UNA UNIVERSIDAD CON ALMA DE GUERRERO

IMPLEMENTACIÓN DE PROTOCOLO DE CIFRADO TLS PARA MEJORAR LA SEGURIDAD DE LAS COMUNICACIONES EN LA CAPA DE TRANSPORTE 2016

Tesis para optar por el Titulo de Ingeniero de Sistemas, que presentan los bachilleres.

AUTORES

Renzo Augusto Ariansen Moncada
Jose Ivan Rojas Diaz

ASESOR

Mg. Alex Franklin Coronado Navarro

CHICLAYO - PERÚ 2016

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

USS | UNIVERSIDAD SEÑOR DE SIPÁN

DEDICATORIA

Dedicamos la presente tesis con mucho cariño a nuestras familias, por estar siempre a nuestro lado brindándonos su ayuda incondicional y apoyo.

A nuestros amigos por estar con nosotros todo este tiempo ayudándonos a que sea posible el desarrollo de este proyecto.

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

AGRADECIMIENTOS

A todas las personas, que en su momento, con sus consejos y apoyo nos ayudaron a seguir adelante. Y a todos los señores profesores que compartieron sus conocimientos para nuestra formación intelectual y profesional

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

ÍNDICE

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

TABLA DE FIGURAS

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

TABLA DE TABLAS

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

RESUMEN

La información es el activo más valioso y susceptible a ataques con fines personales o delictivos que poseen las organizaciones, razón por la cual es una prioridad resguardar su confidencialidad.

Dentro de las preocupaciones de las diferentes organizaciones se encuentra la de que alguien no autorizado tenga acceso a información sensible. Para mitigar este riesgo se busca brindar confidencialidad a la información. Para tal fin es común cifrar la información de manera que de un mensaje se obtiene un respectivo criptograma que es ilegible para quien no conoce como descifrarlo.

Actualmente los sistemas de cifrado de la información han logrado evoluciones importantes, al grado de poder unir las fortalezas de diferentes técnicas de cifrado para ofrecer criptosistemas híbridos que conjugan la seguridad ofrecida por cifrado simétrico con las que ofrece el cifrado asimétrico.

Con base en esto, el presente trabajo consiste en analizar los algoritmos criptográficos de llave secreta DES, 3DES, AES, entre otros, mismos que son acreditados por los organismos internacionales NIST (National Institute of Standards and Technology) de los Estados Unidos de América, NESSIE (New European Schemes for Signatures, Integrity and Encryption) de la Unión Europea y CRYPTREC (Cryptography Research and Evaluation Committee) de Japón.

Palabras clave: TLS, SSL, cifrado, algoritmo, criptografía.

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

ABSTRACT

Information is the most valuable and susceptible to personal attacks or criminal purposes that have active organizations, which is why it is a priority to safeguard confidentiality

Among the concerns of different organizations is that of someone not authorized to have access to sensitive information. To mitigate this risk seeks to provide confidentiality for information. For this purpose it is common to encrypt the information so that a respective message is illegible cryptogram to decipher who did not get called.

Currently the ciphers of information have made significant changes to the extent of being able to unite the strengths of different encryption techniques to provide cryptosystems hybrids that combine the security offered by symmetric encryption with asymmetric encryption offered.

On this basis, this paper is to analyze cryptographic algorithms secret key DES, 3DES, AES, among others, same that are accredited by international agencies NIST (National Institute of Standards and Technology) in the United States, NESSIE (New European Schemes for Signatures, Integrity and Encryption) of the European Union and CRYPTREC (Cryptography Research and Evaluation Committee) of Japan.

Keywords: TLS, SSL, encryption, algorithm, cryptography.

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

INTRODUCCION

La presente tesis se fundamenta en la propuesta de la implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte el mismo que contiene toda la documentación referente al proceso de implementación del protocolo de cifrado TLS, se considera implementar el protocolo de transporte basado en comunicación HTTPS que brinde un servicio de excelencia, calidad con capacidad de cubrir las necesidades de transferencia de datos seguros, confiables, el cual ayude a cumplir con los objetivos propuestos.

A continuación se describe el desarrollo de los capítulos de la investigación:

En el capítulo uno, se plantea la problemática de la investigación, es decir se realiza un análisis de la situación actual de los protocolos y se define cual es la razón de ser de esta tesis. También se describe el objetivo general y específico, enfatizando en el diagnóstico del estado actual de la seguridad de las comunicaciones en la capa de transporte, evaluar, analizar e implementar algoritmos de cifrado basado en comunicación HTTPS, se describe la hipótesis y las variables del proyecto.

En el capítulo dos, se detalla el marco teórico de la investigación la cual contiene las generalidades investigativas del protocolo TLS (Transfer Layer Socket) y las comunicaciones en la capa de transporte, también se detallan conceptos claves que son necesarios para su entendimiento, como son los algoritmos, seguridades y la arquitectura que será utilizada para plantear la solución.

En el Capítulo tres, se muestra el marco metodológico, el cual está constituido por el tipo y diseño de la investigación, la población y muestra, la hipótesis, variables, operacionalización, Métodos, técnicas e instrumentos de recolección de datos, procedimiento para la recolección de datos, Análisis Estadístico e Interpretación de los datos, principios éticos y criterios de rigor científico.

En el Capítulo cuatro, se muestran los resultados obtenidos y estimados, en base al diagnóstico realizado.

En el Capítulo cinco, se muestra la propuesta de investigación, se describe

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

detalladamente las características, estructura, herramientas, etc., de la propuesta elaborada (expedientes técnicos, diseños y estudios de factibilidad).

Asimismo, se muestran las conclusiones y recomendaciones **En el capítulo seis,** orientadas a los objetivos específicos y los factores críticos de éxito.

Finalmente, se muestran las referencias bibliográficas y en los anexos la documentación tal como: La propuesta de solución planteada, las fichas de evaluación de la propuesta e instrumento de recolección de datos y el instrumento de recolección de datos.

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

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1. Situación problemática

Las redes de comunicaciones actuales permiten la conectividad de un gran número de usuarios que pueden estar situados en cualquier parte del mundo, tanto para transmisión de voz (red telefónica), imágenes (redes de distribución de televisión, TV vía satélite) como para la transmisión de datos entre ordenadores (redes locales, metropolitanas, así como redes a nivel mundial, como por ejemplo Internet). La explosión de servicios ofrecidos por estas redes, especialmente las de datos, ha incrementado la dependencia de individuos y organizaciones de la transmisión de datos por estas redes. Esta dependencia ha despertado la conciencia de la necesidad de protección de la información y de garantizar la autenticidad de datos y mensajes, (Forné, Melús, & Soriano, 2011).

El volumen de datos que se trasmiten en las redes se ha incrementado considerablemente, y en ocasiones suelen ser información sensible, por lo tanto es importante codificarlos para enviarlos por una red pública como lo es Internet de manera segura. El cifrado y descifrado de datos requiere un tiempo de cómputo adicional, que dependiendo de su tamaño puede ser considerable, (Pousa, 2011).

Para hacer frente a las amenazas a la seguridad del sistema, se definen una serie de servicios que realzan la seguridad de los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad.

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

No existe un único mecanismo capaz de proveer todos los servicios que se requieren, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información, (System, 2014).

Siendo múltiples las técnicas criptográficas para asegurar las comunicaciones, se tienen en cuenta:

Autenticación - Garantiza que los mensajes no son falsos y realmente provienen del remitente indicado.
Integridad - Similar a la función de checksum, garantiza que nadie ha interceptado y alterado el mensaje.
Confidencialidad - Garantiza que, si el mensaje es capturado, no podrá ser descifrado.

Existen a la fecha alrededor de 900 millones de páginas web, (Stats, 2015), pocas utilizan HTTPS como protocolo de transferencia de datos, siendo un porcentaje pequeño de páginas que utilizan seguridad al momento de transferir los datos.

Un 26.6% de alrededor de 144,531 sitios web analizados (Movement, 2015), resultan ser sitios seguros, lo que nos da un 76.4% de sitios que presentan seguridad inadecuada.

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

1.2. Formulación del problema

¿Cómo mejorar la seguridad de las comunicaciones en la capa de transporte?

1.3. Delimitación de la Investigación

La investigación se realiza en las instalaciones de la Universidad Señor de Sipán, a cargo de los estudiantes Renzo Augusto Ariansen Moncada, José Iván Rojas Díaz, el ingeniero Alex Franklin Coronado Navarro, en los meses de Abril a Diciembre del 2015

1.4. Justificación e importancia

Debido a la creciente demanda de resguardar los datos de cualquier entidad, es necesario que el transporte de la información se realice de forma segura, sobre todo en el acceso y la modificación desde sitios remotos debidamente acreditados, por lo que se requiere la implementación de herramientas y dispositivos que nos permitan minimizar los riesgos para que la información no sea comprometida.

Para dar seguridad al tráfico de información en una red, además de proteger y autenticar la información en todas las operaciones no seguras, se debe de pensar en cifrar los datos y generar túneles entre sitios remotos para minimizar los riesgos de posibles amenazas.

La investigación permitirá comparar los algoritmos de cifrado para determinar mediante diferentes indicadores cual combinación es más convenientes en diferentes términos, y así poder implementarla.

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

1.5. Objetivos de la Investigación

Objetivo general

Implementar protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte.

Objetivos específicos

a. Diagnosticar el estado actual de la seguridad de las comunicaciones en la capa de transporte.
b. Analizar los algoritmos de cifrado.
c. Diseñar un modelo de protocolo de cifrado.
d. Implementar algoritmos de cifrado.

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

CAPITULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

Dentro del ámbito Criptográfico e Implementación de sistemas de seguridad utilizando protocolos de seguridad HTTPS (SSL/TLS) se han hecho una serie de investigaciones y publicaciones, dentro de los cuales podemos destacar los siguientes:

2.1.1 A nivel internacional

(Ordeñez Calero, 2013) En su tesis titulada: “Desarrollo del módulo de gestión de información técnica para TELALCA S.A e implementación de seguridad mediante cifrado SSL del protocolo HTTPS”. Cuyo objetivo es: “Implementar las interfaces que permitan gestionar la información técnica necesaria de los clientes, así mismo las reglas del negocio y garantizar la seguridad de la información mediante implantación de cifrado SSL del protocolo HTTPS. Los resultados obtenidos fueron: “El módulo de administración de información técnica cumple con la funcionalidad requerida por los usuarios y definida en la fase de requerimientos y el sistema garantiza un acceso seguro a la información mediante el cifrado SSL del protocolo HTTPS”. La tesis concluye en que: “Gracias al sistema, el personal técnico de campo puede conocer más fácilmente los datos técnicos necesarios del cliente y las últimas actividades realizadas para dar solución a los problemas presentados, a la vez la implementación del protocolo de seguridad HTTPS en el acceso, la transmisión de la información se realizará mediante un canal cifrado”. Finalmente recomienda:” Se recomienda que para el desarrollo de aplicaciones web se utilice el

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

marco de trabajo Struts, ya que permite la reutilización de código y soporta múltiples interfaces de usuario (HTML, JSP, etc.)".

(Hernández Ortiz , Peña Blanco, Ramirez Amaya, Rodriguez Baños, & Acosta Gil , 2010) En su tesis titulada: "Implementación de un túnel con cifrado para transporte de datos". Cuyo objetivo es: "Implementar un esquema seguro de protección de la información que cifre los datos a través de túneles basados en el protocolo SSL". Los resultados obtenidos fueron: "En el desarrollo de esta tesina se obtuvo la transmisión cifrada de mensajes de syslog con herramientas de código abierto como lo son Stunnel y OpenSSL entre dos máquinas conectadas a través de una red pública de datos recibiendo los beneficios de la confiabilidad de TCP". La tesis concluye: "La implementación realizada, se cubrió el objetivo planteado al inicio del proyecto, implementando un esquema seguro de protección de la información, que en éste caso fueron las bitácoras de syslog, las cuales viajaron cifradas entre un cliente y un servidor dentro de un túnel basado en el protocolo SSL".

(Haro Montero & Gavilanes Sagñay, 2010) En su tesis titulada: "Análisis de funciones criptográficas de código libre en los protocolos SSL y TLS aplicado al portal web de la jefatura provincial de tránsito de Chimborazo". Cuyo objetivo es: "Analizar y comparar las herramientas de código libre para la administración de funciones criptográficas en los protocolos SSL Y TLS aplicado al desarrollo del portal web de la jefatura provincial de

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

transito de chimborazo". Los resultado obtenidos fueron: "OpenSSL es la herramienta que obtiene el mejor resultado con un 93.33% debido a características como la facilidad de uso, difusión, mejor soporte técnico y su funcionalidad. Con un 83.33% GnuTLS está ubicado en la segunda posición y NSS en la tercera posición con un 62.22%. La seguridad de las tres herramientas comparada desde el punto de vista de la fortaleza de sus algoritmos criptográficos y los protocolos implementados por dichas herramientas se puede decir que existe un empate técnico, debido a que GnuTLS y NSS utiliza por defecto el protocolo TLS 1.0 que es equivalente al protocolo SSL 3.0 que utiliza por defecto OpenSSL. En cuanto a la implementación de algoritmos criptográficos y la longitud de sus claves trabajan de forma muy parecida. OpenSSL funcionalmente es mejor porque presenta un mayor número de sub herramientas que permite la creación de claves públicas, privadas y certificados digitales firmados por una propia CA de forma más transparente y organizada, GnuTLS está ubicado en segundo lugar por la documentación que presenta de las sub herramientas implementadas, y NSS tiene el tercero ya que su documentación no es muy comprendida por lo que es menos amigable. OpenSSL es más portable ya que es posible instalar en un mayor número de sistemas operativos y de una forma más sencilla, además es usado en un mayor número de aplicaciones que implementan seguridad ocultando la información. GnuTLS y NSS le siguen obviamente por tener un menor número de aplicaciones que usan sus librerías lo cual se puede deber

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

a su tiempo de vida.

(Villegas Gómez, 2010) En su tesis titulada: “Comparativa de seguridad de algoritmos de cifrado asimétrico”. Cuyo objetivo es: “Con base en la revisión bibliográfica de los tres algoritmos de cifrado de llave pública de la información RSA, ElGamal, y ECES, los cuales proveen el servicio de confidencialidad, estudiar y entender su funcionamiento para posteriormente obtener las ventajas y desventajas de cada uno, con la finalidad de recomendar los casos prácticos dentro de los cuales cada uno de dichos algoritmos pueden ser utilizados”. Los resultados obtenidos fueron:” La comparación entre los sistemas criptográficos detalla puntos primordiales y eligiendo la mejor: En cifrado (ElGamal con primo de 1024 bits con 480), en descifrado (RSA modulo n de 1024 bits con 384), en firma (RSA modulo n de 1024 bits con 384), verificación (ElGamal con primo de 1024 bits con 480)”. La tesis concluye: “Se realizó una revisión de los algoritmos de cifrado basados en criptografía asimétrica RSA, ElGamal y ECES con la finalidad de tener una visión clara de cómo pueden utilizarse dentro de una arquitectura de cifrado de la información en una organización. La revisión de los citados algoritmos consideró el funcionamiento de cada algoritmo para poder entender las fortalezas y debilidades que presentan y por añadidura las ventajas y desventajas de su uso dentro de sistemas de cifrado en las organizaciones. Los algoritmos revisados se concluye que actualmente es más recomendable la implementación del RSA debido al nivel de seguridad y madurez que tiene”. Finalmente se recomienda: “Es recomendable

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

tener más opciones que permitan hacer frente a alguna eventualidad con el funcionamiento del algoritmo principal, Debido a esto se hace mención a que es una buena medida implementar el algoritmo ElGamal como una segunda opción e iniciar una implementación de prueba del algoritmo ECES, debido a que aún no alcanza el nivel de madurez y soporte que requiere una solución a la que se apostará la seguridad de la información de la organización en cuanto confidencialidad se refiere".

(Morales Lara, 2010) En su tesis titulada: "Análisis de los algoritmos de cifrado de llave secreta y su uso dentro de una organización pública". Cuyo objetivo es: Analizar su funcionalidad de algoritmos de cifrado de llave secreta con la finalidad de proponer su inclusión dentro de una arquitectura de cifrado de la información". Los resultado obtenidos fueron: "Se mostró el análisis mediante el funcionamiento, pruebas, fortaleza y vulnerabilidades de algunos de los algoritmos simétricos recomendados por los organismos internacionales NIST, NESSIE y CRYPTREC, con el fin de seleccionar uno de ellos y de recomendar su inclusión dentro de una arquitectura de cifrado de la información de una organización para mantener actualizado su sistema de cifrado de la información". La tesis concluye: Para la elección de los 5 algoritmos a analizar, se consideraron las recomendaciones y los estudios de los organismos en mención, así como las actuales aplicaciones criptográficas en las diversas organizaciones para estar en posibilidad de intercambiar información a nivel organizacional si las condiciones así lo

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

ameritan. Finalmente recomienda: “Se propone el uso del algoritmo criptográfico CAMELLIA. Con el uso de dicho algoritmo se busca incrementar la confidencialidad de la información en la organización ya que como se aprecia, es un algoritmo robusto, resistente a criptoanálisis y avalado por los organismos anteriormente citados, los cuales cuentan con amplio prestigio en materia criptográfica a nivel internacional”.

(Gallegos García, 2011) En su tesis titulada: “Diseño de protocolos criptográficos para votación electrónica”. Cuyo objetivo es:” diseñar protocolos criptográficos para votación electrónica que dejen la fase del conteo de los votos en manos de “t” de “n” autoridades, ciudadanos y candidatos a elegir. Todo esto mediante el uso de primitivas criptográficas de cifrado, firma, funciones hash y secreto compartido, con la finalidad de que los protocolos propuestos puedan ser utilizados dentro de un sistema de información que desarrolle las cuatro etapas de un proceso de votación electrónica”. Los resultado obtenidos fueron:” Se analizaron protocolos criptográficos para votación electrónica como emparejamientos bilineales, criptografía de umbral basado en identidad sin GLP y esquema de firma ciega; tomando requisitos como la seguridad, privacidad, elegibilidad, unicidad, no-coercibilidad, transparencia, exactitud y robustez. La tesis concluye:” El protocolo propuesto mejora las propuestas anteriores desde el punto de vista de las premisas de seguridad que tiene el hecho de trabajar con esquemas que basen su funcionamiento en emparejamientos bilineales”. Finalmente recomienda:” se

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

considera utilizar esquemas de firma de umbral basados en identidad, con la finalidad de continuar trabajando con la idea de distribuir la llave privada, de tal forma que cualquier subconjunto de 't' entidades con 't<n', sea capaz de obtener sombras de firmas".

(Chapaca Garzón & Rojas Bustamante, 2013) En su tesis titulada: "Análisis, diseño y desarrollo de un prototipo de protocolo de transporte basado en comunicación TCP con capacidad de cubrir las necesidades de transferencia de datos seguros, confiables y de alta disponibilidad".
Cuyo objetivo es: "Analizar, diseñar y desarrollar un prototipo de protocolo de transporte basado en comunicación TCP con capacidad de cubrir las necesidades de transferencia de datos seguros, confiables y de alta disponibilidad. ".Los resultados obtenidos fueron: "Tomando en cuenta los puntos fundamentales como confiabilidad (ETCP permitirá asegurar la entrega confiable de los datos desde su punto de origen hacia su punto de llegada asegurándose que siempre la información llegue de manera constante se encuentre disponible), disponibilidad (ETCP protege de interrupciones o caídas de forma automática y en un corto plazo de tiempo con el fin de mantener siempre disponibilidad para la transferencia de datos) y encriptación(En las pruebas realizadas se probó el nivel de encriptación de los mensajes, concepto que va de la mano con la seguridad, en este punto se pudo lograr el cometido principal ya que la lectura del contenido del mensaje era difícil de descifrar, cabe recalcar que en este punto no existe algoritmos empleados que den el 100% de

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

seguridad al momento de encriptar la información, pero en el cometido se puede asegurar que cumple con la funcionalidad de no dar a conocer a cualquiera el contenido de los mensajes enviados por la red)“. La tesis concluye en que: “Los protocolos de comunicación existentes ofrecen diferentes características de seguridad, confiabilidad y disponibilidad, sin embargo del estudio realizado se ve que existe la posibilidad de proponer mejoras e implementar un nuevo prototipo de protocolo de transporte como es ETCP, el cual está basado en el actual protocolo TCP por lo que el resultado obtenido es el de brindar mejoras de seguridad, confiabilidad y alta disponibilidad en cada proceso de comunicación que se realiza en comparación al actual protocolo TCP. “.Finalmente recomienda:” Buscar una secuencia de puertos que no hayan sido usados aún, de esa manera la aplicación desarrollada creara los enlaces directamente sin necesidad de preguntar el puerto donde se levantara. Implementar un modelo de programación multi-hilo, para que de esta manera la aplicación sea menos vulnerable a fallos que se pueden presentar durante el proceso de envío de información. Usar la tecnología WPF de Microsoft para mejorar la funcionalidad del prototipo propuesto ya que este contiene librerías las cuales soportan la concurrencia en la transmisión de datos“.

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

(Perales Paz & Villajuan Guzmán, 2003) En su tesis titulada: “Transmisión de datos vía TCP/IP en tiempo real” Cuyo objetivo es: “Realizar la investigación, estudio, desarrollo e implementación de un sistema de transferencia de datos vía TCP/IP en tiempo real. Este sistema se encarga de emitir como de recibir paquete de datos previamente, codificados de acuerdo a las circunstancias, a través de la red (corporativo o local).” Los resultados obtenidos fueron: “Se establecieron variables de evaluación tales como la seguridad, performance, costo en H & S, tiempo de procesamiento; en el tema de la seguridad, si la aplicación no contaba con elementos de seguridad se encontraría en desventaja respecto a la aplicación web. Ya que para el procesamiento actual se cuenta con procedimientos de generación de páginas web que por ser estáticas tienen únicamente carácter de lectura.

En cambio para la aplicación desarrollada por existir flujo de información en tiempo real entre diversos usuarios, se requiere que la información fluya de manera segura, y entones se dispuso del SSL como alternativa para lograr este cometido. La tesis concluye en que:” Se logró la comunicación mediante TCP entre diferentes aplicaciones desarrolladas en distintas herramientas de software (Microsoft, Sun) y sobre diferentes plataformas (Windows, Unix, Linux), estas fueron una aplicación servidor desarrollado en ANSI C, aplicación servidor java y aplicación cliente bajo Windows. La información que proviene de la aplicación servidor a la aplicación cliente es

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

actualizada de manera automática, sin saber de por medio algún mecanismo ejecutado por parte del usuario; en cambio en la aplicación web se requiere el usuario ejecute un evento para refrescar la información en una página web (presionar el botón actualizar navegador)". Finalmente recomienda:" Utilizar un archivo de configuración para los casos en el cual se definen las variables que puedan sufrir cambios de tal manera que la aplicación sea flexible, permitiéndonos cambiar algunas variables de manera dinámica, por ejemplo, la ruta completa donde se encuentre la aplicación dependiendo del sistema operativo Windows , Linux o Unix ya que cada uno de ellos maneja diferentes sistemas de archivos, además otras variables que pueden cambiar son el "host" donde se ubica la aplicación servidor, el puerto que servirá de escucha para la aplicación servidor. Tener presente el desarrollo de módulos de encriptación, durante la autenticación y durante el envió de información ya que esto; es parte del nivel de seguridad que debería tener todo sistema de transferencia de datos.

(Martinez Garcia, 2011) En su tesis titulada: "Estudio del algoritmo de encriptamiento RSA y TRIPLE DES para mensajes financieros basados en un módulo de seguridad de hardware utilizado en las transferencias interbancarias". Cuyo objetivo es: "Garantizar la confidencialidad, la autenticidad, la integridad y el no repudio del mensaje financiero que se intercambia entre instituciones financieras a nivel mundial a través de un sistema de comunicaciones seguro". Los resultados obtenidos fueron:

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

"El sistema de comunicaciones financiera que se empleo fue SWIFT, el cual es totalmente estable (incluyendo sus sistemas de contingencia), con capacidad para intercambiar información con total seguridad y de forma fiable". La tesis concluye en que: "La seguridad de la información del mensaje financiero no solo se garantiza por las técnicas de encriptamiento, también se garantiza por la red de comunicaciones SWIFT sobre el cual se traslada, debido a que esta red es segura y fiable. SWIFT entrega los HSM a sus clientes para obtener una configuración estandarizada en sus módulos de seguridad de hardware, si un cliente obtiene un HSM que no es entregado por SWIFT, todas sus operaciones criptográficas sobre los mensajes financieros no serían validados por SWIFT. Las claves criptográficas contenidas en las cajas HSM solo pueden ser copiadas en la otra caja que se encuentra en clúster, es decir, estas claves no pueden ser copiadas fuera del clúster (por ejemplo: un servidor de archivos o de base de datos). El encriptamiento por software es lento porque se instala en un computador que comparte sus recursos informáticos (como memoria, procesador) con otras aplicaciones. El encriptamiento por hardware es rápido porque dedica todos los recursos informáticos del dispositivo de hardware para realizar todas las operaciones criptográficas. Las cajas HSM tienen particularidad de tener mayor resistencia a la intrusión física. Como el manipuleo, si se detecta una intrusión de desmontaje o modificación del mismo, este dispositivo debe ser capaz de borrar los parámetros de seguridad críticos. SWIFT es sometido a supervisión debido a su importancia de hacer que todo el

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

sistema financiero funcione sin problemas, por ello se forma un comité que periódicamente revisa muchos puntos informáticos, como en el presente caso: La magnitud de la clave o el tipo de algoritmo a emplear, para así poder mitigar los riesgos operacionales. Cuando el respectivo comité observe que la longitud de la clave o el algoritmo actual ya no son tan seguros, considerara realizar los cambios apropiados. Finalmente recomienda:" Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo, es decir, para una atacante no debería ser de mucha ayuda conocer el algoritmo que se está utilizando. Solo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Debido a que toda la seguridad está en la clave, el espacio de claves posibles debe ser muy amplio. El triple DES es un algoritmo simétrico que está desapareciendo lentamente, siendo reemplazado por el algoritmo simétrico AES. Por su diseño, el DES y por lo tanto el triple DES son algoritmos simétricos lentos. Actualmente, el algoritmo AES puede llegar a ser hasta 6 veces más rápido y es un algoritmo simétrico mucho más seguro, por ello es recomendable que se considere este punto en el comité de seguridad informática que supervisa periódicamente a SWIFT. Es recomendable que las cajas HSM tengan una configuración de alta disponibilidad, es decir se encuentren en clúster para evitar tiempos muertos ante la inoperatividad de uno de ellos.

(Jiménez Bazán, 2000) En su tesis titulada: "Implementación de un sistema cliente/servidor para transmisión encriptado de voz y datos sobre una red local

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

utilizando DSP'S". Cuyo objetivo es: "Implementar una plataforma de transferencia de información, la cual sea montada sobre una red local, en la cual se pueda transmitir archivos de datos y voz en tiempo real adicionando seguridad en la transmisión a través de métodos de encriptación y compresión de voz". Los resultados obtenidos fueron: "La aplicación proporciona mayor velocidad de procesamiento utilizando la comunicación paralela como interface de intercambio de información entre la PC y el DSP. De este modo los datos son transmitidos en forma paralela, y se hace necesario conocer la máxima velocidad de transmisión de datos, para ello se analizó los dos casos propuestos, transmisión PC-DSP (la comunicación es en base al puerto paralelo, por el lado de la PC, y por el puerto digital B por el lado del DSP56002(constituido por 15 pines de propósito general, configurable mediante software para trabajar ya sea en modo entrada como salida)) y Transmisión DSP-PC(Este proceso inverso se utiliza la misma filosofía del caso anterior, es decir, la comunicación utiliza acuse de recibo para la señalización, pero utiliza otros pines en cada interface para lograr la transmisión para recibir los datos hacia la PC ya no se poseen los 8 bits de datos debido a que son utilizados como salida)". La tesis concluye en que: "Se analizó casos de comunicaciones en los que los sistemas tradicionales no garantizan seguridad en la transmisión y enfatizado la necesidad de implementar una plataforma de seguridad para casos específicos de comunicaciones, se demostró la capacidad de IDEA como método de encriptación y puesto en manifiesto la

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

factibilidad y conveniencia de implementar una solución de IDEA sobre hardware, debido a las características del algoritmo. Se analizó las dos metodologías de encriptación y se concluyó que PGP es la más óptima en este caso, debido a que la aplicación está orientada a comunicaciones punto a punto, donde la trasferencia de información es un sentido y no orientada a multipunto". Finalmente recomienda:" Analizar la posibilidad de implementación de IDEA en otros dispositivos DSP tales como procesadores de coma flotante, o dispositivos de menos cantidad de bits tales como 16, verificando si la posible solución proporciona los niveles de seguridad adecuados, y de ser así evaluar y posiblemente implementar esta."

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

2.2. Estado del arte

A continuación se presenta una serie de estudios realizados con referencia a la seguridad informática, protocolos de transferencia de datos y algoritmos de encriptación, mostrándonos grandes rasgos de cómo ha evolucionado:

2014

(Padron Godínez, Prieto Meléndez, Herrera Becerra, & Calva Olmos, 2014)

Se han desarrollado varios escenarios como casos de estudio para la implementación de protocolos seguros, mediante algoritmos criptográficos para garantizar servicios de seguridad en el diseño. Como se mencionó en algunos casos la confidencialidad, integridad, autenticidad dentro de los protocolos la podemos garantizar de manera confiable mediante técnicas de Criptografía, por ello debemos conocer los mecanismos de seguridad, es decir, los cifradores a implementar ya sea en software o hardware. Además tenemos que poder operar la información en bloques o flujo de bloques para la transmisión. Este reporte nos ayudará en forma general a implementar seguridad a los protocolos de comunicación que se emplearán para las telecomunicaciones que se quieren llevar a cabo con satélites artificiales de uso científico. Como trabajo a futuro se estudiará la operación de los equipos y los parámetros de telecomunicaciones para subir comandos y bajar información de los satélites en órbita, así como el rastreo de los mismos en forma segura. Otra aplicación directa de los protocolos de comunicación seguros son las urnas electrónicas que se emplean en votaciones o elecciones de candidatos.

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

(Shazia Riaz, Shafia, Asma Sajid, & Madiha Kanwal, 2014)
La Internet se ha convertido, sin duda, la más grande red pública de datos, permitiendo y facilitando tanto personal como comunicaciones empresariales de todo el mundo. Mientras que el Internet tiene abierto la puerta a un número cada vez mayor de las amenazas de seguridad a partir del cual las empresas deben protegerse. Con el crecimiento de Internet, muchas aplicaciones necesitan segura transmitir datos a aplicaciones remotas y ordenadores. TCP / IP traje de protocolo es parte fundamental para la comunicación por cualquier red, por medio de que TCP / IP con la colaboración de SSL / TLS proporciona la seguridad sólida. SSL está diseñado para resolver los problemas de seguridad como un estándar abierto. Secure Sockets Layer (SSL) es el protocolo de seguridad de Internet de punto a punto de conexiones. Este estudio se centra en el análisis del rendimiento de SSL / TLS con diferentes protocolos, así como que nos llevará a aprender sobre el comportamiento limitante de SSL / TLS en TCP / IP. Además, las futuras ampliaciones de SSL / TLS deben ser parte de este investigación.

(Philco Iphilcoa & Rosero Irosero, 2014)
Los clientes, usuarios, consumidores, etc., de bienes o servicios en línea no tiene plena seguridad de las transacciones comerciales que efectúan, pues la información personal es susceptible de ser interceptada por expertos en informática, los números de tarjetas de 2013, registra a 2.321 ecuatorianos, que presentaron denuncias por fraudes informáticos. Aun así no existen que pierden las víctimas por estos delitos, que originan pérdidas económicas a clientes y los mismos empresarios. Este trabajo académico utiliza el método analítico para investigar el

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

objeto de estudio, para plantear un modelo de procedimiento de seguridad informática de transacciones comerciales en el país. Muchas empresas deben implementar infraestructuras seguras para brindar línea, una de esas estrategias puede ser el cifrado en sus transacciones en línea. Los informes estadísticos de fraude informático en el país, se concluyen que se debe con el uso de protocolos de seguridad robustos, además los usuarios deben adoptar una cultura de seguridad informática.

2013

(Francisco Diaz & Venosa, 2013)

El auge de la firma digital para asegurar transacciones en Internet es un hecho que no se puede pasar por alto hoy en día. Si bien la firma digital de mensajes de correo electrónico y de transacciones WEB es muy importante, existen un sinnúmero de aplicaciones que se pueden beneficiar al introducir un esquema de seguridad que tenga como eje la firma digital (para garantizar, por ejemplo, autenticidad y no repudio). El presente artículo describe los puntos más importantes para construir una aplicación de este tipo.

La propuesta se ilustra con un prototipo desarrollado y operativo en el LINTI, laboratorio de la Facultad de Informática de la Universidad Nacional de La Plata, llevado a cabo por Verónica Fredes y Paula Venosa.

(Lin Rivest, Shamir, & Adleman, 2013)

La era del correo electrónico pronto puede estar sobre nosotros; debemos asegurarnos de que dos propiedades importantes del sistema de correo actual se conservan:

(a) Los mensajes son privadas, y (b) los mensajes se pueden

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

firmar. Se demuestra en este trabajo cómo construir estas capacidades en un sistema de correo electrónico.
En el corazón de nuestra propuesta es un nuevo método de cifrado. Este método ofrece una implementación de un sistema de cifrado de clave pública, un concepto elegante inventado por Diffie and Hellman]. Su artículo motivó nuestra investigación, ya que presentaron el concepto pero no cualquier aplicación práctica de tal sistema.

(Cabrera Aldaya & Cabrera Sarmiento, 2013)
En este trabajo se integran implementaciones hardware de algoritmos criptográficos a la biblioteca OpenSSL la cual es utilizada por aplicaciones sobre el sistema operativo Linux para asegurar redes TCP/IP. Los algoritmos implementados son el AES y las funciones resumen SHA-1 y SHA-256. Estos algoritmos son implementados como coprocesadores del procesador MicroBlaze utilizando interfaces FSL para el intercambio de datos entre ellos. Estos coprocesadores son integrados dentro de la biblioteca OpenSSL considerando la naturaleza multitarea del sistema operativo Linux, por lo que se selecciona un mecanismo de sincronización para controlar el acceso a estos dispositivos. Además son presentados los resultados de velocidad alcanzados por los coprocesadores integrados en la biblioteca utilizando la herramienta speed de la misma. Finalmente es presentado el impacto de estos coprocesadores en la velocidad de transmisión a través de una red privada virtual utilizando la herramienta OpenVPN.

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

(Benton & Bross, 2013)

Nuestro experimento reveló que los ataques MITM SSL tienen patrones de tiempo que podría ser identificada por la observación de las víctimas. Más específicamente, las herramientas de ataque que analizamos cambiaron la mayor parte de la demora al tiempo entre cuando se inició un protocolo de enlace SSL y cuando se recibió el certificado. Además, la mayor parte de la varianza en la RTT se eliminó cuando se conecta a los sitios de todo el mundo debido a los programas de MITM aceptar conexiones TCP inmediatamente. También presentamos métodos independientes de la temporización para revelar cuando se estaban utilizando las herramientas con MITM específicas que probamos.

2012

(Silva Pérez & Morales Luna, 2012)

La creación de sistemas de cómputo en ambientes móviles va de la mano con el uso de medios inalámbricos para transmitir la información necesaria. Dichos medios son ampliamente vulnerables a diversos ataques informáticos que atentan (entre otros) contra la confidencialidad, la integridad y la autenticación tanto de los datos como de los participantes en la comunicación. Debido a esto, es necesario crear mecanismos que permitan una comunicación segura. Uno de los mecanismos más ampliamente utilizados para ofrecer este servicio es sin duda la criptografía, la cual permite el desarrollo de diversos bloques de seguridad dependiendo de las necesidades del sistema, específicamente la infraestructura de clave pública (PKI, del inglés Public Key Infrastructure) ofrece servicios como integridad y autenticación.

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

En este trabajo se realiza un análisis de la importancia del desarrollo de una PKI tomando en cuenta un ambiente de dispositivos móviles, considerando ventajas y desventajas. En el análisis se hace una comparación entre los diferentes desarrollos existentes en la actualidad para la plataforma de desarrollo Android la cual ha ido ganando una enorme popularidad en los últimos años.

(Agulló, Guerra, Silva, & Vivanco, 2012)
En este informe, se pretende dar a conocer cómo es posible interceptar o vulnerar la privacidad de las conexiones en las redes de computadores, cómo se llaman estos ataques y cómo operan, a su vez, y acorde a los cambios tecnológicos que permiten la mejora de la confiabilidad en estas conexiones, se pretende también mostrar las soluciones actuales frente a estos ataques.
Esta seguridad en las conexiones se verá a través de múltiples capas, ya sea en la capa aplicación, capa de transporte, capa de red y capa de enlace. No puede haber un método de seguridad global, que abarque todas las capas, debido a que todas ellas operan de manera independiente, por lo que no están involucradas las unas de las otras.

(Hernández, Carreto, & Menchaca, 2012)
El desarrollo de la tecnología de comunicación basada en redes inalámbricas móviles ha proporcionado nuevas expectativas para el desarrollo de sistemas de comunicación, así como nuevos riesgos, por lo que es necesario implementar modelos de seguridad adecuados para esta tecnología, es por esa causa precisamente que se propone en el presente trabajo el desarrollo

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

de una aplicación basada en un Modelo de Seguridad para Redes la cual permitirá localizar la ubicación del usuario en cuanto este acceda a una aplicación utilizando su identificación personal, la cual estará asociada al dispositivo de comunicación con el cual se conecte a un servicio o red.

2011

(Forné, Melús, & Soriano, 2011)

Las redes de comunicaciones actuales permiten la conectividad de un gran número de usuarios que pueden estar situados en cualquier parte del mundo, tanto para transmisión de voz (red telefónica), imágenes (redes de distribución de televisión, TV via satélite) como para la transmisión de datos entre ordenadores (redes locales, metropolitanas, así como redes a nivel mundial, como por ejemplo Internet). La explosión de servicios ofrecidos por estas redes, especialmente las de datos, ha incrementado la dependencia de individuos y organizaciones de la transmisión de datos por estas redes. Esta dependencia ha despertado la conciencia de la necesidad de protección de la información y de garantizar la autenticidad de datos y mensajes.

En este artículo se presentan las amenazas a la seguridad en redes de transmisión de datos, así como los servicios de seguridad requeridos y los mecanismos necesarios para proveer estos servicios. Entre estos mecanismos destacan los criptográficos, tanto los sistemas convencionales (simétricos) como los de clave pública, concepto introducido en 1976 que produjo una revolución en el mundo de la criptología. Por último se introducen algunos de los algoritmos y aplicaciones criptográficas más extendidos en la actualidad o que de los que se prevé una mayor utilización en los próximos años.

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

2010

(Salgado, Ron, & Solis, 2010)

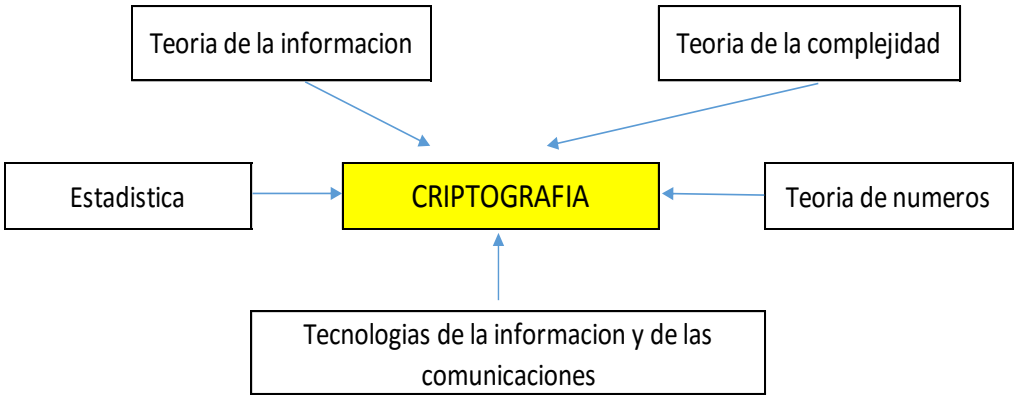
En la actualidad las aplicaciones web se han vuelto indispensables para el manejo de la información en una organización, convirtiéndose en una herramienta que permite al usuario acceder y utilizar un sistema informático a través de internet mediante un navegador web, permitiendo el acceso a la información desde cualquier parte del mundo. La Superintendencia de Bancos y Seguros al ser una institución Pública se ha visto obligada a la adopción de estándares abiertos y software libre para automatizar sus procesos, y ha desarrollado aplicaciones web utilizando la plataforma Java Enterprise Edition (JEE) sin embargo no se ha aplicado ningún tipo de estándar o buenas prácticas en el aseguramiento del aplicativo. El presente proyecto tiene como objetivo el análisis de riesgos de las aplicaciones web utilizando las recomendaciones OWASP Top 10 – para descubrir las vulnerabilidades que se presenta durante el desarrollo de un software y estimar el riesgo asociado para el negocio. A partir de los resultados obtenidos donde se identificaron La ocurrencia de almacenamiento criptográfico inseguro y protección insuficiente en la capa de transporte se realizó una propuesta de buenas prácticas para asegurar las aplicaciones, corregir los riesgos detectados y asegurar el proceso de desarrollo de nuevas funcionalidades y existentes.

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

2.3. Bases teórico científicas

Las raíces etimológicas de la palabra criptografía son Kriptos, que significa oculto, y graphos, que se traduce como escribir, lo que da una clara idea de su definición clásica: arte de escribir mensajes en clave secreta o enigmáticamente fue considerada un arte, hasta que Shannon público en 1949 la *Teoría de las comunicaciones secretas* [SHA49]. Entonces la criptografía empezó a ser considerada una ciencia aplicada, debido a su relación con otras ciencias, como la estadística, la teoría de los números, la teoría de la información y la teoría de la complejidad computacional.

Figura 1 Criptografía Teórica



Fuente: (Gil, 2002, pág. 1)

Teoría de los números

Desde siempre los números han tenido su encanto. K. F. Gauss, probablemente el matemático más destacado de los tiempos modernos, hace un par de siglos decía que la matemática es la reina de las ciencias y la teoría de los números la reina de las matemáticas.

Tales afirmaciones no son gratuitas. En pocas disciplinas es posible hacer tanto con tan poco material, o dicho de otra forma, se pueden plantear tantos problemas interesantes conociendo

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

solo unas cuantas definiciones básicas. Por otro lado, los problemas más bellos (unos podría agregar también los más difíciles) de las matemáticas se encuentran ligados de una u otra forma a la teoría de los números. El ejemplo clásico es seguramente la conjetura más famosa de las matemáticas, los ceros de la función Zeta de Riemann.

Ahora, dentro de la teoría de números, los números primos son una suerte de elegidos. Recordemos que un número p es primo si sus únicos divisores son él mismo y 1. Por ejemplo los números 2,3,4,5,7,11,13,17,19,23 son primos, mientras que 4,6,8,9,10,12,14,15,16,18 no son primos. Inmediatamente surge la pregunta: ¿hay infinitos números primos? Euclides demostró que sí.

Son los aportes científicos: Paradigmas, modelos y teorías, que orientan al análisis del problema y objeto de estudio, que permiten el enjuiciamiento crítico de las teorías.

Teoría de la información

Es la teoría relacionada con las leyes matemáticas que rige la transmisión y el procesamiento de la información. Más concretamente, la teoría de la información se ocupa de la medición de la información y de la representación de la misma (como, por ejemplo, su codificación) y de la capacidad de los sistemas de comunicación para transmitir y procesar información.

La codificación puede referirse tanto a la transformación de voz o imagen en señales eléctricas o electromagnéticas, como al cifrado de mensajes para asegurar su privacidad.

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

La teoría de la información fue desarrollada inicialmente, en 1948, por el ingeniero electrónico estadounidense Claude E. Shannon, en su artículo, A Mathematical Theory of Communication (Teoría matemática de la comunicación). La necesidad de una base teórica para la tecnología de la comunicación surgió del aumento de la complejidad y de la masificación de las vías de comunicación, tales como el teléfono, las redes de teletipo y los sistemas de comunicación por radio. La teoría de la información también abarca todas las restantes formas de transmisión y almacenamiento de información, incluyendo la televisión y los impulsos eléctricos que se transmiten en las computadoras y en la grabación óptica de datos e imágenes. El término información se refiere a los mensajes transmitidos: voz o música transmitida por teléfono o radio, imágenes transmitidas por sistemas de televisión, información digital en sistemas y redes de computadoras, e incluso a los impulsos nerviosos en organismos vivientes. De forma más general, la teoría de la información ha sido aplicada en campos tan diversos como la cibernética, la criptografía, la lingüística, la psicología y la estadística (Shannon , 1948).

Teoría de la estadística

La estadística es el arte y la ciencia de obtener información a partir de los datos. A efectos estadísticos, un dato significa una observación o medición, expresada en un número. Una estadística puede referirse a un determinado valor numérico derivado de los datos. Por ejemplo, las estadísticas del fútbol de 1ra división de Argentina consisten en el estudio de datos sobre ese juego; en cambio, el promedio de tiros al arco contrario de un equipo de fútbol es un estadístico (también llamado estadígrafo). La estadística incluye tres campos: métodos para 1) recopilar los

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

datos; 2) analizarlos, y 3) obtener inferencias a partir de los mismos. La evaluación estadística es muy relevante en diversos casos, que van desde las leyes y regulaciones anti-monopolio hasta los derechos políticos de una población. Razonar en términos estadísticos puede resultar crucial para interpretar test (o contrastes) psicológicos, estudios epidemiológicos, el tratamiento diferencial a los empleados de una empresa, y la toma de huellas dactilares de ADN, por mencionar algunas aplicaciones.

Capa de transporte

Según José Dordoigne "Es el núcleo del modelo OSI. En esta capa, se ponen en marcha distintos mecanismos para establecer el modo conectado, es decir, un medio para garantizar que la información se transmite sin problemas. El primer nivel de conexión consiste en un acuse de recibo sistemático de todos los paquetes recibidos, y esto, en un plazo determinado (dos veces la duración de ida y vuelta normalmente necesaria), porque, de lo contrario, el paquete se da por extraviado y se vuelve a transmitir. Además, el modo conectado ofrece una conexión para la capa superior, como si se tratase de un enlace punto a punto".

Según Jaime Lloret, miguel garcia & Fernando boronat "En esta capa se ven los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Segmenta los datos originados en el equipo emisor, los encapsula en PDUs de nivel de transporte (también llamados paquete de transporte), y les suministra a un servicio de transporte de datos. Verifica que los datos se transmiten correctamente. Realiza la conexión de extremo a extremo, invocando para ello el servicio del nivel de red."

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

Según Alexander Hermida M. & Inmaculada Iglesias F. "Proporciona el servicio de transferencia de datos de un extremo a otro de la red y puede incluir mecanismos de seguridad para garantizar la integridad de los mismos. Además, oculta los detalles de la red a la capa de aplicación."

Servicios Criptográficos

Seguridad de las Comunicaciones

El primer objetivo de los administradores de red es asegurar la infraestructura de la red, incluyendo routers, switches, servidores y hosts. Esto se logra utilizando técnicas de fortificación (hardening), control de acceso AAA, ACLs y firewalls y monitoreando amenazas utilizando IPS.

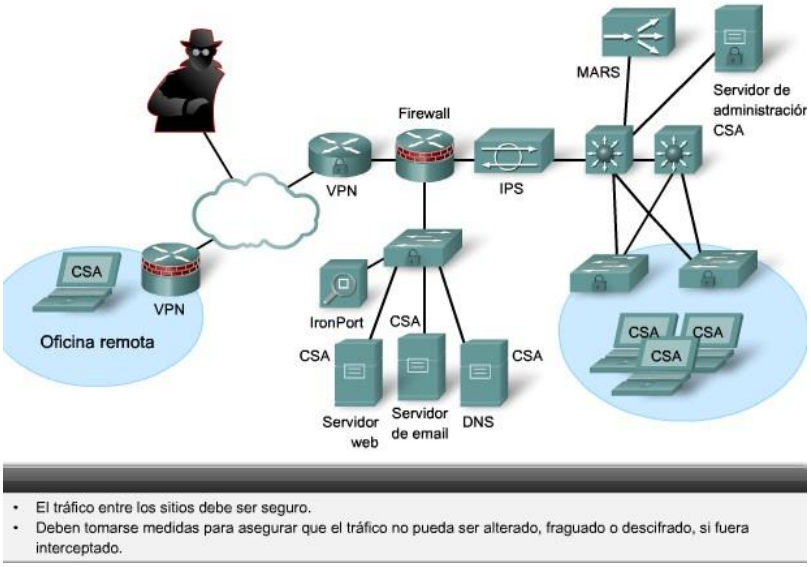
El siguiente objetivo es asegurar los datos a medida que viajan a través de diferentes enlaces. Esto puede incluir el tráfico interno, pero la mayor preocupación es proteger los datos que viajan por fuera de la organización hacia sucursales, trabajadores remotos y socios de negocios.

Asegurar las comunicaciones involucra algunas tareas principales:

Autenticación: Garantiza que los mensajes no son falsos y realmente provienen del remitente indicado. **Integridad**: Similar a la función de checksum, garantiza que nadie ha interceptado y alterado el mensaje. **Confidencialidad**: Garantiza que, si el mensaje es capturado, no podrá ser descifrado.

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

Figura 2 Seguridad de las comunicaciones



Fuente: Cisco

Autenticación

La autenticación garantiza que el mensaje proviene del origen del que dice provenir. La autenticación es similar a ingresar un número de información personal (PIN) seguro para realizar operaciones en un cajero automático. El PIN sólo debe ser conocido por el usuario y la institución financiera. El PIN es un secreto compartido que ayuda a prevenir fraudes.

La autenticación puede lograrse a través de métodos criptográficos. Esto es especialmente importante para aplicaciones y protocolos tales como IP o el correo electrónico, los cuales no poseen mecanismos incorporados para prevenir el fraude del remitente.

Integridad

La integridad de los datos asegura que los mensajes no son alterados durante su transmisión. Gracias a la integridad de los datos, el receptor puede verificar que el mensaje recibido es idéntico al mensaje enviado y que no hubo ninguna manipulación

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

intermedia.

Los nobles europeos aseguraban la integridad de datos de sus documentos lacrando los sobres. En general, el sello era creado sobre un anillo y solían incluir el escudo familiar, iniciales, un retrato o un símbolo o lema personal del propietario del anillo. Un sello intacto en un sobre garantizaba la integridad de su contenido. Además, garantizaba la autenticidad basándose en la impresión única del sello.

Confidencialidad

La confidencialidad de los datos asegura la privacidad, de forma tal que sólo el destinatario pueda leer el mensaje. El cifrado es el proceso de codificar los datos para que no puedan ser leídos por partes no autorizadas. Cuando hablamos de cifrado, los datos legibles son denominados texto plano o texto claro, mientras que la versión cifrada se denomina criptograma (en inglés, ciphertext). El mensaje legible en texto plano es convertido en un criptograma, el cual es ilegible. El descifrado revierte el proceso. Se requiere una clave para cifrar y descifrar un mensaje. La clave es el enlace entre el texto plano y el criptograma.

Históricamente, se han utilizado diferentes métodos y algoritmos de cifrado. Se dice que Julio César aseguraba sus mensajes tomando dos alfabetos, uno al lado del otro y luego desplazando uno de ellos un número específico de lugares. El número de lugares desplazados era la clave. Él convirtió texto plano en criptogramas utilizando esta clave y sólo sus generales, quienes también tenían la clave, sabían cómo descifrar los mensajes. Este método es conocido como Cifrado César.

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

Utilizar una función de hash es otra forma de asegurar la confidencialidad de los datos. Una función de hash transforma un conjunto de caracteres en una representación de la misma que suele ser más corta y de longitud fija. La diferencia entre el cifrado y el hashing es cómo se almacenan los datos. Con el texto cifrado, los datos pueden ser descifrados utilizando una clave. Con la función de hash, una vez que los datos son ingresados y convertidos utilizando dicha función, el texto plano se pierde. Los datos de hash sólo resultan útiles en comparaciones. Por ejemplo, cuando un usuario ingresa una contraseña, dicha contraseña es convertida en un hash y luego comparada con el valor de hash almacenado. Si el usuario olvida su contraseña, es imposible descifrar el valor almacenado y la contraseña debe restablecerse.

El propósito del cifrado y el hashing es garantizar la confidencialidad, de forma tal que sólo las entidades autorizadas puedan leer el mensaje.

Criptografía

Autenticación, integridad y confidencialidad son componentes de la criptografía. La criptografía es tanto la práctica como el estudio del ocultamiento de la información.

Los servicios criptográficos son la base de muchas implementaciones de seguridad y son utilizados para asegurar la protección de los datos cuando los mismos pueden quedar expuestos a partes no confiables. Comprender las funciones básicas de la criptografía y cómo el cifrado proporciona confidencialidad e integridad son partes importantes de la creación de una política de seguridad exitosa. También es importante comprender los problemas involucrados con la

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

administración de la clave de cifrado.

La historia de la criptografía comienza en círculos diplomáticos hace miles de años. Los mensajeros de las cortes reales llevaban los mensajes cifrados a otras cortes. Ocasionalmente, otras cortes no involucradas en la comunicación intentaban robar los mensajes destinados a aquellos reinos que consideraban adversarios. Poco tiempo después, los comandantes militares comenzaron a utilizar el cifrado para asegurar sus mensajes.

Criptoanálisis

Desde que existe la criptografía, existe también el criptoanálisis. El criptoanálisis es la práctica y el estudio para determinar el significado de la información cifrada (romper el código) sin tener acceso a la clave secreta compartida.

Criptología

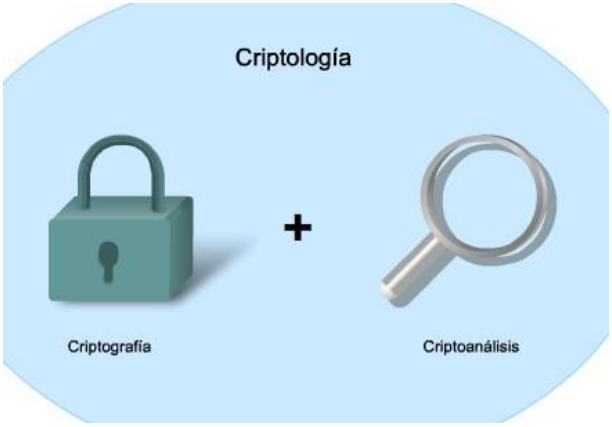
La criptología es la ciencia de crear y romper códigos secretos. Combina dos disciplinas separadas: la criptografía, que es el desarrollo y utilización de códigos y el criptoanálisis, que es la ruptura de dichos códigos. Existe una relación simbiótica entre ambas disciplinas, porque cada una hace mejor a la otra. Las organizaciones de seguridad emplean miembros de ambas disciplinas y los ponen a trabajar unos contra otros.

En algunos momentos de la historia, una de las disciplinas ha estado más avanzada que la otra. Por ejemplo, durante la Guerra de los Cien Años entre Francia e Inglaterra, los criptoanalistas se encontraban más adelantados que los criptógrafos. Francia creía que el cifrado Vigenere era irrompible. Sin embargo, los británicos fueron capaces de romperlo. Algunos historiadores creen que el resultado de la Segunda Guerra Mundial dependió mucho de que

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

el bando ganador fue mucho más exitoso en romper los códigos de su adversario que el bando perdedor. En la actualidad, se cree que los criptógrafos llevan la delantera.

Figura 3 Criptologia



Fuente: Cisco

En el mundo de las redes y las comunicaciones, la autenticación, la integridad y la confidencialidad de los datos se implementan de diversas formas, utilizando diferentes protocolos y algoritmos. La selección del protocolo y algoritmo varía de acuerdo al nivel de seguridad requerido para alcanzar las metas establecidas en la política de seguridad de la red.

Integridad y Autenticidad Básicas

Hash Criptográficos

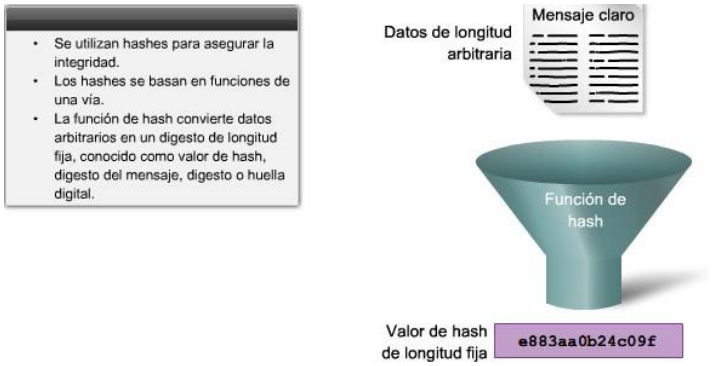
Una función de hash toma datos binarios, llamados mensaje y produce una representación abreviada del mismo, llamada digesto de mensaje. El hashing se basa en una función matemática de un solo sentido relativamente fácil de computar, pero significativamente más difícil de invertir. Moler café es un buen ejemplo de una función de un solo sentido. Es fácil moler granos de café, pero es casi imposible volver a juntar las

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

pequeñas partículas para reconstruir los granos originales.
La función de hashing criptográfico está diseñada para verificar y asegurar la integridad de los datos. Puede ser también utilizada para verificar la autenticación. El procedimiento toma un bloque variable de datos y devuelve una cadena de longitud fija, llamada valor de hash o digesto del mensaje.

La función de hash criptográfico se aplica en muchas situaciones diferentes:
Para proporcionar una prueba de autenticidad, cuando es utilizada con una clave secreta de autenticación simétrica, como IPsec o autenticación de protocolos de enrutamiento.
Para proporcionar autenticación generando respuestas de único uso de una vía a los desafíos de protocolos de autenticación como CHAP (PPP Challenge Authentication Protocol).
Para proporcionar pruebas de verificación de la integridad del mensaje, como en los contratos firmados digitalmente y certificados de infraestructura de clave pública (PKI), como los que deben aceptarse al acceder a un sitio seguro utilizando un navegador web.

Figura 4 Hash Criptográfico

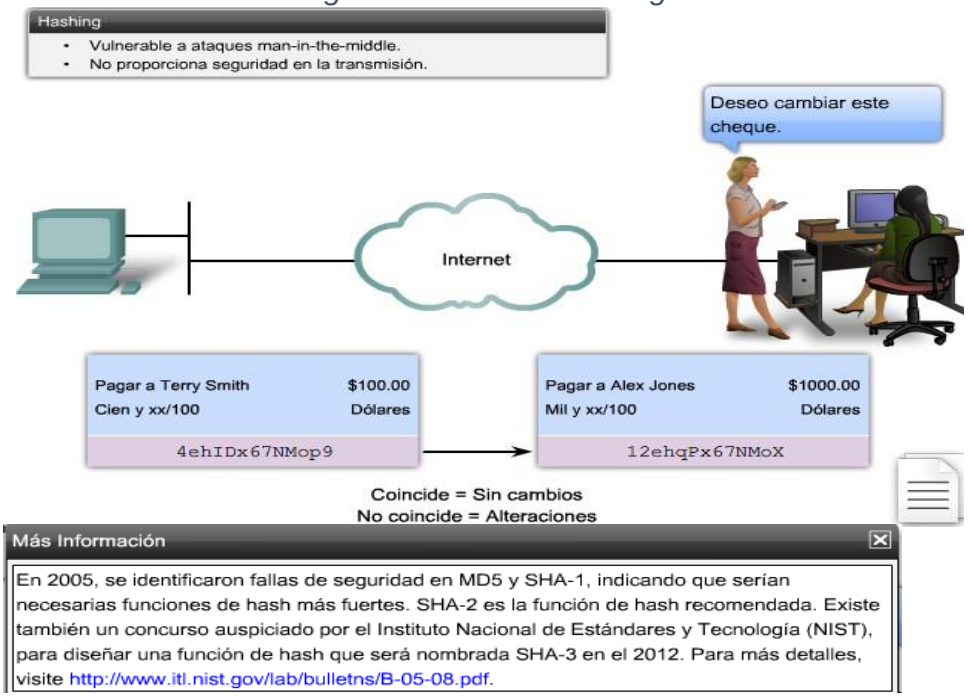


Fuente: Cisco

Matemáticamente, una función de hash (H) es un proceso que toma una entrada (x) y devuelve una cadena de longitud fija, llamada valor de hash (h). La fórmula para el cálculo es h = H(x).
Una función de hash criptográfico debe tener las siguientes propiedades: La entrada puede tener cualquier longitud.
La salida debe ser de longitud fija.
H(x) es relativamente fácil de calcular, cualquiera sea el valor de x.
H(x) es una función de un solo sentido y no es invertible.
H(x) es una función libre de colisiones, por lo que dos valores diferentes de entrada resultarán siempre en dos valores de hash diferentes.
Existen dos funciones de hash bien conocidas:
Message Digest 5 (MD5) con digestos de 128 bits
Secure Hash Algorithm 1 (SHA-1) con digestos de 160 bits

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

Figura 5 Proceso Hashing



Fuente: Cisco

Integridad con MD5 y SHA-1

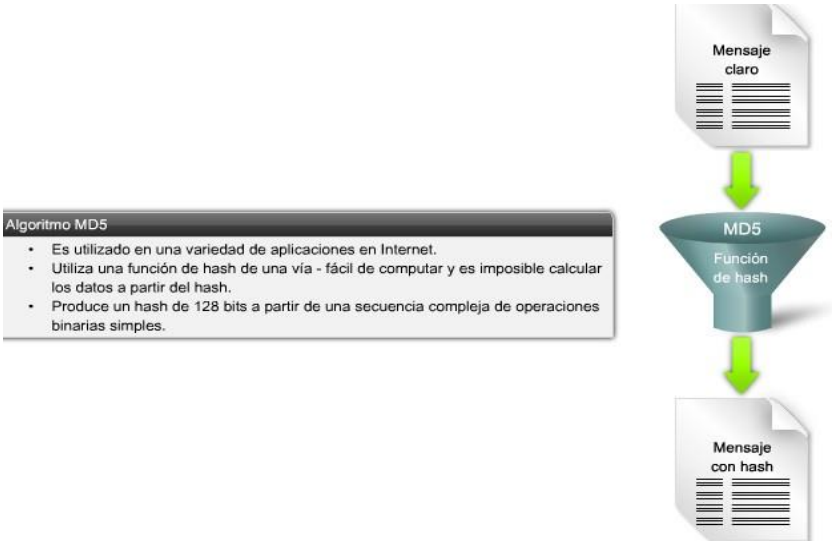
El algoritmo MD5 es un algoritmo de hashing desarrollado por Ron Rivest y utilizado actualmente por una amplia variedad de aplicaciones en Internet.

MD5 es una función de un solo sentido que facilita el cálculo de hash para los datos ingresados, pero vuelve inviable el cálculo de los datos originales dado un único valor de hash. MD5 es también libre de colisiones: es poco probable obtener el mismo valor de hash a partir de dos conjuntos diferentes de datos. MD5 es esencialmente una secuencia compleja de operaciones binarias simples, tales como OR Exclusivo (XOR) y rotaciones, que se ejecutan sobre los datos y producen un digesto del mensaje de 128 bits.

El algoritmo principal se basa en una función de compresión, la cual opera sobre bloques. La entrada es un bloque de datos más un resultado de bloques previos. Los bloques de 512 bits se dividen en 16 sub-bloques de 32 bits. Estos bloques son luego reordenados con operaciones simples en un bucle principal, el cual consiste en cuatro iteraciones. La salida del algoritmo es un conjunto de cuatro bloques de 32 bits que se concatenan para formar un único valor de hash de 128 bits. La longitud del mensaje se codifica así en un digesto.

MD5 se basa en MD4, un algoritmo anterior. MD4 ha sido decodificado y MD5 es ahora considerado menos seguro que SHA-1, según muchas autoridades de la criptografía.

Figura 6 Algoritmo MD5



Fuente: Cisco

El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos desarrolló SHA (Secure Hash Algorithm), el algoritmo especificado en SHS (Secure Hash Standard). SHA-1, publicado en 1994, corrige una falla no publicada de SHA. Su

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

diseño es muy similar al de las funciones de hash MD4 y MD5 desarrolladas por Ron Rivest.

El algoritmo SHA-1 toma un mensaje con menos de 2^64 bits de longitud y produce un digesto de 160 bits. El algoritmo es apenas más lento que MD5, pero al generar un digesto más largo, es más seguro contra ataques de colisión por fuerza bruta y ataques de inversión.

El NIST publicó cuatro funciones de hash adicionales para la familia SHA, cada uno con digestos más largos:

SHA-224 (224 bits)

SHA-256 (256 bits)

SHA-384 (384 bits)

SHA-512 (512 bits)

Estas cuatro versiones son conocidas en forma conjunta como SHA-2, aunque el término SHA-2 no ha sido estandarizado. SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512 son los algoritmos seguros de hash requeridos por ley para su utilización en ciertas aplicaciones del gobierno de los Estados Unidos, incluyendo su uso dentro de otros algoritmos y protocolos criptográficos, para la protección de información sensible no clasificada.

Tanto MD5 como SHA-1 se basan en MD4. Esto hace que MD5 y SHA-1 sean similares en muchos aspectos. SHA-1 y SHA-2 son más resistentes a los ataques por fuerza bruta, ya que sus digestos son al menos 32 bits más extensos que los digestos de MD5.

SHA-1 involucra 80 pasos, mientras que MD5 involucra sólo 64 pasos. El algoritmo SHA-1 además debe procesar un búfer de 160 bits, en lugar de los 128 bits de búfer de MD5. Debido a su menor cantidad de pasos, en general, MD5 se ejecuta con más rapidez, dado el mismo dispositivo.

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

Al seleccionar un algoritmo de hashing, es preferible usar SHA-1 o SHA-2 ante MD5. No ha sido probado que MD5 contenga fallas críticas, pero su seguridad es cuestionable en la actualidad. Si el desempeño es un problema, el algoritmo MD5 es levemente más rápido que el algoritmo para SHA-1. Debe considerarse que MD5 puede probarse como menos seguro que SHA-1.

Figura 7 Hashing e integridad de datos con MD5, SHA-1 y SHA256

En este ejemplo, se muestran los hashes resultantes a partir del texto plano utilizando MD5, SHA-1 y SHA256. Note la diferencia en la longitud de las claves entre los diferentes algoritmos. Cuánto más larga sea la clave, más segura será la función de hash.

Fuente: Cisco

Administración de Claves

La administración de claves suele considerarse la parte más difícil en el diseño de un criptosistema. Muchos criptosistemas han fallado debido a errores en su administración de claves y todos los algoritmos criptográficos modernos requieren procedimientos de administración del claves. En la práctica, la mayor parte de los ataques a los sistemas criptográficos están dirigidos al nivel de la administración de claves, en lugar del algoritmo criptográfico en sí. Existen algunas características esenciales a considerar sobre la administración de claves:

Generación: Era tarea de César seleccionar la clave de su cifrado. La clave del cifrador Vigenere también es seleccionada por el remitente y el destinatario. En los sistemas criptográficos

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

modernos, la generación de claves es en general un proceso automatizado y no llevado a cabo por el usuario final. Es necesaria la utilización de buenos generadores de números aleatorios para asegurar que todas las claves puedan ser igualmente generadas; así, los atacantes no pueden predecir qué claves tienen más posibilidades de ser utilizadas.

Verificación: Algunas claves son mejores que otras. Casi todos los algoritmos criptográficos tienen algunas claves débiles que no deberían ser utilizadas. Con la ayuda de procedimientos de verificación de claves, es posible regenerarlas si llegaran a aparecer.

Almacenamiento: En un sistema operativo multi-usuario moderno que utiliza criptografía, una clave puede ser almacenada en la memoria. Esto presenta un posible problema cuando la memoria es llevada al disco, ya que un troyano instalado en la PC puede tener acceso a las claves privadas de dicho usuario.

Intercambio: Los procesos de administración de claves deben proveer un mecanismo de intercambio de claves que permita resolver un acuerdo seguro sobre el material de generación de claves con el otro participante, probablemente sobre un medio no confiable.

Revocación y destrucción: La revocación notifica a todas las partes interesadas que una clave determinada ha sido comprometida y no debe seguir siendo utilizada. La destrucción elimina las claves viejas, evitando que los atacantes maliciosos puedan recuperarlas.

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

Se utilizan dos términos para describir a las claves: longitud de clave (key length) y espacio de claves (keyspace). La longitud de la clave es la cantidad de bits que la conforman, mientras que el espacio de claves es la cantidad de posibilidades que pueden generarse con una cantidad específica de bits. A medida que aumenta la longitud de la clave, el espacio de claves se incrementa en forma exponencial:

Una longitud de 2 bits (2^2) = espacio de claves de 4, porque existen cuatro claves posibles (00, 01, 10 y 11).Una longitud de 3 bits (2^3) = espacio de claves de 8, porque existen ocho claves posibles (000, 001, 010, 011, 100,101, 110 y 111).Una longitud de 4 bits (2^4) = espacio de 16 claves posibles. Una longitud de 40 bits (2^40)= espacio de 1.099.511.627.776 claves posibles.

Figura 8 Administración de claves

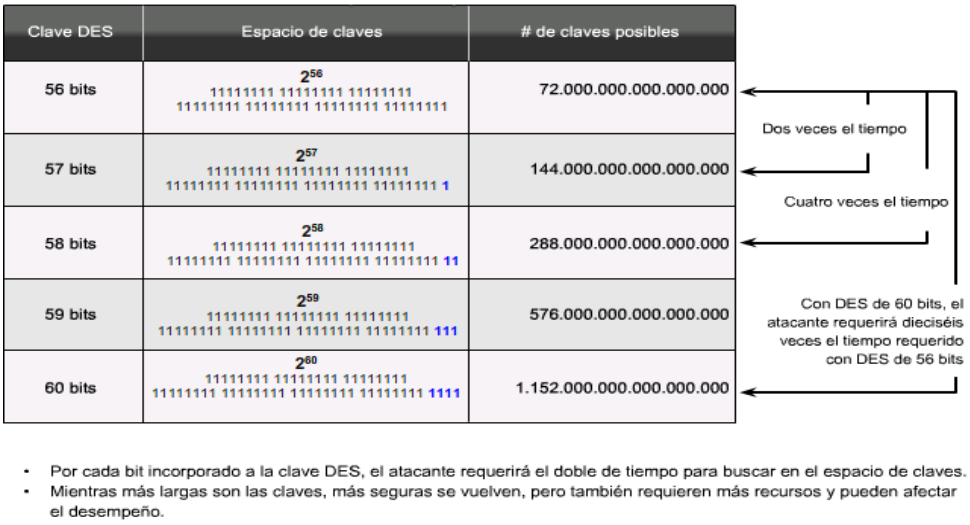
Fuente: Cisco

El espacio de claves de un algoritmo es el conjunto de todas las claves posibles. Una clave con una longitud de n bits produce un espacio de claves de 2^n posibles valores. Agregando un bit a la clave, se duplica el tamaño del espacio de claves. Por ejemplo, DES con sus claves de 56 bits tiene un espacio de claves mayor a 72.000.000.000.000.000 (2^56) combinaciones posibles.

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

Agregando un bit a la longitud de la clave, el espacio de claves se duplica y un atacante necesita el doble de tiempo para buscar entre todas las posibilidades.

Figura 9 Creación de claves criptográficas



Fuente: Cisco

Es posible crear diferentes tipos de claves criptográficas:

Claves simétricas, que pueden ser intercambiadas entre dos routers que soporten una VPN.

Claves asimétricas, utilizadas para asegurar aplicaciones HTTPS.

Firmas digitales, utilizadas para conectarse a un sitio web seguro.

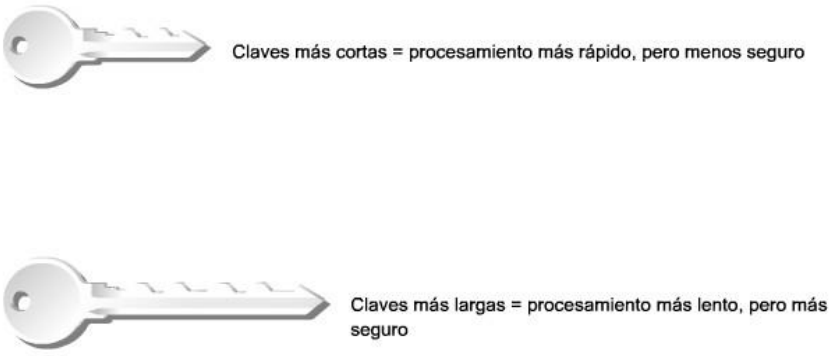
Claves hash, utilizadas en la generación de claves simétricas y asimétricas, firmas digitales y otros tipos de aplicaciones.

Sin importar el tipo de clave del que se trate, todas comparten problemas similares. Seleccionar una longitud de clave adecuada es un problema. Si el sistema criptográfico es confiable, la única forma de quebrarlo es mediante un ataque por fuerza bruta. El ataque por fuerza bruta consiste en una búsqueda a través de

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

todo el espacio de claves probando todas las claves posibles hasta encontrar una capaz de descifrar los datos. Si el espacio de claves es lo suficientemente grande, la búsqueda requiere una enorme cantidad de tiempo, volviendo impracticable el esfuerzo.

Figura 10 Longitud de claves



Fuente: Cisco

Confidencialidad

Cifrado

El cifrado criptográfico puede proporcionar confidencialidad en diferentes capas del modelo OSI, incorporando varias herramientas y protocolos:

El correo electrónico seguro, las sesiones seguras de base de datos (Oracle SQL*net) y la mensajería segura (sesiones de Lotus Notes) proveen confidencialidad a nivel de la capa de aplicación. Existen dos enfoques para asegurar la seguridad de los datos cuando se utilizan varios métodos de cifrado. El primero consiste en proteger los algoritmos. Si la seguridad de un sistema de cifrado se basa en mantener en secreto a los algoritmos en sí, debe custodiarse en extremo el código del algoritmo. Si se revela el algoritmo, cada una de las partes involucradas debe cambiar

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

de algoritmo. El segundo enfoque indica proteger las claves. Con la criptografía moderna, todos los algoritmos son públicos: las claves criptográficas son las que aseguran el secreto de los datos. Estas son secuencias de bits, las cuales se ingresan en el algoritmo de cifrado junto con los datos a cifrar.

Dos clases básicas de algoritmos de cifrado protegen las claves: simétrico y asimétrico. Ambos difieren en el uso que hacen de las claves. Los algoritmos de cifrado simétricos utilizan la misma clave, también llamada clave secreta, para cifrar y descifrar los datos. La clave debe ser pre-compartida. Una clave pre-compartida es bien conocida por ambos participantes antes de comenzar la comunicación cifrada. Dado que ambas partes deben custodiar la clave secreta, los algoritmos de cifrado aplicados pueden utilizar claves de menor longitud. Las claves más cortas dan como resultado tiempos de ejecución más rápidos. Los algoritmos simétricos son generalmente menos intensivos computacionalmente que los algoritmos asimétricos.

Los algoritmos de cifrado asimétricos utilizan diferentes claves para cifrar y descifrar los datos. Los mensajes seguros pueden ser intercambiados sin la necesidad de una clave pre-compartida. Debido a que ambas partes no poseen una clave pre-compartida, deben utilizarse claves muy largas para frustrar a los atacantes. Estos algoritmos utilizan muchos recursos y tienen una ejecución más lenta. En la práctica, los algoritmos asimétricos son cientos y hasta miles de veces más lentos que los algoritmos simétricos.

Para comprender mejor las diferencias entre ambos tipos de algoritmos, considere un ejemplo donde Alice y Bob viven en

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

diferentes localidades y desean intercambiar mensajes secretos entre sí a través del sistema de correo. En este ejemplo, Alice desea enviar un mensaje secreto a Bob.

Algoritmo simétrico

En el ejemplo del algoritmo simétrico, Alice y Bob poseen llaves idénticas para un mismo candado. Estas llaves fueron intercambiadas antes de enviar cualquier mensaje secreto. Alice escribe un mensaje secreto y lo guarda en una pequeña caja, la cual cierra utilizando el candado con su llave. Luego, envía la caja a Bob. El mensaje se encuentra seguro dentro de la caja a medida que ésta viaja a través del sistema de correo postal. Cuando Bob recibe la caja, utiliza su llave para abrir el candado y recuperar el mensaje. Bob puede utilizar la misma caja y candado para enviar un mensaje secreto a Alice.

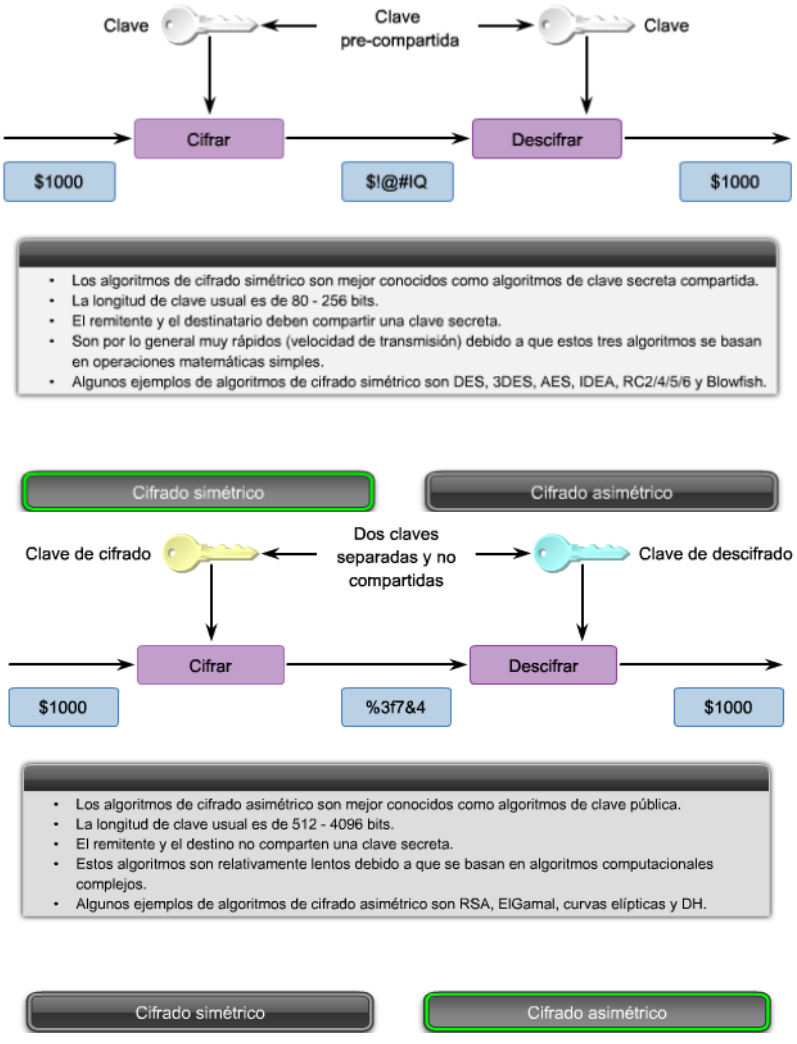
Algoritmo asimétrico

En el ejemplo del algoritmo asimétrico, Bob y Alice no intercambiaron llaves antes de enviar sus mensajes secretos. En su lugar, Bob y Alice poseen candados diferentes con sus llaves diferentes correspondientes. Cuando Alice decide enviar un mensaje secreto a Bob, primero debe contactarlo y pedirle que le envíe su candado abierto en la caja. Bob envía el candado, pero retiene su llave. Cuando Alice recibe el candado, escribe el mensaje secreto y lo guarda en la caja. También pone su candado abierto dentro de la caja, pero retiene su llave. Luego, cierra la caja con el candado de Bob. Una vez que Alice cierra la caja, ya no es capaz de acceder a su contenido porque no posee la llave para ese candado. Entonces, envía la caja a Bob. A medida que la caja recorre el sistema de correo, nadie puede abrirla. Cuando

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

Bob recibe la caja, puede utilizar su llave para abrir el candado y recuperar el mensaje de Alice. Para enviar una respuesta segura, Bob guarda su mensaje secreto en la caja junto con su candado abierto y cierra la caja con el candado de Alice. Luego, Bob envía la caja nuevamente a Alice.

Figura 11 Funcionalidad del algoritmo asimétrico



Fuente: Cisco

El cifrado simétrico es la forma más utilizada de criptografía, debido a que una menor longitud de clave aumenta la velocidad de ejecución. Además, los algoritmos de clave simétrica se basan

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

en operaciones matemáticas simples, que pueden ser fácilmente aceleradas por hardware. El cifrado simétrico es utilizado con frecuencia para cifrar datos a la velocidad de transmisión en las redes de datos y para proporcionar cifrado en bloques cuando se requiere privacidad de los datos, como por ejemplo en una VPN. Con el cifrado simétrico, la administración de claves puede ser un desafío. Las claves de cifrado y descifrado son las mismas. El origen y el destinatario del mensaje deben intercambiar la clave secreta simétrica (utilizando un canal seguro) antes de comenzar el cifrado. La seguridad de un algoritmo simétrico se basa en mantener en secreto de la clave simétrica. Obteniendo la clave, cualquiera puede cifrar y descifrar los mensajes.

DES, 3DES, AES, SEAL y las series RC (Rivest Ciphers), incluyendo RC2, RC4, RC5 y RC6, son algoritmos bien conocidos de cifrado con clave simétrica. Existen muchos otros algoritmos de cifrado, tales como Blowfish, Twofish, Threefish y Serpent. Sin embargo, estos protocolos no son soportados por plataformas Cisco o bien aún no han ganado una aceptación masiva.

Figura 12 Algoritmos simétricos

Algoritmo de cifrado simétrico	Longitud de la clave (en bits)	Descripción
DES	56	Diseñado por IBM durante la década del '70 y adoptado como estándar del NIST hasta 1997. Aunque ha sido considerado anticuado, DES sigue siendo muy utilizado. DES fue diseñado para ser implementado sólo por hardware y por lo tanto es extremadamente lento por software.
3DES	112 y 168	Basado en la utilización de DES tres veces consecutivas: los datos son cifrados tres veces. Por lo tanto, es considerado mucho más fuerte que DES. Sin embargo, es lento al compararlo con algunos nuevos cifrados por bloques, como AES.
AES	128, 192, y 256	AES es veloz tanto por software como por hardware, es relativamente fácil de implementar y requiere muy poca memoria. Como nuevo estándar de cifrado, está siendo implementado actualmente en gran escala.
Software Encryption Algorithm (SEAL)	160	SEAL es un algoritmo alternativo a DES, 3DES y AES. Utiliza una clave de cifrado de 160 bits y tiene un menor impacto sobre la CPU al compararlo con otros algoritmos basados en software.
Las series RC	RC2 (40 y 64) RC4 (1 a 256) RC5 (0 a 2040) RC6 (128, 192, y 256)	Los algoritmos RC son un conjunto de algoritmos de cifrado de clave simétrica inventado por Ron Rivest. RC1 nunca fue publicado y RC3 fue quebrado antes de poder ser utilizado. RC4 es el cifrado de flujo más utilizado a nivel mundial. RC6, un cifrado por bloques de 128 bits, está basado en gran parte en RC5 y fue un finalista de AES desarrollado en 1997.

Fuente: Cisco

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

Las técnicas más utilizadas de criptografía de cifrado simétrico son los cifrados de bloque y los cifrados de cadena. Cifrado por bloques. El cifrado por bloques (block cipher) transforma un bloque de texto plano de longitud fija en un bloque criptográfico común de 64 o 128 bits. El tamaño del bloque define qué cantidad de datos puede cifrarse por vez. Actualmente, el tamaño del bloque, también conocido como longitud fija, es en general de 64 o 128 bits. La longitud de la clave se refiere a la clave de cifrado utilizada. Este criptograma es descifrado aplicando la transformación inversa del bloque criptográfico, utilizando la misma clave secreta.

El cifrado por bloques en general resulta en una salida de datos más larga que los datos de entrada, debido a que el criptograma debe ser un múltiplo del tamaño de los bloques. Por ejemplo, DES cifra bloques en porciones de 64 bits, utilizando una clave de 56 bits. Para lograr esto, el algoritmo de bloques toma una porción de datos por vez, por ejemplo porciones de 8 bytes, hasta que se rellena el bloque completo. Si hay menos datos que los necesarios para completar un bloque, el algoritmo agrega datos artificiales (blancos) hasta que los 64 bits son utilizados.
El cifrado por bloques incluye DES con bloques de 64 bits, AES con bloques de 128 bits y RSA con bloques de tamaño variable.

Data Encription Standard (DES)

El Data Encryption Standard (DES) es un algoritmo de cifrado simétrico, utilizado normalmente en modo de cifrado por bloques. El algoritmo DES es en esencia una secuencia de permutaciones y sustituciones de bits de datos, combinadas con una clave de cifrado. Se utiliza el mismo algoritmo y la misma clave tanto para

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

el cifrado como el descifrado.

DES tiene una longitud de clave fija. La clave tiene una longitud de 64 bits, pero sólo se utilizan 56 bits para el cifrado. Los 8 bits restantes son utilizados para la paridad. El bit menos significativo de cada byte de la clave es utilizado para indicar la paridad impar. Una clave DES siempre tiene una longitud de 56 bits. Cuando se utiliza DES con una clave débil de 40 bits, la clave de cifrado contiene 40 bits secretos y 16 bits conocidos, lo cual conforma una clave de 56 bits. En este caso, la fortaleza de la clave DES es de 40 bits.

Figura 13 Características del algoritmo DES

Características de DES	
Descripción	Estándar de cifrado de datos
Línea de tiempo	Estandarizado en 1976
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	56 bits
Velocidad	Media
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	Días (6.4 días con la máquina COPACABANA, un dispositivo especializado en cracking)
Recursos consumidos	Medio

Fuente: Cisco

Aunque DES utiliza en general el método de cifrado por bloques, también puede utilizar el método de cifrado de flujo. Para cifrar o descifrar más de 64 bits de datos, DES utiliza dos métodos de cifrado por bloque estandarizados, Electronic Code Book (ECB) o Cipher Block Chaining (CBC).

Ambos métodos de cifrado utilizan la operación lógica XOR con la siguiente definición:
1 XOR 1 = 0

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

1 XOR 0 = 1

0 XOR 1 = 1

0 XOR 0 = 0

3DES

Con los avances en el poder de procesamiento de las computadoras, las claves DES originales de 56 bits se volvieron demasiado cortas para soportar ataques realizados con tecnología de mediano presupuesto. Una forma de aumentar la longitud efectiva de la clave DES, sin modificar el algoritmo bien analizado, consiste en utilizar repetidas veces el mismo algoritmo con diferentes claves.

La técnica de aplicar DES tres veces seguidas a un mismo bloque de texto plano es conocida como 3DES. En la actualidad, los ataques por fuerza bruta sobre 3DES son considerados impracticables debido a que los algoritmos básicos han sido bien analizados durante sus más de 35 años de utilización. Por lo tanto, es considerado muy confiable. La implementación IPsec de Cisco utiliza DES y 3DES en el modo CBC.

Figura 14 Características de 3DES

Características de 3DES	
Descripción	Estándar de cifrado de datos triple
Línea de tiempo	Estandarizado en 1977
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	112 y 168 bits
Velocidad	Lenta
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	4.6 miles de millones de años, con tecnología actual
Recursos consumidos	Medio

Fuente: Cisco

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

3DES utiliza un método llamado 3DES-Encrypt-Decrypt-Encrypt (3DES-EDE) para cifrar texto plano. Primero, el mensaje es cifrado utilizando la primera clave de 56 bits, llamada K1. Luego, los datos se descifran utilizando la segunda clave de 56 bits, llamada K2. Finalmente, los datos son nuevamente cifrados con la tercera clave de 56 bits, llamada K3.

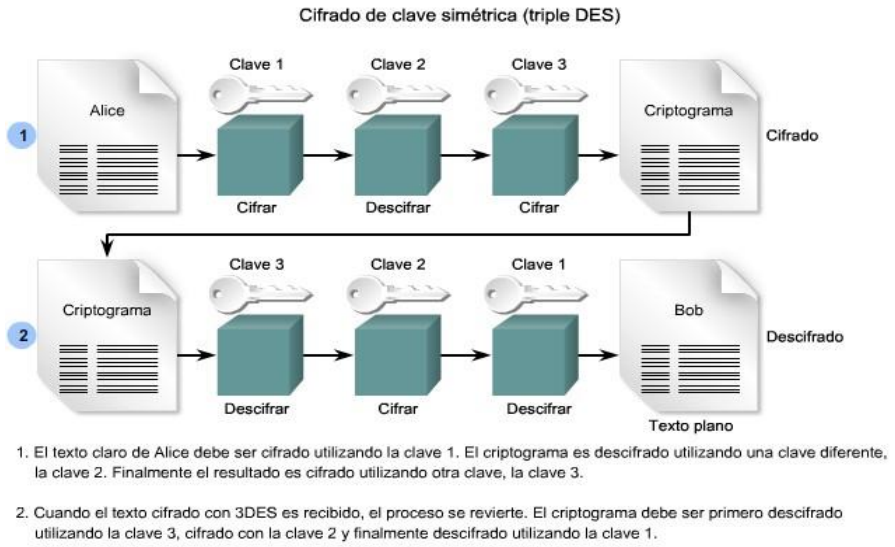
El procedimiento 3DES-EDE es mucho más efectivo en el aumento de la seguridad que el simple cifrado de los datos tres veces con tres claves diferentes. Cifrando datos tres veces consecutivas utilizando claves diferentes de 56 bits equivale a una fortaleza de clave de 58 bits. El procedimiento 3DES-EDE, por otro lado, provee un cifrado con una longitud efectiva de clave de 168 bits. Si las claves K1 y K3 son iguales, como sucede en algunas implementaciones, se obtiene un cifrado menos seguro de 112 bits.

Para descifrar el mensaje, debe utilizarse el proceso inverso a 3DES-EDE. Primero, el criptograma se descifra utilizando la clave K3. Luego, los datos son cifrados utilizando la clave K2. Finalmente, los datos vuelven a descifrarse utilizando la clave K1.

Aunque 3DES es muy seguro, también consume recursos en forma intensiva. Por este motivo, se desarrolló el algoritmo de cifrado AES, el cual ha sido probado tan seguro como 3DES, pero con resultados mucho más veloces.

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

Figura 15 Cifrado de clave simétrica (triple DES)



Fuente: Cisco

Advanced Encryption Standard (AES)

Durante algunos años, se había pensado que DES llegaría eventualmente al final de su utilidad. En 1997 fue anunciada la iniciativa AES y se invitó al público a proponer esquemas de cifrado para reemplazar a DES. Luego de un proceso de estandarización de 5 años, durante los cuales se presentaron y evaluaron 15 diseños diferentes, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) seleccionó el cifrado por bloques de Rijndael para el algoritmo AES.

El cifrado Rijndael, desarrollado por Joan Daemen y Vincent Rijmen, posee una longitud de bloque y longitud de clave variables. Rijndael es un cifrado por bloques iterativo, lo que significa que el bloque de entrada inicial y la clave de cifrado atraviesan múltiples ciclos de transformación antes de generar los datos de salida. El algoritmo puede operar sobre bloques de

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

tamaños variables, utilizando claves de diferente longitud. Pueden utilizarse claves de 128 bits, 192 bits o 256 bits, para cifrar bloques de datos de 128, 192 o 256 bits de longitud y es posible utilizar cualquiera de las nueve combinaciones de bloques y claves.
La implementación Rijndael aceptada para AES contiene sólo algunas capacidades del algoritmo Rijndael. El algoritmo fue escrito de forma tal que la longitud de los bloques o de la clave puedan ser fácilmente extendidos en múltiplos de 32 bits y el sistema está diseñado específicamente para su implementación por hardware o por software en un amplio rango de procesadores.

El algoritmo AES ha sido analizado extensivamente y ahora es utilizado en todo el mundo. Aunque no ha sido probado con el uso cotidiano en igual grado que 3DES, AES con cifrado Rijndael es el algoritmo más eficiente. Puede ser utilizado en ambientes de baja latencia y gran volumen de transferencia, especialmente cuando 3DES no puede procesar los requisitos de latencia o transferencia. Se espera que aumente la confianza en AES con el transcurso del tiempo, a medida que se intenten más ataques en su contra.

Figura 16 Características de AES

Características de AES	
Descripción	Estándar de cifrado avanzado
Línea de tiempo	Estándar oficial desde 2001
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	128, 192, y 256
Velocidad	Alta
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	149 trillones de años
Recursos consumidos	Bajos

Más información

Para obtener más información sobre AES, visite http://www.nist.gov/aes. En 2008, el NIST llevó adelante una competencia, similar a la de la iniciativa AES, para desarrollar una nueva versión de SHA. Para obtener más información, visite http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

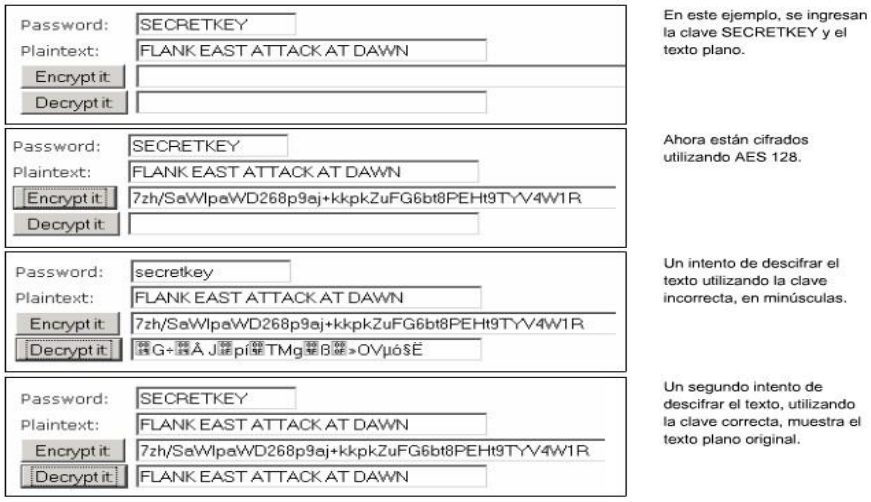
Fuente: Cisco

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

AES fue seleccionado para reemplazar a DES por diferentes razones. La longitud de clave de AES la vuelve mucho más segura que DES. AES se ejecuta con mayor velocidad que 3DES sobre hardware de similares características. AES es más eficiente que DES y 3DES, usualmente por un factor de cinco cuando es comparado con DES. AES es más adecuado en ambientes de baja latencia y alta transferencia, especialmente si se utiliza sólo cifrado por software.

A pesar de estas ventajas, AES es un algoritmo relativamente joven.

Figura 17 Cifrado y descifrado del algoritmo AES



Fuente: Cisco

Algoritmos de Cifrado Alternativos

SEAL (Software-optimized Encryption Algorithm) es un algoritmo alternativo a los algoritmos DES, 3DES y AES, basados en software. Phillip Rogaway y Don Coppersmith diseñaron SEAL en 1993. Es un cifrado de flujo que utiliza una clave de cifrado de 160 bits. Al ser un cifrado de flujo, los datos deben ser cifrados de forma continua, por lo que es más veloz que el cifrado por bloques. Sin embargo, posee una fase de inicialización más

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

extensa, durante la cual se crea un conjunto grande de tablas utilizando SHA.

Figura 18 Características de SEAL

Características de SEAL	
Descripción	Algoritmo de cifrado optimizado por software
Línea de tiempo	Publicado por primera vez en 1994. La versión actual es la 3.0 (1997)
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	160
Velocidad	Alta
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	Desconocido, pero considerado muy seguro
Recursos consumidos	Bajos

Fuente: Cisco

Los algoritmos RC fueron diseñados en parte o completamente por Ronald Rivest, quien también inventó MD5. Los algoritmos RC están ampliamente distribuidos en muchas aplicaciones de red debido a su velocidad favorable y su capacidad de utilizar claves de longitud variable.

Existe una cantidad de algoritmos RC ampliamente utilizados:
RC2 - Cifrado por bloques con clave de longitud variable, diseñado como un reemplazo para DES.
RC4 - Cifrado de flujo más utilizado a nivel mundial. Este algoritmo consiste en un cifrado de flujo Vernam con clave de longitud variable, utilizado con frecuencia en productos de cifrado de archivos y para comunicaciones seguras, tales como dentro de SSL. El cifrado por software se ejecuta rápidamente y es considerado seguro, aunque puede implementarse en forma insegura, como en el caso de WEP (Wired Equivalent Privacy).
RC5 - Cifrado por bloques rápido, con longitudes variables de bloque y de clave. RC5 puede ser utilizado como reemplazo para DES, si el tamaño de los bloques se configura en 64 bits.

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

RC6 - Desarrollado en 1997, RC6 fue un finalista de AES (Rijndael ganó). Rivest, Sidney y Yin diseñaron un cifrado por bloques de 128 a 256 bits basado en RC5. Su objetivo principal de diseño era cumplir con los requisitos de AES.

Figura 19 Código Ron o códigos Rivest

Código de Ron o códigos Rivest				
Descripción	RC2	RC4	RC5	RC6
Línea de tiempo	1987	1987	1994	1998
Tipo de algoritmo	Cifrado por bloques	Cifrado de flujo	Cifrado por bloques	Cifrado por bloques
Tamaño de clave (en bits)	40 y 64	1 - 256	0 a 2040 bits (se sugiere 128)	128, 192, o 256

Fuente: Cisco

Intercambio de claves Diffie-Hellman

Whitfield Diffie y Martin Hellman inventaron el algoritmo Diffie-Hellman (DH) en 1976. El algoritmo DH es la base de la mayoría de los métodos automáticos de intercambio de claves actuales y es uno de los protocolos de red más comunes hoy día. Diffie-Hellman no es un mecanismo de cifrado y no es utilizado para cifrar datos sino que es un método para intercambiar de forma segura las claves para cifrar datos.

En un sistema de claves simétricas, ambos extremos de la comunicación deben tener claves idénticas. El intercambio seguro de dichas claves siempre se ha presentado como un desafío. Los sistemas de claves asimétricas resuelven este desafío porque utilizan dos claves. Una clave es llamada clave privada, mientras que la otra se llama clave pública. La clave privada es secreta y sólo conocida por el usuario. La clave pública se comparte en forma abierta y se distribuye con facilidad.

DH es un algoritmo matemático que permite a dos computadoras generar una clave secreta idéntica en ambos sistemas, sin

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

haberse comunicado con anterioridad. La nueva clave compartida nunca es realmente intercambiada entre los participantes. Pero debido a que ambas partes la conocen, puede ser utilizada para cifrar el tráfico entre los dos sistemas. Su seguridad se basa en la dificultad de calcular los logaritmos discretos de números muy grandes.

DH es usado en general para el intercambio de datos utilizando una VPN IPsec, datos cifrados en Internet utilizando SSL o TSL o cuando se intercambian datos con SSH.
Aunque DH es utilizado con algoritmos simétricos para crear claves compartidas, es importante recordar que en realidad se trata de un algoritmo asimétrico.

Criptografía de clave publica

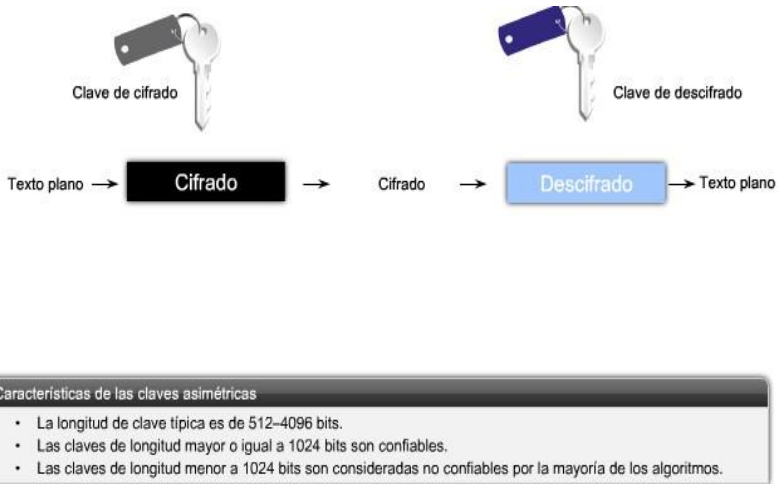
Los algoritmos asimétricos, también conocidos como algoritmos de clave pública, están diseñados de forma tal que la clave utilizada para cifrar los datos sea diferente a la utilizada para descifrarlos. La clave de descifrado no puede ser calculada en un tiempo razonable a partir de la clave de cifrado y viceversa.
Existen cuatro protocolos que utilizan algoritmos de clave asimétrica: Internet Key Exchange (IKE), un componente fundamental de las VPNs IPsec Secure Socket Layer (SSL), ahora implementado como el estándar IETF TLS SSH Pretty Good Privacy (PGP), un programa de computadora que provee privacidad y autenticación criptográficas y se utiliza con frecuencia para incrementar la seguridad de las comunicaciones de correo electrónico.

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

Los algoritmos asimétricos utilizan dos claves: una clave pública y una clave privada. Ambas pueden utilizarse en el proceso de cifrado, pero se requiere la clave complementaria correspondiente para su descifrado. Por ejemplo, si se utiliza una clave pública para cifrar los datos, la clave privada correspondiente los descifra. La operación inversa también es válida: si se cifran los datos con la clave privada, debe utilizarse la clave pública correspondiente para descifrarlos.

Este proceso permite que los algoritmos asimétricos proporcionen autenticación, integridad y confidencialidad.

Figura 20 Características de las claves asimétricas

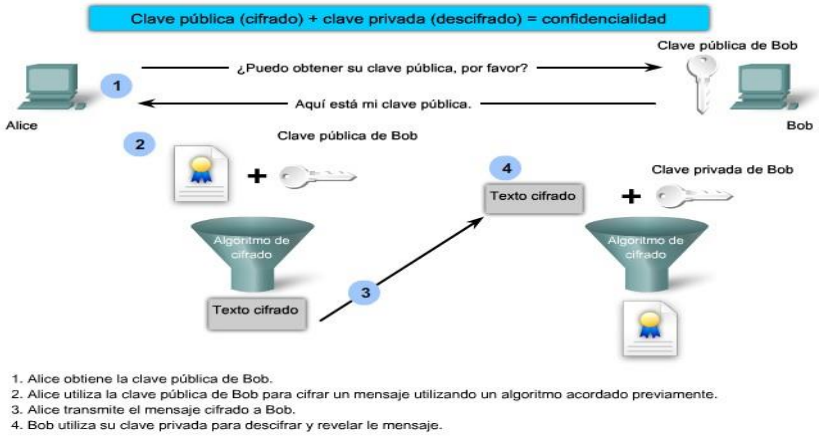


Fuente: Cisco

El objetivo de confidencialidad de los algoritmos asimétricos se logra cuando el proceso de cifrado comienza con la clave pública. Cuando la clave pública es utilizada para cifrar los datos, la clave privada debe ser utilizada para descifrar los datos. Sólo uno de los hosts posee la clave privada, por lo tanto, se logra la confidencialidad.

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

Figura 21 Confidencialidad de algoritmos asimétricos

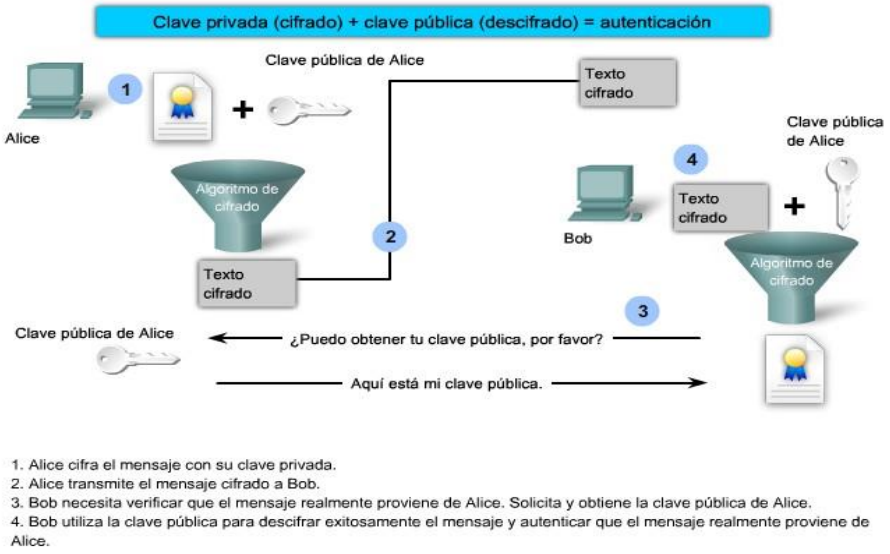


Fuente: Cisco

El objetivo de autenticación de los algoritmos asimétricos se logra cuando el proceso de cifrado comienza con la clave privada.

Cuando la clave privada es utilizada para cifrar los datos, la clave pública correspondiente debe ser utilizada para descifrar los datos. Debido a que sólo un host posee la clave privada, sólo dicho host puede haber cifrado el mensaje, probando así la autenticidad del remitente.

Figura 22 Autenticidad de algoritmos asimétricos



Fuente: Cisco

Para enviar un mensaje que asegure su confidencialidad, autenticación e integridad, es necesaria la combinación de dos fases de cifrado.

Fase 1 - Confidencialidad

Alice desea enviar un mensaje a Bob, asegurando la confidencialidad del mensaje (sólo Bob puede leer el documento en texto plano). Alice utiliza la clave pública de Bob para cifrar el mensaje. Sólo Bob puede descifrarlo, utilizando su clave privada.

Fase 2 - Autenticación e Integridad

Además, Alice desea asegurar la autenticación e integridad del mensaje (Bob está seguro de que el documento no ha sido modificado y que fue enviado por Alice). Alice utiliza su clave privada para cifrar un hash del mensaje. De esta forma, Bob puede utilizar la clave pública de Alice para verificar que el mensaje no ha sido modificado (el hash recibido es igual al calculado localmente, en base a la clave pública de Alice). Además, esto verifica que Alice es realmente quien envió el mensaje, porque nadie más posee su clave privada.

Al enviar un mensaje cifrado con la clave pública de Bob y un hash cifrado con la clave privada de Alice, se aseguran la confidencialidad, la autenticidad y la integridad.

Existe una variedad de algoritmos de clave asimétrica bien conocidos:

Diffie-Hellman

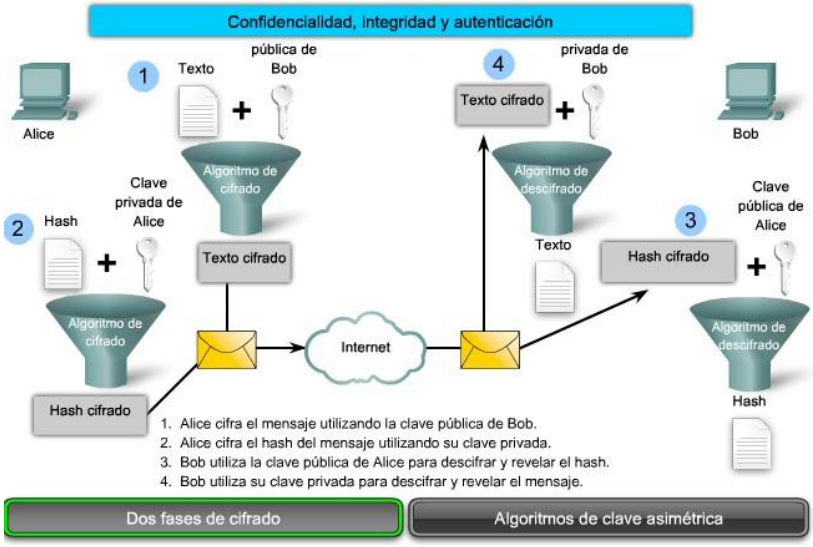
Digital Signature Standard (DSS), el cual incorpora el Algoritmo de Firma Digital (DSA - Digital Signature Algorithm) Algoritmos de cifrado RSA

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

ElGamal

Técnicas de curva elíptica

Figura 23 Fases de cifrado asimétrico



Fuente: Cisco

Firmas Digitales

Las firmas manuscritas han sido utilizadas por mucho tiempo como prueba de autoría de los contenidos de un documento. Las firmas digitales pueden proporcionar las mismas funciones que las firmas manuscritas y mucho más.

Las firmas digitales son utilizadas en las siguientes situaciones:

Para proveer una prueba única del origen de los datos, los cuales sólo pueden ser generados por un único participante, tales como firmas de contratos en ambientes de comercio electrónico.

Para autenticar a un usuario, utilizando la clave privada de dicho usuario y la firma que genera.

Para probar la autenticidad e integridad de certificados PKI.

Para proveer una marca de tiempo segura utilizando una fuente de tiempo confiable.

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

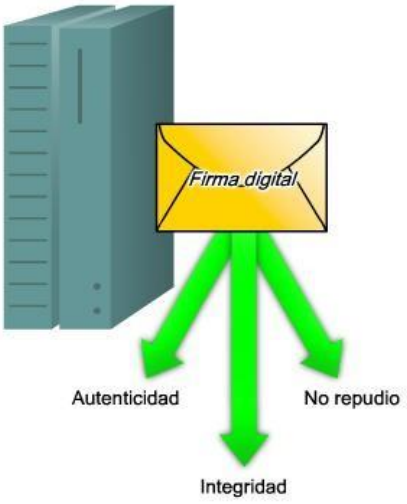
Específicamente, las firmas digitales proveen tres servicios básicos de seguridad:

Autenticidad de los datos firmados digitalmente - Las firmas digitales autentican un origen, probando que un cierto participante ha visto y firmado los datos en cuestión.

Integridad de los datos firmados digitalmente - Las firmas digitales garantizan que los datos no han sido modificados desde el momento en que fueron firmados.

No repudio de la transacción - El destinatario puede enviar los datos de un tercero, quien acepta la firma digital como prueba de que este intercambio de datos tuvo lugar. Quien firma los datos no puede repudiar haber firmado los datos.

Figura 24 Firma digital



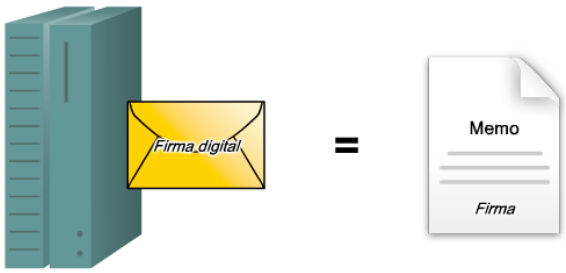
Fuente: Cisco

Las firmas digitales poseen propiedades específicas que permiten probar la autenticación de entidades y la integridad de los datos:

La firma es auténtica y no puede ser falseada. Es una prueba de que el firmante, nadie más, ha firmado el documento.La firma no es reutilizable. La firma es parte del documento y no puede ser movida a un documento diferente. La firma es inalterable. Una vez firmado un documento, éste no puede ser alterado. La firma no puede ser repudiada. Por motivos legales, la firma y el documento son considerados objetos físicos. Los firmantes no pueden alegar luego que no fueron ellos quienes realizaron la firma.

Los procedimientos actuales de firma digital no son simplemente implementados durante operaciones públicas. De hecho, una firma digital moderna se basa en una función de hash y un algoritmo de clave pública.

Figura 25 Firma digital dato



Fuente: Cisco

El proceso de firma digital consta de seis pasos:

El dispositivo de origen (firmador) calcula un hash a partir del documento.
El dispositivo de origen cifra el hash con la clave privada del firmador.
El hash cifrado, conocido como firma, es incorporado al documento.
El dispositivo de destino (verificador) acepta el documento con la

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

firma digital y obtiene la clave pública del dispositivo de origen.
El dispositivo de destino descifra la firma utilizando la clave pública del dispositivo de origen. Este paso revela el valor de hash calculado por el dispositivo de origen.
El dispositivo de destino calcula un hash a partir del documento, sin incluir su firma y compara este hash con el hash descifrado a partir de la firma. Si ambos valores de hash coinciden, el documento es auténtico. Fue firmado por quien se supone como firmador y no ha sido modificado desde que se generó la firma.
Se requieren tanto el cifrado como las firmas digitales para asegurar que el mensaje es privado y no ha sido modificado.

Los algoritmos asimétricos bien conocidos, tales como RSA o DSA (Digital Signature Algorithm), son utilizados en general para realizar las firmas digitales.

DSA

En 1994, el instituto NIST de los Estados Unidos seleccionó a DSA como el Estándar de Firma Digital (DSS - Digital Signature Standard). DSA está basado en el problema del logaritmo discreto y sólo puede proveer firmas digitales.

La verificación de firmas es demasiado lenta y el proceso mediante el cual el NIST seleccionó a DSA fue demasiado secreto y arbitrario. DSS ahora incorpora dos posibles algoritmos adicionales: Criptografía de Clave Pública Reversible Utilizando Firma Digital (la cual utiliza RSA) y el Algoritmo de Firma Digital de Curva Elíptica (ECDSA - Elliptic Curve Digital Signature Algorithm).

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

El administrador de red debe decidir si RSA o DSA resulta más adecuado para una situación determinada. La generación de firmas DSA es más veloz que la verificación de firmas DSA. Por otro lado, la verificación de firmas en RSA es más veloz que la generación de firmas.

Rivest, Shamir y Alderman

RSA es uno de los algoritmos asimétricos más comunes. Ron Rivest, Adi Shamir y Len Adleman inventaron el algoritmo RSA en 1977. Se trata de un algoritmo patentado de clave pública. Su patente expiró en septiembre del año 2000 y el algoritmo es ahora del dominio público.

El algoritmo RSA es muy flexible porque posee una clave de longitud variable, por lo que la clave puede ser acortada para acelerar el procesamiento. A cambio, mientras más corta es la clave, menos seguro es el algoritmo.

Las claves RSA tienen por lo general entre 512 y 2048 bits de longitud. RSA ha soportado años de criptoanálisis intensivo. Aunque la seguridad de RSA nunca ha sido probada o refutada, esto sugiere cierto nivel de confianza en el algoritmo. La seguridad de RSA se basa en la dificultad de factorizar números muy grandes. En caso de descubrirse un método sencillo para factorizar estos números grandes, la efectividad de RSA se vería destruida.

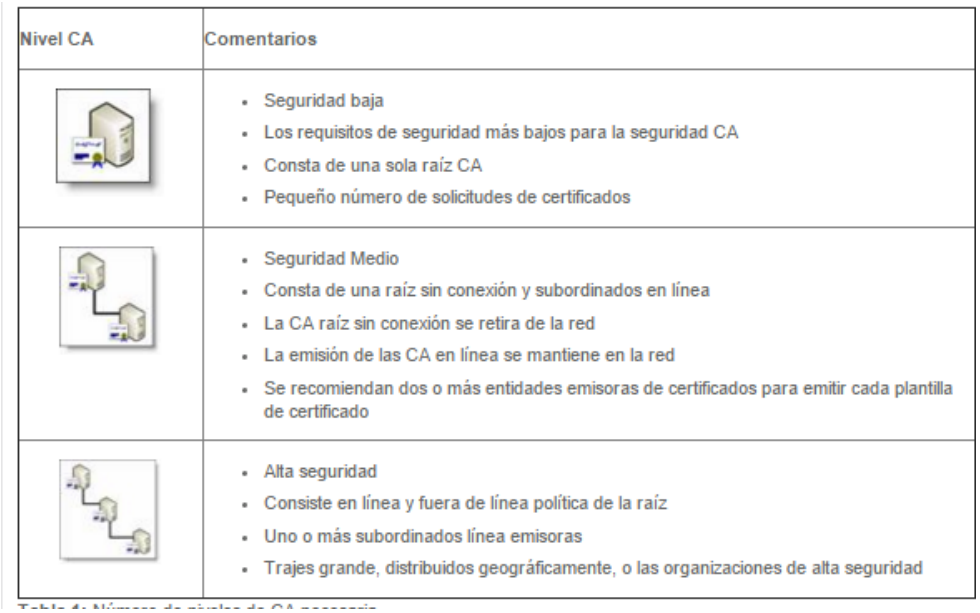
El algoritmo RSA se basa en una clave pública y en una clave privada. La clave pública puede ser distribuida, pero la clave privada debe ser mantenida en secreto. No es posible determinar la clave privada a partir de la clave pública, utilizando ningún algoritmo computable y viceversa.

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

Las claves RSA son de largo plazo y en general son cambiadas o renovadas luego de algunos meses o incluso años. RSA es utilizado principalmente para asegurar la confidencialidad de los datos mediante el cifrado y para la autenticación o no repudio de los datos, o ambos, mediante la generación de firmas digitales.

Diseño de una Infraestructura de PKI

Figura 26 PKI



Nivel CA	Comentarios
	• Seguridad baja • Los requisitos de seguridad más bajos para la seguridad CA • Consta de una sola raíz CA • Pequeño número de solicitudes de certificados
	• Seguridad Medio • Consta de una raíz sin conexión y subordinados en línea • La CA raíz sin conexión se retira de la red • La emisión de las CA en línea se mantiene en la red • Se recomiendan dos o más entidades emisoras de certificados para emitir cada plantilla de certificado
	• Alta seguridad • Consiste en línea y fuera de línea política de la raíz • Uno o más subordinados línea emisoras • Trajes grande, distribuidos geográficamente, o las organizaciones de alta seguridad

Fuente: Technet

Los números y los niveles de CA deben implementar básicamente dependiendo de los requisitos de seguridad y disponibilidad. Se debe tratar de organizar la jerarquía de acuerdo a las necesidades.

Existen políticas de certificado en el que se describe cómo y quién va a emitir y distribuir los certificados a un sujeto (por ejemplo, los sujetos de ser usuarios, equipos, dispositivos, etc.). Si alguna vez es posible que se necesite más de una política de certificados, debido a la legal, geográfica, organizativa o el uso de certificados en base, entonces definitivamente se va a necesitar una jerarquía

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

PKI de 3 niveles, ya que este requisito requerirá 2 o más políticas CA a nivel 2 (también conocida como la política de las CA).

Al implementar una PKI, siempre tendrá que comenzar con una CA raíz, no importa si nos ocupamos de un 1 nivel, 2-nivel o jerarquía PKI de 3 niveles. Desde la raíz CA será siempre la raíz de confianza, y más a menudo implementado mediante el uso de un certificado auto-emitida, es esencial que usted protege la clave privada de la entidad emisora raíz lo mejor que pueda. Esto siempre debe ser el caso, no importa cuántos niveles de la jerarquía PKI consiste. Si su jerarquía PKI consta de 2 niveles o más, entonces su raíz CA requiere una cantidad mínima de acceso, ya que sólo serán las entidades emisoras de certificados subordinadas que requieren acceso a la CA raíz Sin embargo, como la distancia desde la raíz CA aumenta (es decir, se añaden más niveles), los requisitos de seguridad disminuyen y los de acceso aumenta con respecto a la CA subordinadas. Este será un factor importante cuando tenemos que empezar a instalar las CA.

Figura 27 Tamaño recomendado de clave

Papel CA	Tamaño de la clave
Root CA	4096
Política de CA	4096
CA emisora	2048

Fuente: Technet

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

Figura 28 Pros y contras de clave privada

Método de protección	Pros (+)	Contras (-)
Certificado tienda local	• Fácil de implementar (por defecto) • Bajo costo	• Seguridad baja • Construido en CSP sólo es FIPS 140-1 compatible
Autenticación basada en chip (Smart Card o Token USB)	• Bastante fácil de implementar • Bajo costo • FIPS 140-2 compatibles	• Seguridad física baja, debido a la tarjeta inteligente o token pueden ser fácilmente perdidos o robados • Requiere presencia física cuando se inicia Servicios de certificados • Requiere CSP especial que sea compatible con FIPS 140-2 y soporta Microsoft Certificate Services
Las máquinas virtuales cifradas	• Fácil de implementar • Bajo costo • No depende del hardware • FIPS 140-2 compatibles	• Seguridad Medio • Vulnerable a los ataques analógicas, ya que el disco duro o DVD que contiene la máquina virtual puede ser fácilmente perdidos o robados
Módulo de seguridad de hardware (HSM)	• Muy alta seguridad • FIPS 140-2 Nivel 2 y 3 compatible • Puede ser PCI o LAN basada • A menudo puede ser utilizado como aceleradores SSL, así	• Alto costo (dependiendo de la configuración) • Requiere una planificación cuidadosa y por defecto

Fuente: Technet

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

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 que 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.

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

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.

b) Se asignan los Ip's.

FASE III:

a) Se hace el diseño físico de la red

b) Configuración de los servidores.

c) Modelo de red: Basado en servidor.

d) Configuración de los clientes de la red.

FASE IV:

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

b) Análisis de tráfico de la red

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

2.4. Definición de términos básicos

Transport Layer Security (TLS; en español «seguridad de la capa de transporte») y su antecesor Secure Sockets Layer (SSL; en español «capa de conexión segura») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

X.509 es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 específica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. Su sintaxis, se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One), y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail).

La criptografía asimétrica (en inglés asymmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves1 (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves. Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario

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

podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador.
La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo documentos electrónicos o software, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido.

Algoritmo (del griego y latín, dixit algorithmus y este a su vez del matemático persa Al-Juarismi) es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

Criptografía (del griego κρύπτος '(criptos), «oculto», y γραφη (grafé), «escritura», literalmente «escritura oculta»). Tradicionalmente se ha definido como el ámbito de la criptología el que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el Arte como en la Ciencia. Por tanto,

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

el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos.

OpenSSL es un proyecto de software libre basado en SSLeay, desarrollado por Eric Young y Tim Hudson. Consiste en un robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS). Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad, como el Transport Layer Security (TLS). OpenSSL también permite crear certificados digitales que pueden aplicarse a un servidor, por ejemplo Apache.

Llave pública y llave privada son un par de "llaves" digitales asociadas a una persona o entidad y generadas mediante métodos criptográficos. La llave pública es usada para cifrar la información, haciendo una analogía, es como la llave utilizada para cerrar una puerta y mantener fuera a cualquier persona mientras que la llave privada se usa para descifrar, es decir, la llave que abre la puerta y sólo la posee la persona autorizada, por lo tanto ésta debe mantenerse en secreto.

Una Autoridad Certificadora (AC, en inglés CA) es una entidad confiable que se encarga de garantizar que el poseedor de un certificado digital sea quien dice ser, bridando confianza a ambas partes de una comunicación segura SSL/TLS.

FTP: File Transfer Protocol protocolo de transferencia de archivos

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

en modo seguro; se utiliza en entornos TCP/IP.

HTML: HyperText Markup Language, lenguaje para la publicación de datos mediante la realización de presentaciones en modo grafico a través de un navegador de internet.

HTTP: HyperText Transfer Protocol, protocolo de transferencia de archivos que permiten manejar todo tipo de información.

HTTPS: HTTP Secure, es la versión HTTP que utiliza SSL para el cifrado de datos en los intercambios entre un cliente y un servidor web.

ICMP: Es una extensión del protocolo de internet (IP), y permite generar mensajes de error paquetes de prueba y mensajes informativos relacionados con IP. Básicamente, se usa para comprobar la existencia de la maquina consultada.

IEEE: Institute of Electrical and Electronics Engineers, es el organismo de normalización que se encarga de las normas importante para redes, relativas a las capas bajas.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

ISO: Especializada en el desarrollo y la normalización de estándares técnicos, ISO es una organización no gubernamental internacional. Agrupa a más de 150 países y su sede está en Ginebra.

LAN: Local Area Network, Red de área local, rede de computadoras ubicadas en el mismo ambiente, piso o edificio.

MAC: Médium Access Control, capa inferior del nivel de conexión del modelo OSI introducida por el IEEE. Administra el acceso al soporte físico integrando así el método de acceso al soporte y el direccionamiento físico.

NetBIOS: Network Basic Input/Output System, es una interfaz de

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

programación para aplicaciones de red, disponible para aplicaciones cliente/servidor en cualquier protocolo de capas medias.

OSI: OPEN SYSTEMS INTERCONNECTION (interconexión de sistemas abiertos) conjunto de protocolos diseñados por comités ISO con el objetivo de convertirlos en estándares internacionales de arquitectura de redes de computadoras.

PC: acrónimo de personal computer (computadora personal)

TCP/IP: Conjunto de protocolos que definen a la internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

Protocolo: Conjunto de reglas que definen la forma en que las computadoras se comunican entre sí.

Proxy: Es un ordenador que pertenece a una red y que hace de intermediario entre los diferentes puestos de la red y la conexión a internet para estos puestos. Esto facilita que todos los ordenadores de esta red tengan que pasar por el proxy para poder entrar en internet, de forma que podamos aumentar la seguridad, administrar el número de conexiones y realizar función de cache de páginas vistas en la web de internet.

RPV: Red Privada Virtual, ver VPN.

SET: Está orientado a la realización de pagos con tarjeta de crédito y débito en internet. Además de cubrir los aspectos generales de la seguridad informática como la integridad o confidencialidad, cubre ámbitos relacionados con la propia venta como el registro del comprador y del vendedor o la gestión de pagos.

SSL: Esta constituida de mecanismos de seguridad necesarios como el cifrado de datos, la autenticación de clientes y servidores o la integridad de los mensajes.

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

TLS: Transport Layer Security, es el sucesor de SSL para la protección del nivel aplicativo.

UDP: User Datagram Protocol, protocolo del nivel de transporte del grupo TCP/IP que proporciona un modo no fiable.

URL: Uniform Resource Locator, ruta de red que permite identificar un recurso TCP/IP de manera única.

UTP: Unshielded Twisted Pair, par trenzado no blindado.

VPN: Es una red privada de datos que utiliza infraestructuras de comunicaciones públicas, pero conservando la privacidad, es decir, en vez de cifrar cada una de las comunicaciones, cifra el canal y con ello se obtiene la misma funcionalidad que una red privada, pero a un coste menor y con mayor seguridad. Tecnológicamente esta red es superior a los otros protocolos, aunque requiere un intercambio de claves seguro entre los extremos y una infraestructura más compleja.

WAN: Wide Área Network, expresión que designa una red muy amplia en términos geográficos.

WINS: Windows Internet Naming Service, es un servicio dinamico que permite convertir entre redes los nombres NetBIOS en dirección IP.

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

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo y Diseño de Investigación

Tipo: Investigación cuantitativa

Diseño: Cuasi Experimental

Figura 29 Diseño Investigación

Donde:
X = Protocolo de cifrado TLS
O_1 = Diagnostico del estado actual de la seguridad de las comunicaciones en la capa de transporte
O_2 = Evaluación de los algoritmos de cifrado
O_3 = Diseño de un modelo de protocolo de cifrado
O_4 = Implementación del algoritmo de cifrado

Fuente: Propia

3.2. Población y Muestra

Población: Páginas Web

Muestra: Páginas Web con cifrado (HTTPS)

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

3.3. Hipótesis

Si implementamos protocolo de cifrado de TLS entonces mejoraremos la seguridad de las comunicaciones en la capa de transporte.

3.4. Variables

Variable Independiente: Protocolo de cifrado TLS

Alteración de las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Variable Dependiente: Seguridad de las comunicaciones en la capa de transporte

Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

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

3.5. Operacionalización

Variable Dependiente	Dimensiones	Indicadores	Técnicas e instrumentos de recolección de datos
Seguridad de las comunicaciones en la capa de transporte	Medidas de rendimiento	Negociación entre cliente y servidor (HANDSHAKE)	Sniffer, observación, ficha técnica
		Tiempo de procesamiento	Sniffer, observación, ficha técnica
		Compatibilidad de navegadores web con algoritmos de cifrado	Sniffer, Ficha técnica
		Costo computacional	Sniffer, observación, ficha técnica
	Datos transmitidos	Datos sin Cifrado	Sniffer, observación, ficha técnica
		Datos con cifrado	Sniffer, observación, ficha técnica
		Proporción de tamaño entre datos con cifrado y datos sin cifrado	$\frac{dcc}{dsc}$ $\frac{(dcc-dsc)}{dsc} \times 100\%$

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

3.6. Métodos, técnicas e instrumentos de recolección de datos

Observación

Se observaran todos los eventos a lo largo de la investigación.

Técnicas: Registro de observaciones

Se usan para recopilar los datos de las pruebas.

Instrumento: Ficha de registro de eventos

Se utiliza para el registro de eventos de las pruebas de aplicación de las técnicas.

Pruebas

Se realizaran pruebas para analizar los resultados obtenidos

Sniffer

Software de captura de paquetes.

3.7. Procedimiento para la recolección de datos

El desarrollo de la siguiente investigación se ha basado en la utilización de técnicas de cifrado de datos:

Recopilación de datos.

Pre-procesamiento de datos.

Sniffeo.

Simulación.

Resultados.

Se realizara mediante la puesta en ejecución de las técnicas usadas y evaluar el desempeño de cada una de ellas de acuerdo con los indicadores que se han establecido.

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

3.8. Análisis Estadístico e Interpretación de los datos

Tabulación de datos

Uso de tablas estadísticas.

Uso de gráficos estadísticos como producto del procesamiento de los datos obtenidos de las pruebas realizadas y procesadas.

Análisis de datos

Interpretación de indicadores de acuerdo con las pruebas que se realizaran.

3.9. Principios éticos

Objetividad: El análisis de la situación encontrada se basara en criterios técnicos imparciales.

Confidencialidad: Se asegurara que los registros usados para la prueba que son de un ámbito privado no se hagan públicos.

Veracidad: La información mostrada será verdadera.

Integridad: La información utilizada no sufrirá modificaciones a lo largo de la investigación.

3.10. Criterios de rigor científico

Validación: Se validaran los instrumentos de recolección de datos.

Contrastación: Se contrastará la hipótesis a través de métodos estadísticos debido al diseño cuasi experimental.

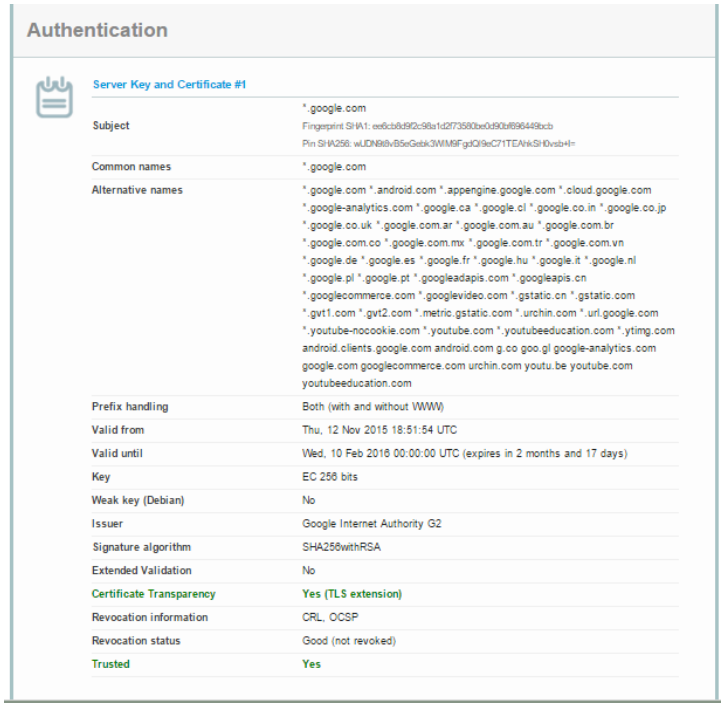
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Resultados en tablas y gráficos.

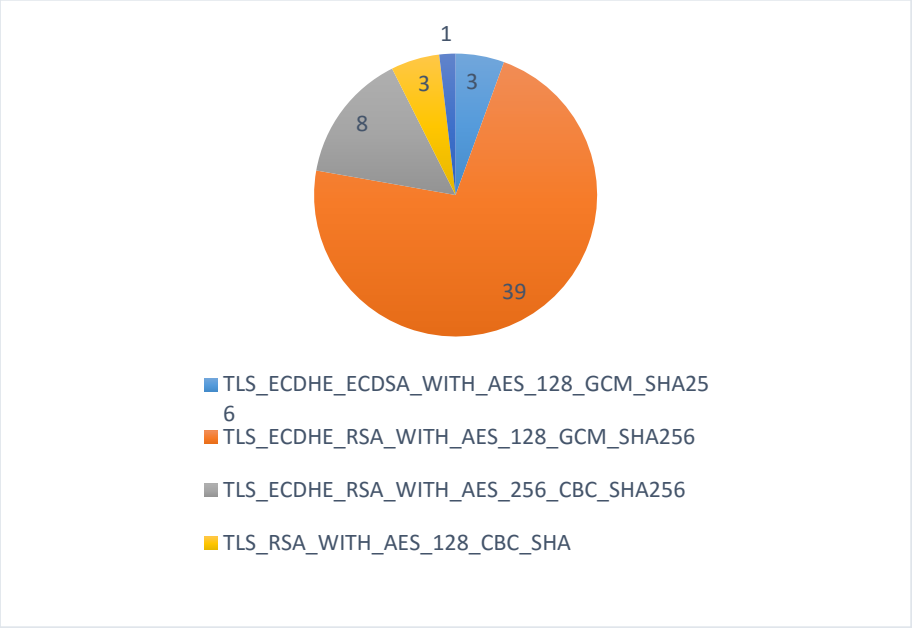
4.1.1 Combinación de algoritmos de cifrado más usados por las páginas web más visitadas

Figura 30 Análisis de páginas web



Fuente: propia

Figura 31 Páginas más visitadas



Fuente: Propia

Según el análisis realizado (Company, 2015) de las 100 páginas más visitadas, se analizó 53 con seguridad y 1 sin seguridad, de las cuales se evaluó las combinaciones de algoritmos de cifrado. Mediante la figura N° 31 podemos apreciar que la combinación más utilizada de algoritmos de cifrado en la actualidad-es: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, la cual utiliza una variante del algoritmo Diffie-Hellman de curva elíptica (ECDHE) para establecer una comunicación secreta por un medio inseguro, RSA para probar la identidad del servidor con llave publica de 2048 bits, AES_128_GCM que proporciona un cifrado autenticado, y SHA256 que es el algoritmo de Hash.

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

4.1.2 Negociación entre el cliente y el servidor Handshake

Figura 32 Tamaño Handshake

Protocolo TCP/IP	Dominio	Puerto	Handshake (bytes)
http	trademap.org	80	No implementado
https	google.com	443	4109
https	facebook.com	443	3741
https	youtube.com	443	4890
https	yahoo.com	443	5913
https	amazon.com	443	4976
https	wikipedia.org	443	3615
https	baidu.com	443	5168
https	qq.com	443	4841
https	taobao.com	443	3730
https	live.com	443	5495
https	linkedin.com	443	3360
https	yandex.com	443	3788
https	hao123.com	443	5007
https	vk.com	443	5749
https	bing.com	443	4567
https	twitter.com	443	3759
https	instagram.com	443	3904
https	msn.com	443	4001
https	aliexpress.com	443	4841
https	pinterest.com	443	3581
https	ask.com	443	4841
https	blogspot.com	443	4150
https	apple.com	443	4050
https	tmall.com	443	3730
https	wordpress.com	443	5305
https	reddit.com	443	3504
https	paypal.com	443	4207
https	mail.ru	443	3388
https	tumblr.com	443	3312
https	sohu.com	443	5783
https	microsoft.com	443	5005
https	imgur.com	443	4011
https	imdb.com	443	3236
https	netflix.com	443	3734
https	craigslist.org	443	7678
https	outbrain.com	443	4609
https	kat.cr	443	6257
https	diply.com	443	3449
https	dropbox.com	443	2821
https	github.com	443	3274
https	adcash.com	443	4234
https	popads.net	443	5317
https	dailymotion.com	443	3260
https	pixnet.net	443	3126
https	sogou.com	443	4386
https	bongaca.com	443	5433
https	booking.com	443	3194
https	adnetworkperformance.com	443	3329
https	jd.com	443	3614
https	adobe.com	443	4742
https	indiatimes.com	443	4841
https	directrev.com	443	5057
https	huffingtonpost.com	443	4841
Promedio			4354

Fuente: Propia

El tamaño promedio del handshake en las páginas analizadas es 4354 bytes, esto quiere decir que alrededor de 4Kbytes son trasmitidos en la negociación inicial entre el cliente que accede a la página y el servidor que la contiene.

4.1.3 Tiempo de procesamiento Handshake

Figura 33 Tiempo de procesamiento Handshake

Protocolo TCP/IP	Dominio	Puerto	Tiempo tcp handshake(ms)
http	trademap.org	80	508
https	google.com	443	451
https	facebook.com	443	223
https	youtube.com	443	176
https	yahoo.com	443	386
https	amazon.com	443	250
https	wikipedia.org	443	387
https	baidu.com	443	563
https	qq.com	443	298
https	taobao.com	443	932
https	live.com	443	475
https	linkedin.com	443	914
https	yandex.com	443	1931
https	hao123.com	443	2387
https	vk.com	443	700
https	bing.com	443	512
https	twitter.com	443	258
https	instagram.com	443	192
https	msn.com	443	295
https	aliexpress.com	443	746
https	pinterest.com	443	324
https	ask.com	443	1650
https	blogspot.com	443	175
https	apple.com	443	116
https	tmall.com	443	2700
https	wordpress.com	443	1903
https	reddit.com	443	590
https	paypal.com	443	385
https	mail.ru	443	1846
https	tumblr.com	443	381
https	sohu.com	443	885
https	microsoft.com	443	117
https	imgur.com	443	806

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

https	imdb.com	443	415
https	netflix.com	443	384
https	craigslist.org	443	1926
https	outbrain.com	443	876
https	kat.cr	443	539
https	diply.com	443	862
https	dropbox.com	443	305
https	github.com	443	294
https	adcash.com	443	271
https	popads.net	443	1746
https	dailymotion.com	443	312
https	pixnet.net	443	2348
https	sogou.com	443	1901
https	bongaca.com	443	380
https	booking.com	443	267
https	adnetworkperformance.com	443	206
https	jd.com	443	2608
https	adobe.com	443	425
https	indiatimes.com	443	298
https	directrev.com	443	2104
https	huffingtonpost.com	443	368
Promedio			801.80

Fuente: Propia

El tiempo promedio del handshake de TCP en las páginas analizadas es de 801,80 ms, lo cual refleja que tarda aproximadamente 1 s para establecer la negociación con el servidor.

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

4.1.4 Tiempo de procesamiento de SSL/TLS handshake

Figura 34 Tiempo de procesamiento SSL/TLS handshake

Protocolo TCP/IP	Dominio	Puerto	Tiempo SSL handshake (ms)
http	trademap.org	80	No implementado
https	google.com	443	871
https	facebook.com	443	437
https	youtube.com	443	425
https	yahoo.com	443	946
https	amazon.com	443	685
https	wikipedia.org	443	669
https	baidu.com	443	1266
https	qq.com	443	411
https	taobao.com	443	3557
https	live.com	443	1186
https	linkedin.com	443	1783
https	yandex.com	443	2907

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

https	hao123.com	443	3674
https	vk.com	443	1535
https	bing.com	443	1140
https	twitter.com	443	651
https	instagram.com	443	474
https	msn.com	443	683
https	aliexpress.com	443	1816
https	pinterest.com	443	556
https	ask.com	443	2170
https	blogspot.com	443	422
https	apple.com	443	251
https	tmall.com	443	3587
https	wordpress.com	443	2321
https	reddit.com	443	832
https	paypal.com	443	725
https	mail.ru	443	2806
https	tumblr.com	443	953
https	sohu.com	443	2078
https	microsoft.com	443	254
https	imgur.com	443	1411
https	imdb.com	443	689
https	netflix.com	443	679
https	craigslist.org	443	3156
https	outbrain.com	443	2290
https	kat.cr	443	1253
https	diply.com	443	1380
https	dropbox.com	443	950
https	github.com	443	766
https	adcash.com	443	716
https	popads.net	443	2476
https	dailymotion.com	443	1022
https	pixnet.net	443	4039
https	sogou.com	443	3332
https	bongaca.com	443	734
https	booking.com	443	754
https	adnetworkperformance.com	443	513
https	jd.com	443	3124
https	adobe.com	443	966
https	indiatimes.com	443	419
https	directrev.com	443	3697
https	huffingtonpost.com	443	644
Promedio			1454.36

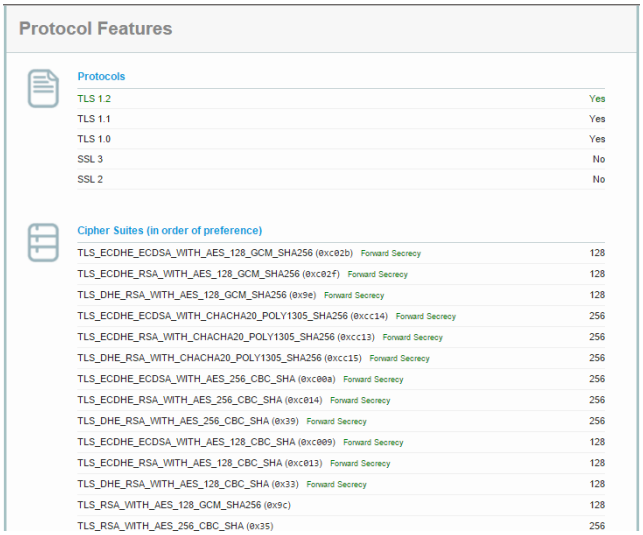
Fuente: Propia

El tiempo promedio del handshake de SSL/TLS en las páginas analizadas es de 1454 ms, lo cual refleja que tarda poco más de 1 segundo para establecer la negociación con el servidor usando el protocolo HTTPS.

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

4.1.5 Compatibilidad de navegadores web con algoritmos de cifrado

Figura 35 Análisis de Navegador web



Fuente: Propia

Tabla 1 Compatibilidad de navegadores con el protocolo SSL/TLS

	NAVEGADOR	Internet Explorer (v11.0.96)	Google Chrome (v46.0)	Safari (v5.1.7)	Opera (v32.0)	Mozilla Firefox (v41.0)	Mozilla Developer (v43.0)	Comodo Dragon (v45.6)
PROTOCOLOS	TLS 1.2	Si	Si	No	Si	Si	Si	Si
	TLS 1.1	Si	Si	No	Si	Si	Si	Si
	TLS 1.0	Si	Si	Si	Si	Si	Si	Si
	SSL 3	Si	No	Si	No	No	No	No
	SSL 2	No	No	No	No	No	No	No

Fuente: Propia

Podemos apreciar en la tabla N° 1 que los navegadores más usados son compatibles con las últimas versiones del protocolo de cifrado SSL/TLS, perdiendo la compatibilidad con las versiones más antiguas del protocolo.

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

Tabla 2 Compatibilidad de las combinaciones permitidas por los navegadores

	NAVEGADOR	Internet Explorer	Google Chrome	Safari	Opera	Mozilla Firefox	Mozilla Developer	Comodo Dragon
COMBINACIONES DE CIFRADO	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Si	Si	Si	Si	Si	Si	Si
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Si	Si	Si	Si	Si	Si	Si
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Si	Si	No	Si	Si	Si	Si
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Si	Si	Si	Si	Si	Si	Si
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Si	Si	Si	Si	Si	Si	Si
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	No	Si	No	Si	No	No	si
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	No	Si	No	Si	No	No	Si
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Si	Si	No	Si	Si	Si	Si
	TLS_RSA_WITH_AES_128_GCM_SHA256	No	Si	No	Si	No	No	Si
	TLS_RSA_WITH_AES_256_CBC_SHA	Si	Si	Si	SI	Si	Si	Si
	TLS_RSA_WITH_AES_128_CBC_SHA	Si	Si	Si	Si	Si	Si	Si
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Si	Si	Si	Si	Si	Si	Si
	TLS_RSA_WITH_RC4_128_SHA	No	No	Si	No	No	No	No
	TLS_RSA_WITH_RC4_128_MD5	No	No	Si	No	No	No	No
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Si	Si	No	No	No	No	Si
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	No	Si	No	No	Si	Si	Si
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	No	Si	No	No	Si	Si	Si
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	No	Si	No	No	No	No	Si
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Si	No	Si	No	No	No	No
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Si	No	Si	No	No	No	No
	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	Si	No	Si	No	No	No	No
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Si	No	No	No	No	No	No
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Si	No	No	No	No	No	No
	TLS_RSA_WITH_AES_256_GCM_SHA384	Si	No	No	No	No	No	No
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Si	No	No	No	No	No	No
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Si	No	No	No	No	No	No
	TLS_RSA_WITH_AES_256_CBC_SHA256	Si	No	No	No	No	No	No
	TLS_RSA_WITH_AES_128_CBC_SHA256	SI	No	No	No	No	No	No
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Si	No	No	No	No	No	No
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	Si	No	No	No	No	No	No
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	Si	No	No	No	No	No	No
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Si	No	No	No	No	No	No

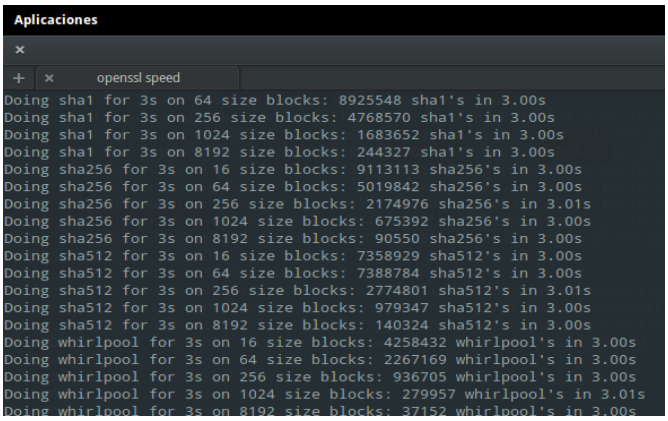
Fuente: Propia

La siguiente tabla N° 2 muestra la compatibilidad de los navegadores con las combinaciones existentes de algoritmos del protocolo SSL/TLS, podemos apreciar que la combinación TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 que fue evaluada anteriormente resulto ser la más utilizada por las páginas web y tiene compatibilidad con todos los navegadores salvo Safari, con lo cual podemos decir que según nuestro análisis la combinación escogida es adecuada para su uso.

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

4.1.6 Costo computacional

Figura 36 Análisis de algoritmos HASH



Fuente: Propia

Tabla 3 Costo computacional de algoritmos HASH

Type/paq	16 bytes(kb)	64 bytes(kb)	256 bytes(kb)	1024 bytes(kb)	8192 bytes(kb)
sha1	61695.53	175386.62	382422.19	541341.51	634058.07
rc4	366380.13	586570.67	687242.15	718823.77	725027.38
aes-128 cbc	110777.77	120815.13	122967.98	124390.40	123473.31
aes-192 cbc	94165.14	100747.01	102667.43	103323.65	103273.63
aes-256 cbc	81640.59	86693.59	87798.27	88380.76	88552.53
sha256	46105.87	102795.97	177884.25	219389.11	234657.11
sha512	37684.47	150545.28	226691.50	319419.05	364802.55

Fuente: Propia

Se realizaron pruebas en periodos de 3 segundo en una computadora con procesador Core i5 3230m a 2.60Ghz, inyectando paquetes de 16, 64, 256, 1024 y 8192 kb, para lo cual analizamos que el algoritmo de Hash (sha256) puede procesar paquetes en 1 segundo de manera más eficiente que los demás, siendo un gasto computacional bajo para un equipo de gama media/baja.

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

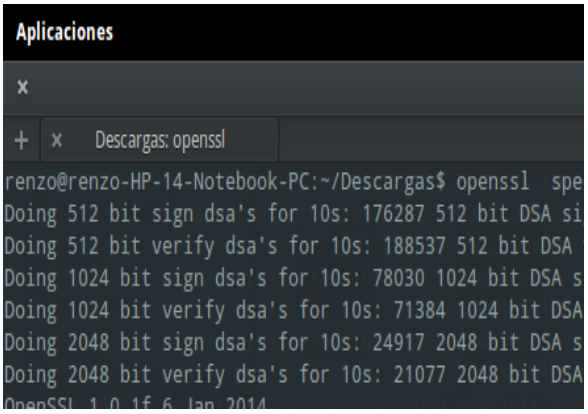
Tabla 4 Conexiones posibles del algoritmo de clave pública RSA

Algoritmo & key	sign (s)	verify (s)	sign/s	verify/s
rsa 512 bits	0.000026	0.000002	38750.50	433333.30
rsa 1024 bits	0.000095	0.000007	10557.10	152421.70
rsa 2048 bits	0.000691	0.000019	1447.60	51461.00
rsa 4096 bits	0.004494	0.000071	222.50	14075.80

Fuente: Propia

Se realizaron pruebas en una computadora con procesador core i5 3230m a 2.60Ghz, la cual sirvió como simulador del servidor web, podemos comprobar que con el algoritmo de clave pública RSA con key de 2048 bits que fue el más utilizado por las páginas web analizadas. Nuestro servidor puede hacer una firma en 0.000691 segundos, soportar alrededor de 1447 conexiones SSL por segundo, y a su vez verificar cerca de 51461 firmas por segundo.

Figura 37 Analisis de algoritmo dsa



Fuente: Propia

Tabla 5 Conexiones posibles del algoritmo de clave pública DSA

Algoritmo & key	sign (s)	verify (s)	sign/s	verify/s
dsa 512 bits	0.000066	0.000069	15229.00	14591.10
dsa 1024 bits	0.000153	0.000165	6540.40	6045.20
dsa 2048 bits	0.000490	0.000576	2042.70	1735.20

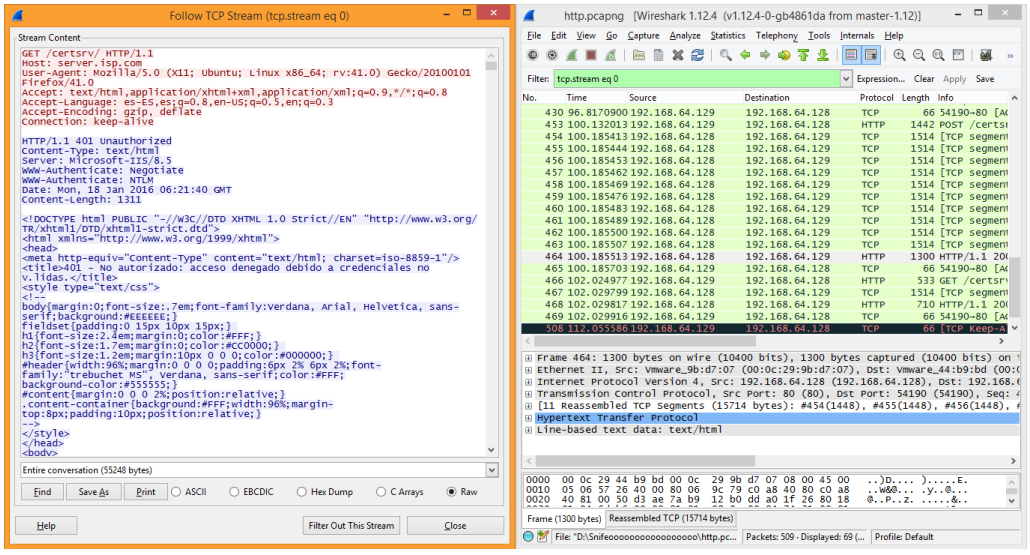
Fuente: Propia

Comparando algoritmos rsa de la tabla N°4 con algoritmos dsa de la tabla N°5 en la cual analizamos que el dsa con key 2048 bits que soporta más conexiones a su vez (2042.70 conexiones por segundo), pero verifica menos firmas por segundo (1735.20) que el rsa.

4.1.7 Datos sin cifrado

Evaluando el tráfico en una comunicación vía HTTP se demostró que todos los datos son enviados sