if)#ip add 192.168.1.1 255.255.255.0
R2(config-if)#no shu
R2(config)#ip route 0.0.0.0 0.0.0.0 200.200.1.2
R2(config)#
R2#wr
Building configuration...
[OK]
```

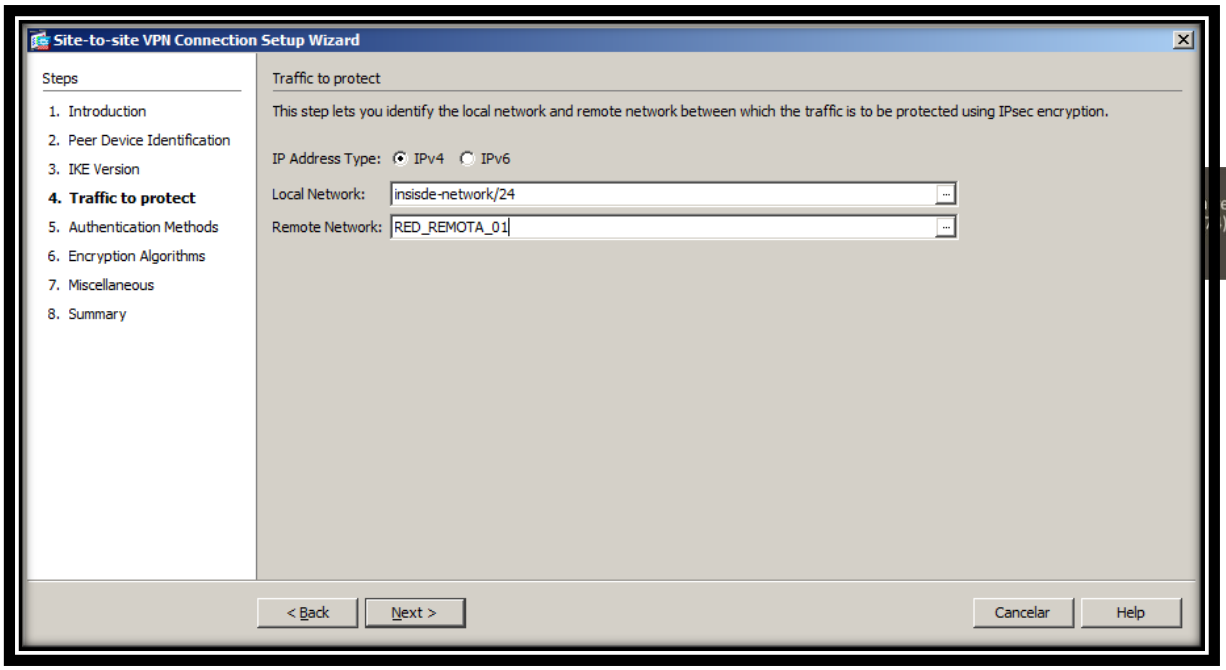
Configuración de Cisco ASA – Sistema Criptográfico





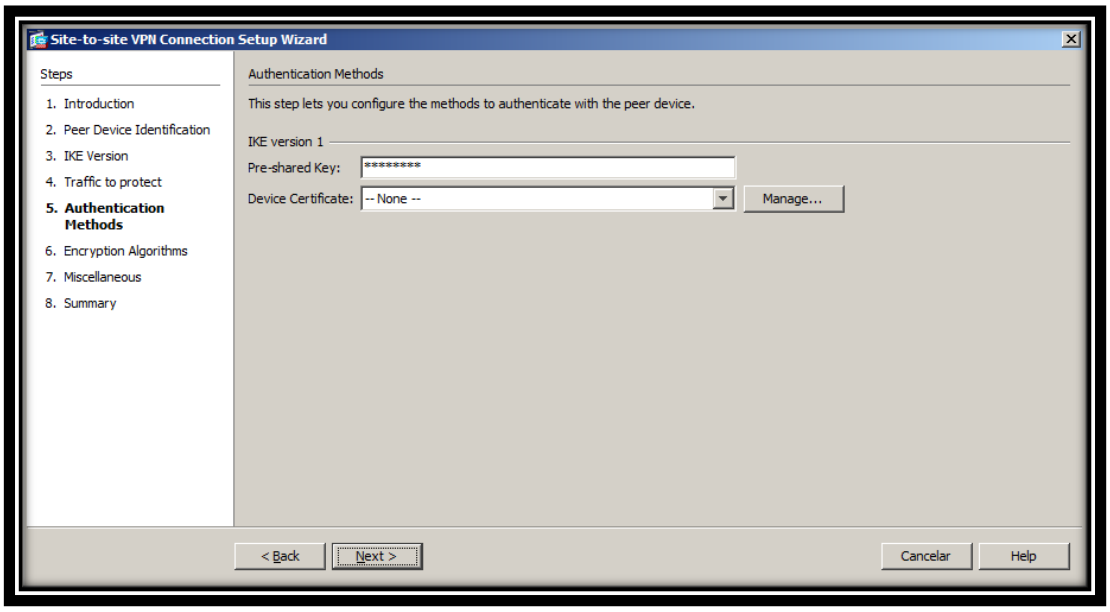
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe



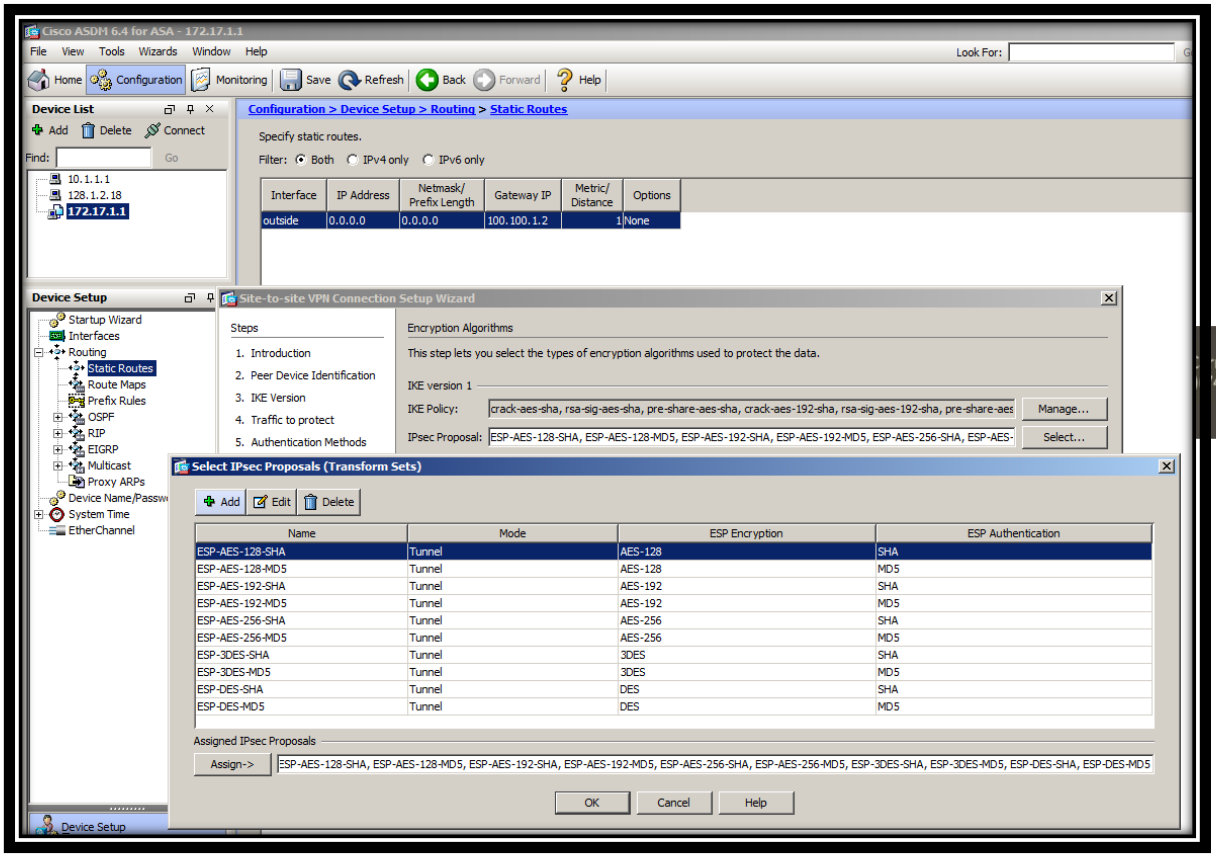


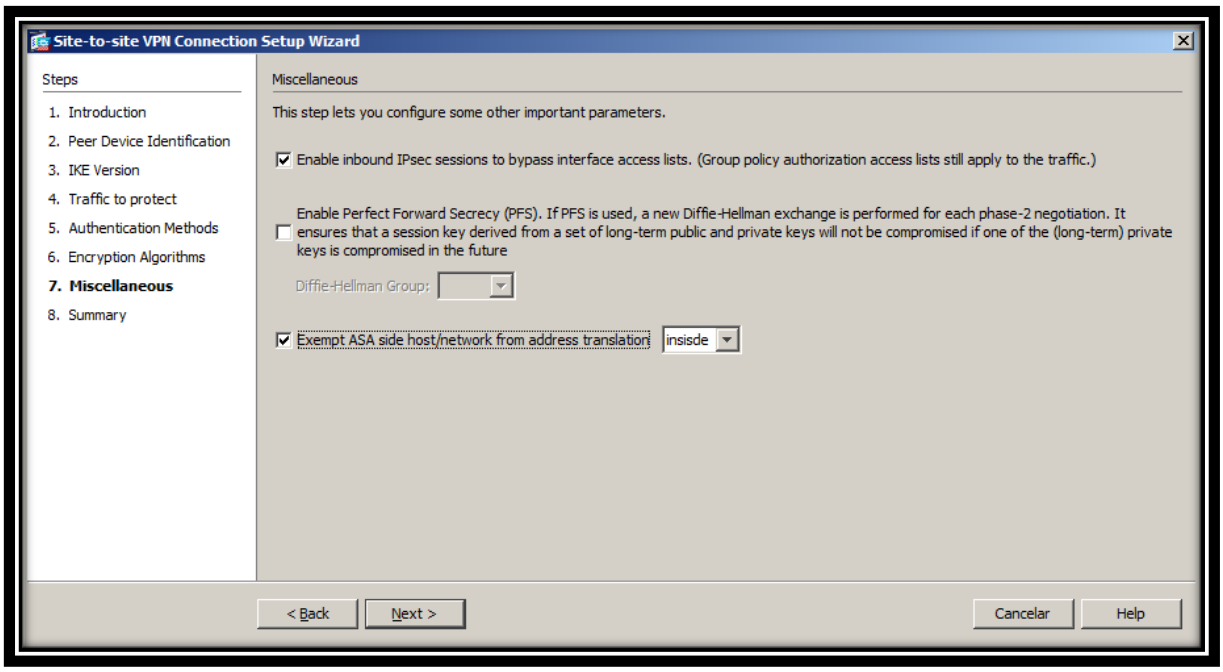
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

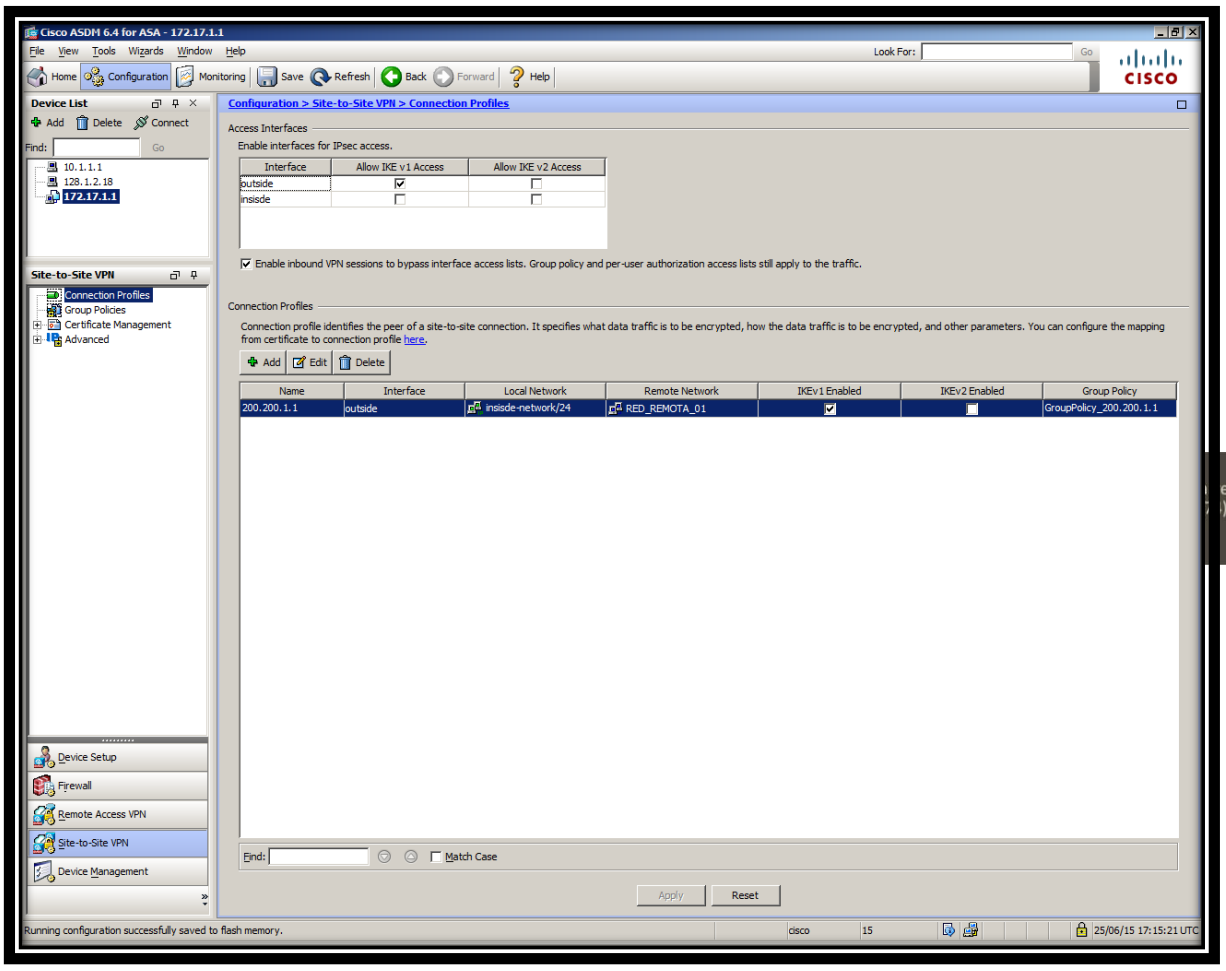
Pre-shreedkey: 0123456789



Configuración de Algoritmos criptográficos





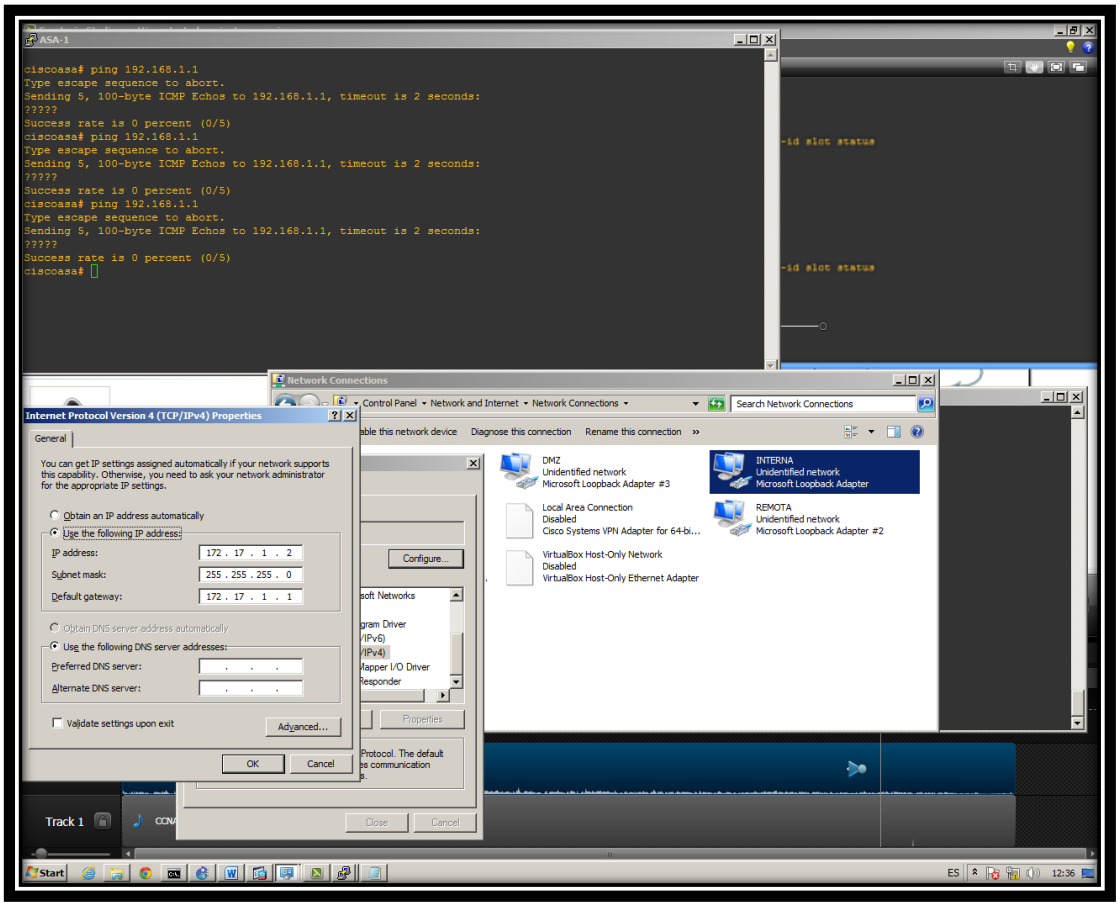


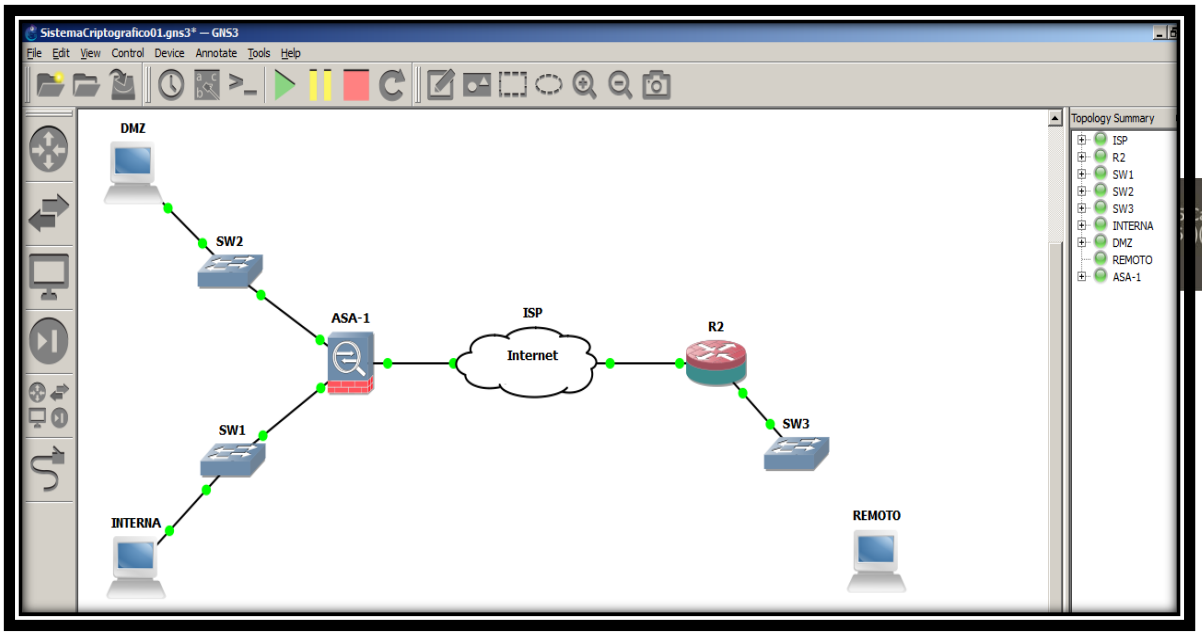
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Configuración de Sistema Criptográfico – Remoto R2

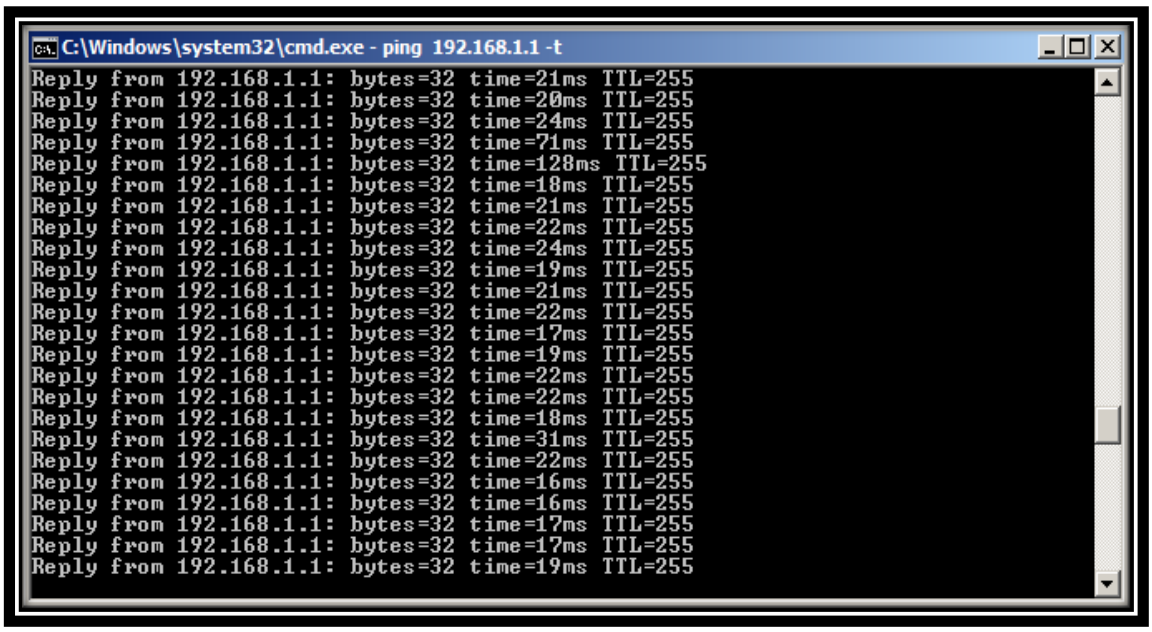
```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#hash sha
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#crypto isakmp key 0123456789 address 100.100.1.1
R2(config)#crypto ipsec transform-set TSET esp-aesesp-sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.1.0 0.0.0.255
R2(config)#crypto map CRYPTO 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R2(config-crypto-map)#set peer 100.100.1.1
R2(config-crypto-map)#match address 101
R2(config-crypto-map)#set transform-set TSET
R2(config-crypto-map)#exit
R2(config)#inter fas tEthernet 0/1
R2(config-if)#crypto map CRYPTO
*Mar  1 00:14:11.659: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
R2#wr
Building configuration...
*Mar  1 00:14:13.331: %SYS-5-CONFIG_I: Configured from console by
console[OK]
R2#
```

Realizando Pruebas





Con el comando PING probamos comunicación con route R2
Desde la red Interna



Desde el Router R2
R2#show crypto isakmpsa
IPv4 Crypto ISAKMP SA
dstsrc state conn-id slot status
200.200.1.1 100.100.1.1 QM_IDLE 1001 0 ACTIVE

R2#show crypto ipsecsa

interface: FastEthernet0/1
Crypto map tag: CRYPTO, local addr 200.200.1.1

protectedvrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remoteident (addr/mask/prot/port): (172.17.1.0/255.255.255.0/0/0)
current_peer 100.100.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pktsencaps: 506, #pkts encrypt: 506, #pkts digest: 506
#pktsdecaps: 506, #pkts decrypt: 506, #pkts verify: 506
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pktscompr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 200.200.1.1, remote crypto endpt.: 100.100.1.1
pathmtu 1500, ipmtu 1500, ipmtuidb FastEthernet0/1
current outbound spi: 0x6B5915AB(1801000363)

inboundespsas:
spi: 0x82E567A6(2196072358)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, crypto map: CRYPTO
sa timing: remaining key lifetime (k/sec): (4476456/3240)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

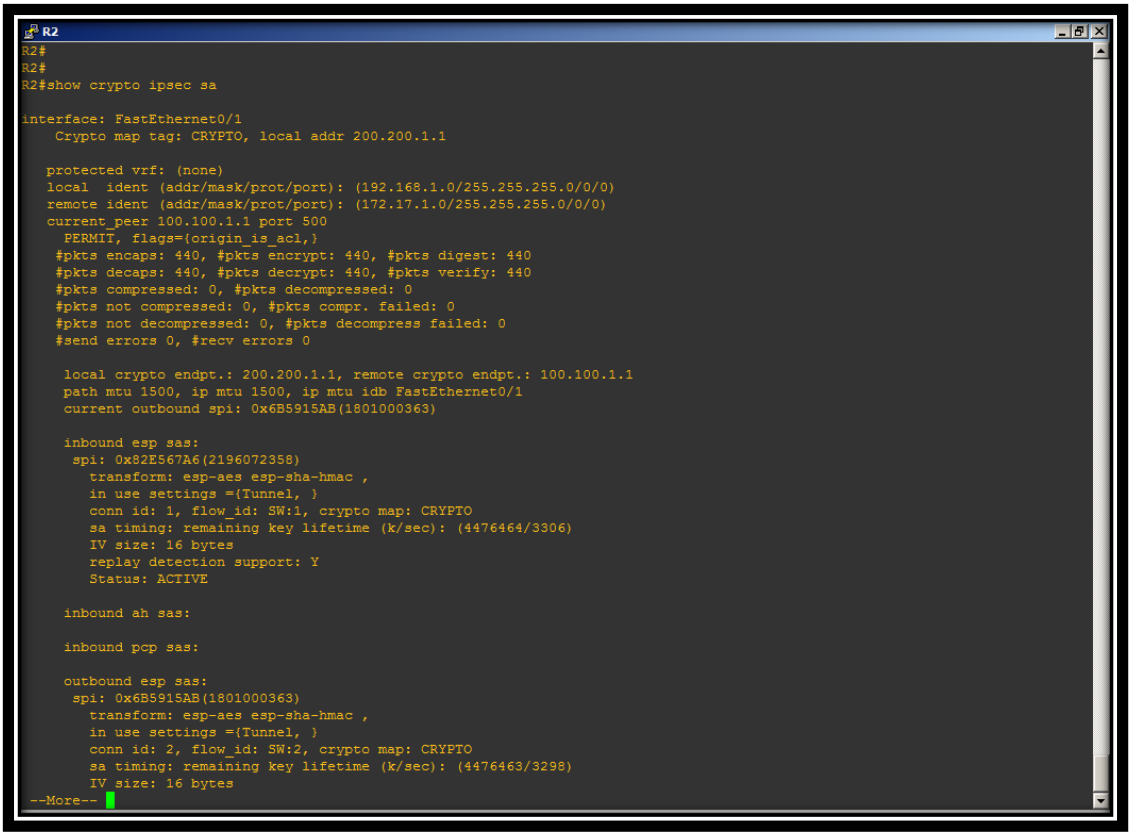
inbound ah sas:

inboundpcpsas:

outboundespsas:
spi: 0x6B5915AB(1801000363)
transform: esp-aesesp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, crypto map: CRYPTO
sa timing: remaining key lifetime (k/sec): (4476456/3236)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outboundpcpsas:



R2#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
R2#

R2#show crypto map

Crypto Map "CRYPTO" 10 ipsec-isakmp
Peer = 100.100.1.1
Extended IP access list 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.1.0 0.0.0.255
Current peer: 100.100.1.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
TSET,
}
Interfaces using crypto map CRYPTO:
FastEthernet0/1

R2#

Desde Cisco ASA
ciscoasa# show crypto isakmpsa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 200.200.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#

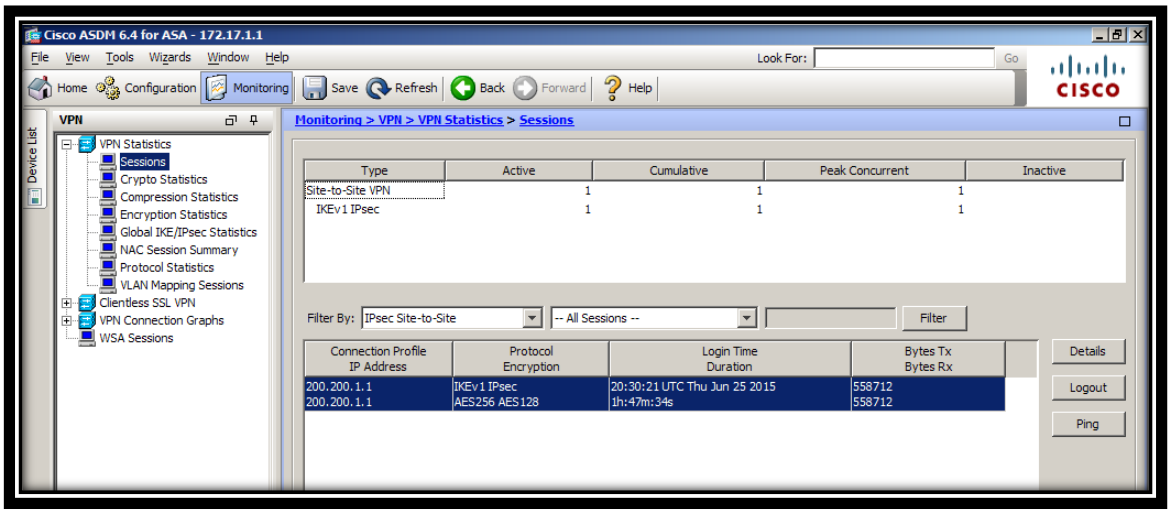
ciscoasa# show crypto ipsecsa
interface: outside
Crypto map tag: outside_map, seqnum: 1, local addr: 100.100.1.1

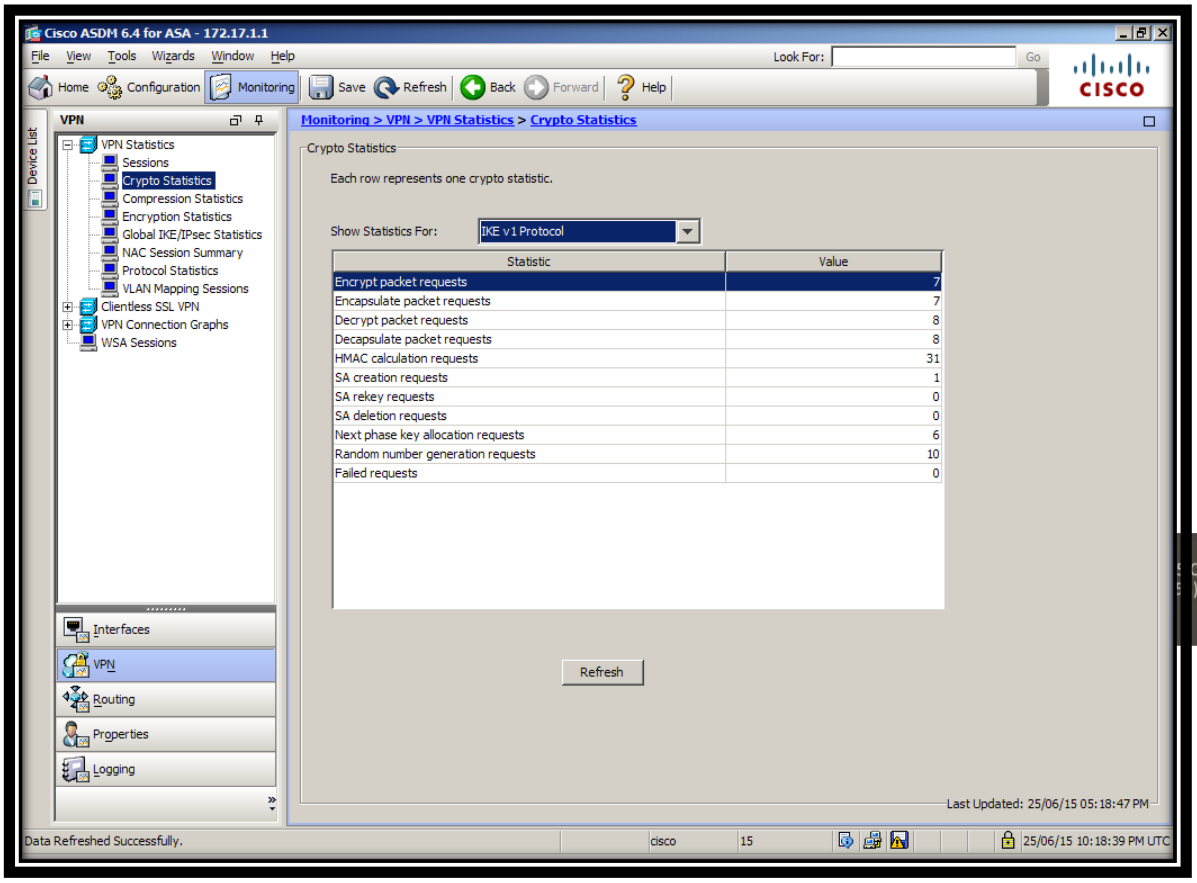
access-listoutside_cryptomap extended permit ip 172.17.1.0 255.255.255.0 192.168.1.0255.255.255.0
localident (addr/mask/prot/port): (172.17.1.0/255.255.255.0/0/0)
remoteident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer: 200.200.1.1

#pktsencaps: 3211, #pkts encrypt: 3211, #pkts digest: 3211
#pktsdecaps: 3211, #pkts decrypt: 3211, #pkts verify: 3211
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 3211, #pkts comp failed: 0, #pktsdecomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulatedfrgs needing reassembly: 0
#send errors: 0, #recv errors: 0

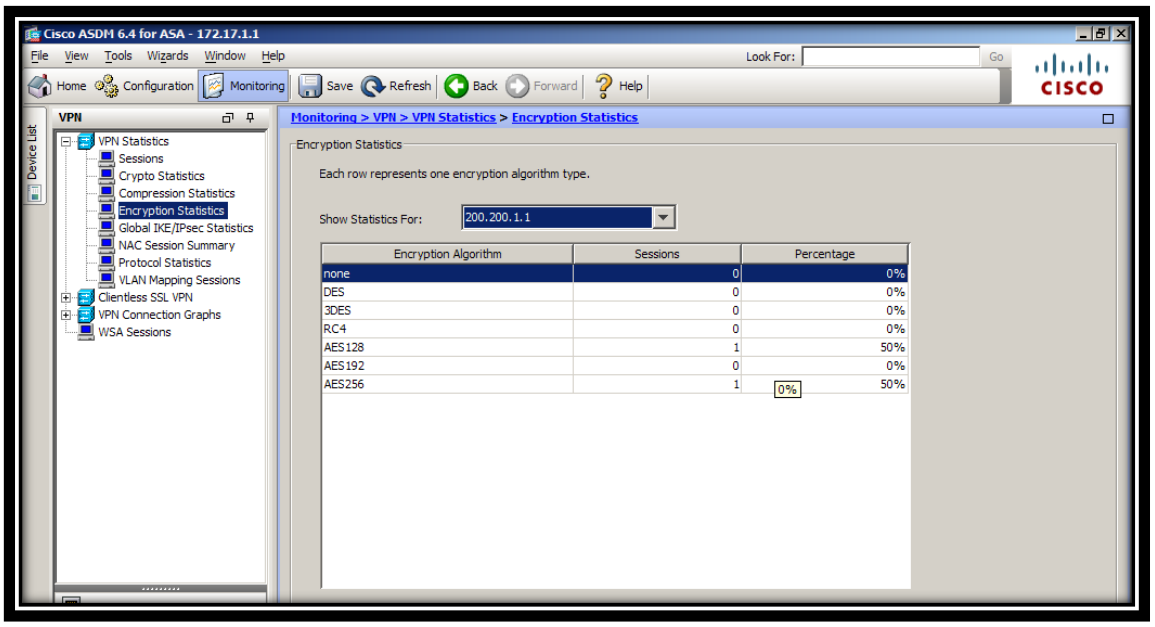
```
local crypto endpt.: 100.100.1.1/0, remote crypto endpt.: 200.200.1.1/0
pathmtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 5DC8A253
current inbound spi : 5D1274C1

inboundespsas:
spi: 0x5D1274C1 (1561490625)
transform: esp-aesesp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373998/3578)
      IV size: 16 bytes
replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x007FFFFF
outboundespsas:
spi: 0x5DC8A253 (1573429843)
transform: esp-aesesp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373998/3578)
      IV size: 16 bytes
replay detection support: Y
      Anti replay bitmap:
0x00000000 0x00000001

ciscoasa#
```

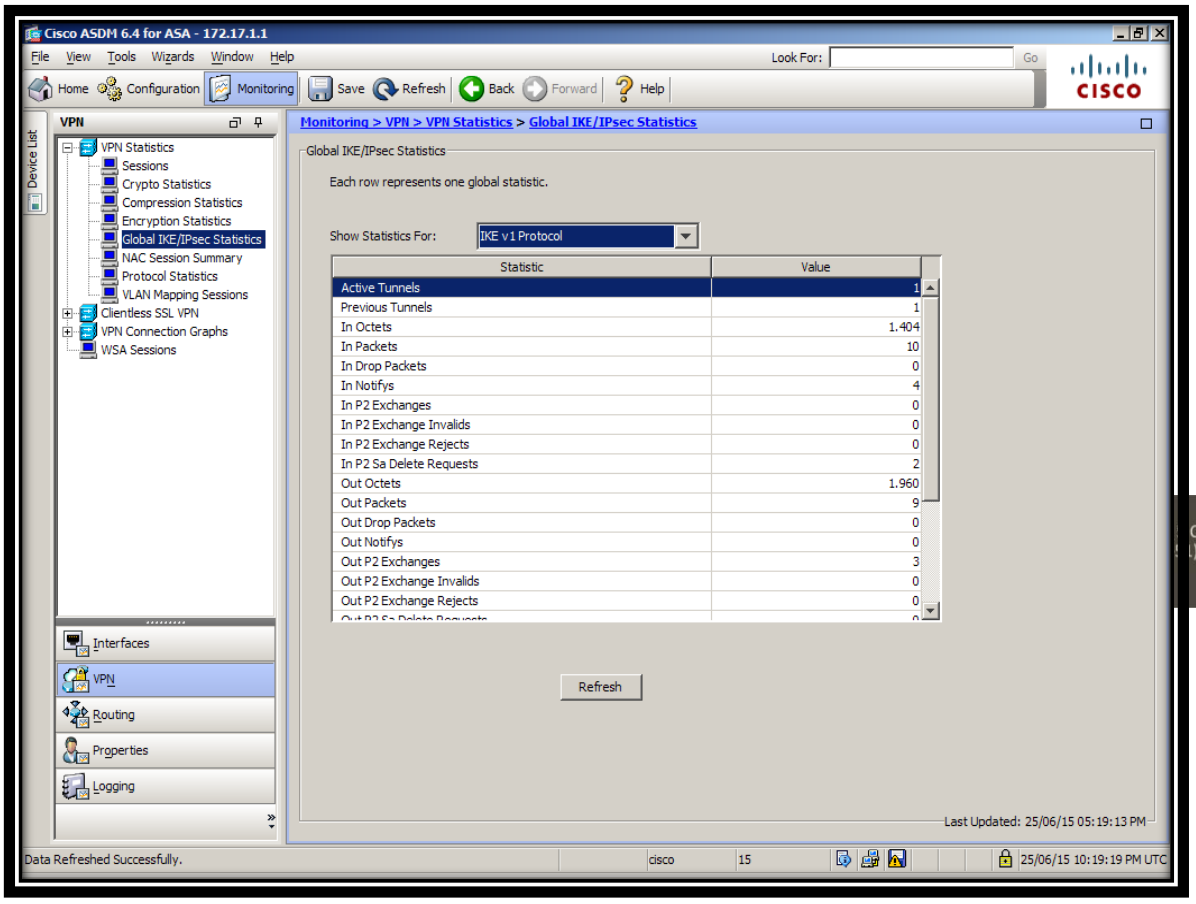
Desde modo grafico en Cisco ASA



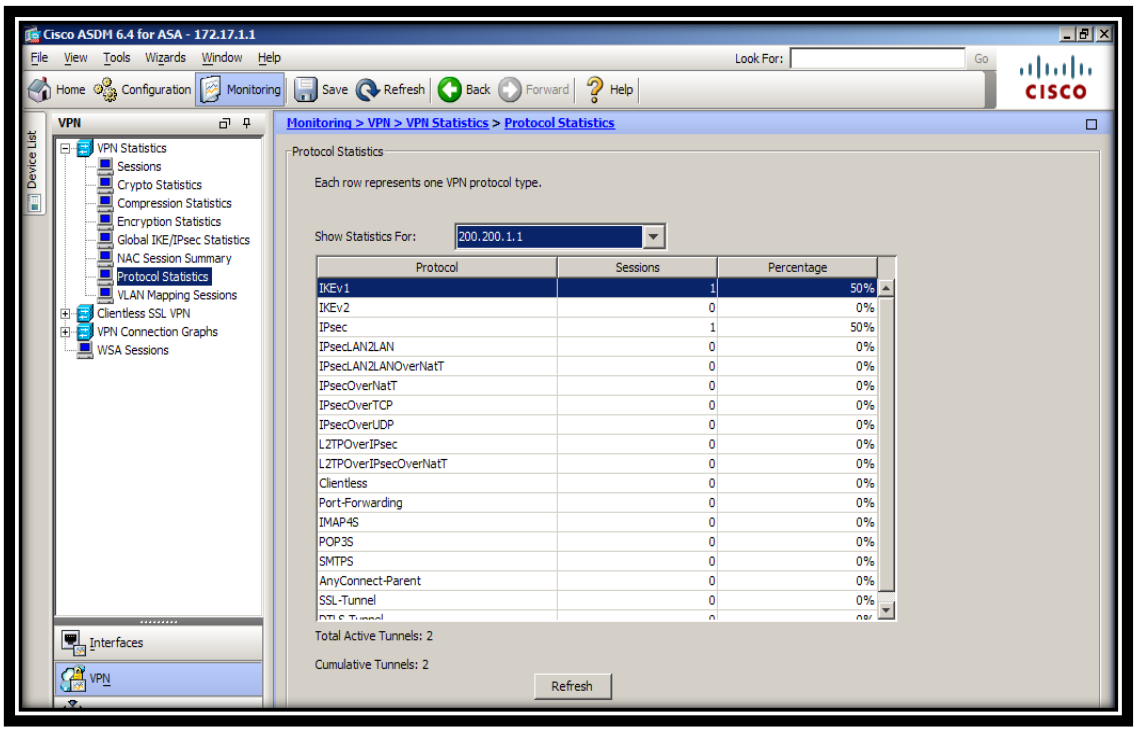


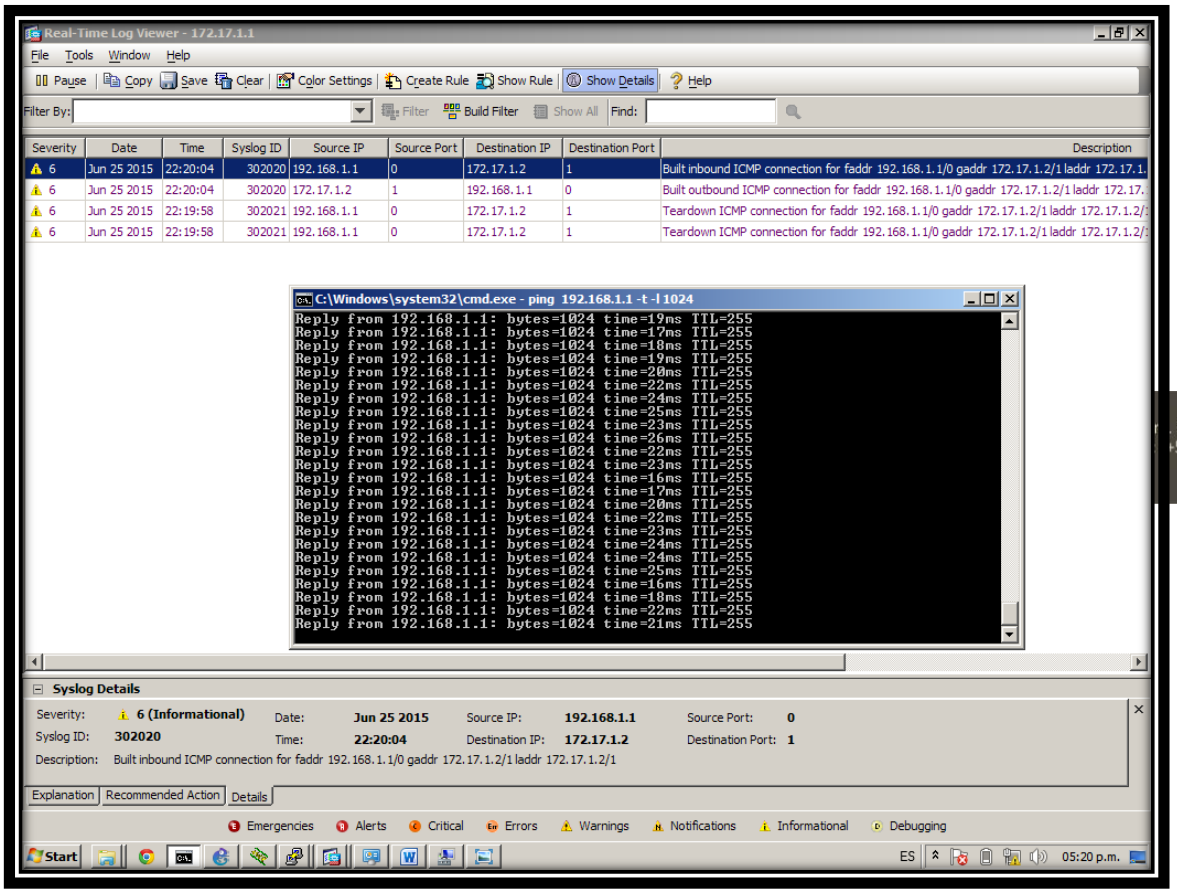
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe





Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe





Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.6 Evaluación Costo-Beneficio

Se aplicó un análisis del costo beneficio de la propuesta, el cual fue ejecutado antes de la implementación del proyecto y está basado en tiempos estimados de costos y valores estimados de beneficios. Este análisis costo – beneficio fue utilizado como una herramienta administrativa para determinar si se debe aprobar el proyecto para su implementación, el cual se muestra a continuación teniendo en cuenta los siguientes criterios:

Técnico

El Instituto Superior Tecnológico Privado “ABACO”, si cuenta con los recursos tecnológicos necesarios para llevar acabo la implementación del presente Sistema.

Económico

a. Sistema Criptográfico a través de Algoritmos Avanzados de Encriptación para mejorar la Seguridad Perimetral de una Red Informática

b. Tiempo de vida del proyecto 04 años.

Tabla 14: Tabla de análisis preliminar de costos

	Año 0	Año 1	Año 2	Año 3	Total
INVERSIÓN INICIAL	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**
Costos de Servicios y Materiales	613.60				613.60
Costos de Personal	5000.00				5000.00
Costos de Software	0.00				0.00
Costos de Hardware	0.00				0.00
Total Inversión Inicial	5613.60	0.00	0.00	0.00	5613.60
GASTOS CONCURRENTES U OPERATIVOS	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**
Administración del Sistema		1500.00	1500.00	1500.00	4500.00
Mantenimiento de Servidor		1500.00	1500.00	1500.00	4500.00
Total Inversión Concurrente	0.00	3000.00	3000.00	3000.00	9000.00
Total Todos los Gastos Por Año	5613.60	3000.00	3000.00	3000.00	14613.60
Total Todos los Gastos Acumulados	5613.60	8613.60	11613.60	14613.60	
BENEFICIOS	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**
Reducción de Personal en la Sección Personal 1		18000.00	18000.00	18000.00	108000.00
Reducción de Personal en la Sección Personal 2		36000.00	36000.00	36000.00	108000.00

Total Bruto de Beneficios Por Año	0.00	54000.00	54000.00	54000.00	162000.00
Total Bruto de Beneficios Acumulado	0.00	54000.00	108000.00	162000.00	
Total NETO de Beneficios Por Año	0.00	51000.00	51000.00	51000.00	153000.00
Total NETO de Beneficios Acumulado	0.00	51000.00	102000.00	153000.00	
FLUJO DE CAJA NETO	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**	**(S/.)**
Flujo de Caja Neto Anual	-5613.60	51000.00	51000.00	51000.00	147386.40
Flujo de Caja Neto Acumulado	-5613.60	45386.40	96386.40	147386.40	

Fuente: Elaboración Propia

5.5.1 Valor Actual Neto (VAN)

El VAN es un procedimiento que permitirá calcular el valor presente de un determinado número de flujos de caja futuros.

El cálculo del VAN se ha realizado utilizando la función: VNA(tasa;período_1:período_3)+período_0, del programa Excel. Donde la tasa de interés es del 10% y los períodos son extraídos de Flujo de Caja Neto Anual presentado en el cuadro la Tabla Nª 14 de análisis preliminar de costos.

El resultado obtenido es de S/. 121, 215.85; Lo que indica el buen nivel de rentabilidad del proyecto propuesto.

5.5.2 Tasa Interna del Retorno (TIR)

El TIR es la tasa de interés con la cual el valor actual neto o valor presente neto (VAN o VPN) es igual a cero.

Al igual que el VAN, el cálculo del TIR se ha realizado utilizando la función del programa Excel: TIR(período_0:período_3).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6.1 Conclusiones

El objetivo de este proyecto fue Implementar un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática. Se ha cumplido este objetivo general desarrollando consecuentemente cada objetivo específico.

a) Se realizó el diagnóstico del estado actual de la seguridad perimetral de una red la informática, para determinar cómo se lleva a cabo la gestión de la red y así poder tomar decisiones en el desarrollo del proyecto.

b) Se identificó los factores influyentes en la seguridad perimetral de una red informática. El cual permitió reestructurar el diseño dando como resultado un diseño centralizado, escalable y seguro. Todo el diseño de la estructura y la topología fue documentando.

c) Se realizó el diseño del sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de la red informática del instituto Abaco. Este proceso se llevó a cabo mediante el diseño de la estructura y la topología la cual fue implementada en un prototipo, y finalmente se documentó.

d) Se obtuvieron los resultados que generará la implantación del sistema criptográfico a través de algoritmos avanzados de

encriptación en la seguridad perimetral de la red informática del instituto Abaco. La cual se procedió a documentar.

e) Se implementó el sistema criptográfico a través de algoritmos avanzados de encriptación en la seguridad perimetral de la red informática del instituto Abaco, utilizando un prototipo, simulado en GNS3.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6.2 Recomendaciones

a) A continuación se presenta algunas recomendaciones para la administración de la red.

b) La implementación del sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática, por su relevancia institucional debe de estar en constante mejorar y actualización.

c) Se recomienda realizar un mantenimiento preventivo y correctivo de las instalaciones de red de la organización, para que esta no llega a funcionar incorrectamente llegando a degradar sus prestaciones.

d) Se recomienda tener en cuenta las actualizaciones de las versiones de las herramientas de software que sirven como soporte al sistema, ya que esto permitirá que el sistema se mantenga actualizado con respecto a los últimos avances en uso y seguridad.

e) Realizar un proceso de capacitaciones al personal encargado del manejo de las tecnologías de la información de la organización, para asegurar el uso adecuado y obtener los beneficios esperados.

f) Se recomienda desarrollar políticas de seguridad, en el manejo de información, ya que esta es el activo de toda organización.

REFERENCIAS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Referencias Bibliográficas

a) *Modelo de Gestión ENJ* . (7 de Julio de 2010). Obtenido de http://enj.org/wiki/index.php5?title=06.1.1_Eje_Institucional

b) *Rational Unified Process* . (2010). Recuperado el 2014, de http://aalbertovargasc.files.wordpress.com/2014/03/metodopesadesrup1.pdf

c) CÓDIGO DEONTOLÓGICO DEL COLEGIO DE INGENIEROS DEL PERÚ. (2012). Lima, Perú.

d) Instituto Nacional de Tecnologias . (2012). Madrid. Obtenido de http://recursostic.educacion.es/observatorio/web/ca/software/programacion/490-lorena-arranz

e) *¿Qué es un Sistema operativo?* (2013). Obtenido de http://pciserviciosmx.wordpress.com/2013/06/14/que-es-un-sistema-operativo/

f) *Criptografía asimétrica*. (2013). Obtenido de http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

g) *MySQL*. (2013). Recuperado el 2014, de http://es.wikipedia.org/wiki/MySQL

h) *METODOLOGÍA DEL DESARROLLO CON CISCO*. (2014). Obtenido de http://metodologiaspararedes.blogspot.com/

i) *Check Point, en la seguridad perimetral de RBA*. (2014). Obtenido de http://www.ciospain.es/industria-y-utilities/check-point-en-la-seguridad-perimetral-de-rba

j) *Superintendencia de Banca, Seguros y AFP de la Republica del Perú*. (13 de 06 de 2014). Obtenido de http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&pfl=0&jer=154

k) Alcaraz Moreno, N., & Noreña, A. (2012). Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa. Colombia.

l) Álvarez, J. R. (2012). *Implantación de los procesos de gestión de incidentes y gestión de problemas según ITILv3 en el área de tecnologías de información de una entidad financiera.* Lima: Pontificia Unviersidad Católica del Perú.

m) Alvarez, M. A. (2010). *Instroduccion a los lenguajes de la web*. Recuperado el 2014, de http://www.desarrolloweb.com/articulos/392.php

n) Alvarez, M. A. (2011). *Programa Para Crear Webs.* Recuperado el 2014, de http://www.desarrolloweb.com/articulos/introduccion-css3.html

o) Ariza Zambrano, S. P. (2012). Plan de acción para la implementación de una mesa de servicio para la adminsitración de incidentes y solicitudes de cambios soportado en el modelo ITIL caso aplicado a la empresa soluciones y servicios informáticos empresariales S.A.S. Bogotá, Colombia: Universidad EAN sede Bogotá.

p) Avila, T. M. (Octubre de 2010). *Certificaciones y normativas de calidad en software.* Obtenido de http://www.it360.es/certificaciones-normativas-calidad-en-desarrollo-de-software.php

q) Bárbara Salas , V. (5 de Noviembre de 2014). *Diario Gestion*. Recuperado el 13 de Marzo de 2015, de http://gestion.pe: http://gestion.pe/tecnologia/tendencia-2015-seguridad-informatica-mundo-corporativo-se-encuentra-mira-cibercriminales-2113007

r) Benítez Díaz, M. A. (Mayo de 2013). Implementación de un Service Desk para la gestión de la infraestructura tecnológica para la empresa Alpha Electronics, basado en ITILv3. Quito, Ecuador: Universidad Internacional SEK Facultad de Sistemas y Telecomunicaciones.

s) Bono Cabre, R. (2013). Diseños cuasi-Experimentales. http://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&sqi=2&ved=0CDIQFjAB&url=http%3A%2F%2Fwww.ub.edu%2Fdeia%2Farchivos%2F111006211920_Disenos_cuasi_1_WOP_P.ppt&ei=UgJoU97lHs6YyATwz4LoCw&usg=AFQjCNHCM9z78DaEVGG_9dmW8FyfbrLMRQ&bv.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

t) Bowman, M. (04 de Mayo de 2013). *¿Qué es y para qué sirve jQuery y HTML5?* . Recuperado el 2014, de http://qaendispositivosmoviles.wordpress.com/2013/05/04/que-es-y-para-que-sirve-jquery-y-html5/

u) Cabrera Aldaya, M. A., & Cabrera Sarmiento, D. A. (2014). Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA.

v) Carrión Barco, G. (2013). *Herramientas de Software para ITSM y CMDB.* Lambayeque.

w) Castro, L. (2013). *¿Qué es HTML 5?* Recuperado el 2014, de http://aprenderinternet.about.com/od/Glosario/g/Que-Es-Html-5.htm

x) Chavarry Sandoval, C. J. (2012). Propuesta de un modelo de gestión de TI orientado a los servicios basado en el marco de trabajo ITIL aplicado al Departamento de TI de la Universidad de Lamabayeque. Chiclayo, Lambayeque, Perú: Universidad Santo Toribio de Mogrovejo.

y) CIPPEC. (2012). *Centro de Implementación de Políticas Públicas para la Equidad y el crecimiento*. Recuperado el 2014, de http://www.cippec.org/instituciones-y-gestion-publica

z) Cisco, S. (29 de Octubre de 2013). *CCNA 3 v4.0.* EEUU: Cisco System.

aa) Comercio., E. (06 de Agosto de 2014). *El 67% de los bancos en Perú ha sufrido ataques internos*. Recuperado el 12 de Marzo de 2015, de http://elcomercio.pe: http://elcomercio.pe/economia/peru/67-bancos-peru-ha-sufrido-ataques-internos-noticia-1747987

bb) Cromo Uruguay, M. C. (10 de Agosto de 2014). *La moda de encriptar la información*. Recuperado el 13 de Marzo de 2015, de http://www.cromo.com.uy: http://www.cromo.com.uy/2014/08/aplicaciones-para-una-comunicacion-encriptada/

cc) Cruz Loján, J. D., Cando Sisalema, N. L., & Paredes Rosas, N. J. (2012). Sistema de gestión de configuraciones y cambios para el Departamento

de Administración y Desorrollo tecnológico de Información y Comunicaciones de la Universidad Central de Ecuador. Quito, Ecuador: Universidad Central de Ecuador.

dd) Departamento de Sistemas Informáticos y Computación. (2010). *Proceso de Desarrollo de Software.* Recuperado el Lunes de Abril de 2014, de http://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0CFAQFjAG&url=http%3A%2F%2Fwww.dsic.upv.es%2Fasignaturas%2Ffacultad%2Flsi%2Fdoc%2FIntroduccionProcesoSW.doc&ei=9fR4U5b_NOPLsQTlpIHIDQ&usg=AFQjCNGAyOzvxjChM6izsIaI_eLoQhtk

ee) Desarrolladores de Laravel, L. (13 de Septiembre de 2013). *Introduccion - Documentation Laravel PHP Framework*. Obtenido de http://laravel.com/docs/4.2/introduction

ff) Di Virgilio, M., & Solano, R. (2012). *Monitoreo y Evaluacion de politicas, programas y proyectos sociales.* Buenos Aires: VERLAP S.A.

gg) Direccion Nacional de Cuentas, I. (2009). *Economia de la Region Lambayeque*.

hh) Dr. Hernández Sampieri, R., Dr. Fernández Collado, C., & Dra. Baptista Lucio, M. d. (2006). *Metotologia de la investigacion.* Distrito Federal de Mexico: INTERAMERICANA EDITORES, S.A. DE C.V.

ii) Drumkey, D. (2013). *Conociendo CSS3 - Animaciones.* Recuperado el 2014, de http://www.ayuda-bloggers.info/2012/12/conociendo-css3-animaciones.html

jj) ERP, S. (2012). *Software ERP en Mexico*. Obtenido de http://www.sistema-erp.net/erppyme.htm

kk) ERP, S. (2014). *Software a medida*. Obtenido de http://www.tuerp.com/g/tipos

ll) ERP, S., & Integradas, S. (2014). *Alojamiento en la Nube*. Obtenido de http://www.sagerp.co/index.php/menu-system/en-la-nube-vs-local/10-sag-erp

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

mm) Fernández Prieto, A., Soledad Luque, P., & Rezzonico, G. (2011). *Área de Monitoreo y Evaluación del Programa Remediar + Redes.* Recuperado el 2014, de http://remediar.gov.ar/files/publicacioncompletalineadebase(2)(1).pdf

nn) Fernández, E. (2008). UNiTIL Gobierno y Gestión de TIC basado en ITIL. Fuenlabrada, Madrid, España: Universidad Rey Juan Carlos España.

oo) Flores Villarroel, C. (2011). *Cloud Computing*. Recuperado el 2014, de http://es.slideshare.net/CorinaFlores/cloud-computing-definicin-ser

pp) Framework popularity, S. (2013). *SitePoint*. Obtenido de http://michelletorres.mx/wp-content/uploads/2014/08/chart1-1024x853.png

qq) Galan. (2015). *Mi Obra.* Lima: Limusa.

rr) Garcia Echevarria, M. d. (2013). Diseño de una propuesta de Gobierno electronico para la mejora de la gestion Gubernamental Regional de Lambayeque. Chiclayo, Perù, Region Lambayeque.

ss) García Felipe, M. (2010). *Implementación de técnicas de seguridad remota. Seguridad perimetral*. Obtenido de www.it.uc3m.es/~lmiguel/ids2.pdf

tt) García Romanos, J. (2008). La gestión de la configuración y la gestión de activos como una gestión del conocimiento. *REICIS Revista Española de Innovación, IV*(1), 18-35.

uu) Gerencia Regional de Planeamiento, P. y. (2013). Plan Operativo institucional. Lima, Region Lima- Sede Central.

vv) Gloria, C. G. (2005). *Tipos de Servidores de Bases de Datos*. Recuperado el 2013 de Octubre de 08, de http://www.itlp.edu.mx/publica/revistas/revistasli/anteriores/marzo99/servidores.html

ww) González, M. P. (13 de Diciembre de 2010). *Bligspot*. Obtenido de http://manuelpereiragonzalez.blogspot.com/2010/12/diez-motivos-para-programar-en-java.html

xx) Granguillhome Morfin, R. (2013). LA EVALUACIÓN DE LAS ACCIONES DE COOPERACIÓN INTERNACIONAL PARA EL DESARROLLO. *1a. Edición, 2013,* 458. (C. &. Maldonado Trujillo, Ed.) Mexico, Distrito Federal.

yy) Guitiérrez Cóndor, J. (31 de Octubre de 2013). *Proyecto de Ley Nª 2856/2013-CR.* Recuperado el 2014, de Estándares y Especificaciones de Interoperabilidad: http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc02_2011_2.nsf/d99575da99ebfbe305256f2e006d1cf0/be8a4fd1dc0f978b05257c150070ceba/$FILE/PL02856311013.pdf

zz) Hax, A. y. (1997). *Estrategias para el Liderazgo Competitivo.* Editorial Dolmen.

aaa) Hernández Orallo, E. (2013). Seguridad y privacidad en los sistemas informáticos. *Actas de Seguridad*.

bbb) Hernández Sampieri, R. (2010). Metodologia de la investigacion . En R. Hernández Sampieri, *Metodologia de la investigacion* . Mexico.

ccc) Herramientas para calculos financieros. (2014). Obtenido de http://es.calcuworld.com/calculadoras-empresariales/calculadora-tir/

ddd) Herramientas para calculos financieros. (2014). Obtenido de http://es.calcuworld.com/calculadoras-empresariales/calculadora-van/

eee) Herrarte Sánchez , P. (4 de Abril de 2013). *Patrón MVC. Modelo Vista Controlador*. Obtenido de http://www.devjoker.com/contenidos/catss/525/Patron-MVC-Modelo-Vista-Controlador.aspx

fff) HOTELES, R. L. (30 de Septiemble de 2014). Entrevistas a los administradores de los hoteles tomados como muestra en la investigacion . (E. Alejandria Bustamante, Entrevistador)

ggg) IBM. (2014). *Rational Rose Enterprise*. Recuperado el 2014, de http://www-03.ibm.com/software/products/es/enterprise/

hhh) Ing. Román Zamitiz, C. A. (2013). *TEMAS ESPECIALES DE COMPUTACIÓN*. Recuperado el 2014, de http://profesores.fi-b.unam.mx/carlos/aydoo/uml.html

iii) Instituto Tecnologico de Sonora, a. (2013). *Introduccion a los Sistemas de Información*. Obtenido de http://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p4.htm

jjj) Jose Baltazar, J. C. (2011). *Diseño e Implementación de un esquema de seguridad perimetral para redes de datos caso practico: dirección general del colegio de ciencias y humanidades*. México: Universidad Nacional Autónoma de México.

kkk) Katia, L. (2005). *Encriptacion RSA de archivos de texto.* Perú: PUCP.

lll) Kolthof, A. (2008). *Operación del servicio basada en ITILv3 Guía de gestión.* Van Haren Publishing.

mmm) Latindevelopers, P. L. (8 de Septiembre de 2011). *Comparacion entre MySQL y SQL Server*. Recuperado el 2014, de http://www.latindevelopers.com/articulos/sql-server/diferencias-entre-mysql-y-sql-server.php

nnn) Loic Martinez, F., & Segovia Perez, F. J. (2005). *Introducción a la ingeniería de software Modelos de desarrollo de programas.* Zaragoza: Delta Publicaciones.

ooo) Majluf, N., & Hax, A. (1997). *Estrategias para el Liderazgo Competitivo.* Editorial Dolmen.

ppp) Mamani Casilla, R. N. (2012). *PLan Operativo Institucional.* Recuperado el 2014, de http://administradorenlared.blogspot.com/2012/10/plan-operativo-institucional-poi_3.html

qqq) Marie Mokate, K. (2013). *Convirtiendo el "monstruo" en aliado: La evaluación como herramienta de la gerencia social.* Recuperado el 2014, de http://preval.org/documentos/2080.pdf

rrr) Meavilla, V. (2009). LA CRIPTOGRAFÍA CLÁSICA. Bilbao.

sss) Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud*. Obtenido de http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

ttt) Merino, J. I., & Inzunza Figueroa, N. (2010). *Evaluación Técnico-Económica de servicios de Cloud Computing para su Implementación en PYMES.* Chile: Universidad Tecnología de Chile.

uuu) Microsoft, L. M. (2015). *Seguridad de la Información: Más que una actitud, un estilo de vida*. Recuperado el 12 de Marzo de 2015, de http://www.microsoft.com: http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

vvv) MINISTROS, P. D. (19 de Noviembre de 2008). *Estándares y Especificaciones de Interoperabilidad del Estado Peruano.* Obtenido de http://spij.minjus.gob.pe/Graficos/Peru/2008/noviembre/19/RM-381-2008-PCM_19-11-08.pdf

www) Ocampo Díaz, C. E. (Noviembre de 2012). *Slideshare*. Obtenido de http://www.slideshare.net/cesarocampodiaz/servis-desk-ejemplo

xxx) Oficina Regional de Planeamiento, P. y. (2013). *Informe de Seguimiento del Plan Operativo Institucional 2013.* Chiclayo.

yyy) Oliveros, A., & Martínez, S. (2012). *Aspectos éticos de la investigación en Ingeniería de Software que involucra seres humanos.* Recuperado el 2014, de http://sedici.unlp.edu.ar/bitstream/handle/10915/23714/Documento_completo.pdf?sequence=1

zzz) Ortega, E., & Delgado, D. (2009). *METODOLOGÍAS DE DESARROLLO PARA SISTEMAS DE TIEMPO REAL. UN ESTUDIO COMPARATIVO*. Recuperado el 2014, de

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

http://www.scielo.org.ve/scielo.php?pid=s1316-48212009000100008&script=sci_arttext&tlng=es

aaaa) Osiatis. (2013). *Econocom Osiatis*. Obtenido de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_configuraciones/vision_general_gestion_de_configuraciones/vision_general_gestion_de_configuraciones.php

bbbb) Osio Rojas, N. (2009). El e-Gobierno como estrategia para mejorar la administracion Publica. Aragua, Venezuela.

cccc) Pacherres, A. Ó. (2012). Análisis y diseño del Service Desk basado en ITILv3 para el área de mesa de ayuda de FIA-USMP. Lima, Lima, Perú: Universidad San Martín de Porres.

dddd) Pedraza Enrriquez, A. (2010). Propuesta de un modelo gerencial estrategico socialmente responsable en el gobierno electronico para la gestion de los gobierno Locales en el Estado de Aragua. Aragua, Venezuela.

eeee) Perez Camarena, R. K. (2013). La Institucionalización del Sistema de evaluación del Programa Nacional Wawa Wasi, del ministerio de la Mujer y Desarrollo Social, entre los años 2003 - 2011. Lima, Perù.

ffff) Perez Ruiz, A. N. (2012). *Implementacion de tecnologia de Cloud Computing para ofrecer servicios de infraestructura (IaaS) en la Facultad de Telemática.*Colima.

gggg) Pultorak, D., Henry, C., & Leenards, P. (2008). *Microsoft Operations Framework (MOF) 4.0* (Primera ed.). Van Haren Publishing.

hhhh) Pultorak, D., Henry, C., & Leenards, P. (2008). *Microsoft Operations Framework (MOF) 4.0* (Primera ed.). Van Haren Publishing.

iiii) Quispe Carita, V., Huamantuco Solorzano, D., & Vargas Yupanqui, J. (2011). *Metodología RUP*. Puno: Universidad Nacional del Antiplano.

jjjj) Ramió, J. (2009). *Libro Electrónico de Seguridad Informática y Criptografía*. Obtenido de http://swgu.ru/sg37r15

kkkk) Realsec Peru, C. d. (8 de Julio de 2014). *La importancia de la Criptografía en el desarrollo del Gobierno Electrónico Peruano*. Recuperado el 18 de Marzo de 2015, de www.relasec.com: http://www.realsec.com/noticias/importancia-criptografia-desarrollo-gobierno-electronico-peruano/

llll) Reyes, E., & Reyes, P. (2007). *Análisis de Costo/Beneficio de Soluciones de Software.* Recuperado el 2014, de http://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDYQFjAC&url=http%3A%2F%2Fplanificacionymodelado.wikispaces.com%2Ffile%2Fview%2FAn%25C3%25A1lisis%2Bde%2BCosto%2B7sm.doc&ei=7hxKU-D2D6q50gHfhoGYAg&usg=AFQjCNF3HDovm5huok05s0p4UezC6qx7J

mmmm) Rodrigues, J. E. (2010). *ERP (Entreprise Resource Planning) - Sistemas de Planeación de los Recursos de la Empresa Como el Nuevo Enfoque de Gestión*. Obtenido de http://www.taringa.net/posts/info/1210393/Sistemas-de-Planeacion-de-los-Recursos.html

nnnn) RUP, M. (Noviembre de 2010). *Software Recopilation*. Obtenido de http://softwarerecopilation.wordpress.com/modelo-rup/

oooo) SISE, I. S. (2013). *Manual Modelamiento y Diseño de Base de Datos - v0810.* Recuperado el 2014, de http://es.scribd.com/doc/40031583/Manual-Modelamiento-y-Diseno-de-Base-de-Datos-v0810

pppp) SOFTWARE, E. (2010). *Software ERP*. Obtenido de http://www.ecuosoft.com/%C2%BFque-es-erp.aspx

qqqq) Software, N. (2012). *Nuevos Horizontes para Hotelería y Turismo*. Obtenido de http://www.newhotel.com/Files/Newsletter%20December.pdf

rrrr) Soto, J. (2010). *Algoritmos de encriptacion simetricos que procesa bloques de 192 bits, con llaves de cifrado de 192 bits, empleando los teoremas factorial y JV*. Mexico: Instituo Politecnico Nacional.

ssss) Spagni, M. B. (2005).

tttt) Stahie, S. (22 de Junio de 2012). *Red Hat Enterprise Linux 6.3 fue lanzado oficialmente.* Recuperado el 2014, de http://news.softpedia.es/Red-Hat-Enterprise-Linux-6-3-fue-lanzada-oficialmente-277163.html

uuuu) SUPERINTENDENCIA DE BANCA, S. Y. (2008). Gestión Integral de Riesgos. . *Resolución S.B.S. N° 37-2008*. Perú: SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP.

vvvv) SUPERINTENDENCIA DE BANCA, S. Y. (2009). Gestión del Riesgo Operacional. *Resolución S.B.S. N° 2116-2009*. Perú: SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP.

wwww) Superintendencia de Banca, Seguros y AFP. (17 de Julio de 2014). *Tasa de interés promedio*. Obtenido de http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&pfl=0&jer=154

xxxx) Tapia Cachay, E. (2011). *Implementacion de un sistema bajo tecnologia web para mejorar los procesos de gestion hotelera, para la empresa "Gran Marques Hotel" de la ciudad de trujillo.* chiclayo.

yyyy) Torres Mirez, V. (2011). *Desarrollo de un sistema parametrizable utilizando Cloud Computing en su modalidad de software como servicio, para agilizar su implantación en restaurantes.* Chiclayo.

zzzz) Urueña, A., & Valdecasa, E. (2012). *Cloud Computing Retos y Oportunidades*. Recuperado el 2014, de http://www.ontsi.red.es/ontsi/sites/default/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

aaaaa) Valenzuela, J. (2012). *Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña.* Lima: PUCP.

bbbbb) van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., y otros. (2008). *Transición del Servicio basaba en ITILv3* (Primera ed.). Van Haren Publishing.

ccccc) Vitaly Kamluk, S. L. (05 de Diciembre de 2013). *Kaspersky Security Bulletin 2013, amenazas Corporativas.* Recuperado el 20 de Marzo de 2015, de http://www.viruslist.com/sp/analysis?pubid=207271238

ddddd) web, F. d. (26 de Marzo de 2002). *Foros del web*. Obtenido de http://www.forosdelweb.com/f15/mysql-sql-server-70127/

eeeee) Xin Wang, Z. Y. (2010). UNa Práctica ITSM basada en ITIL - Un caso de estudio en empresas manufacturera de acero. Beihang, Biejing, China: Biehang University.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe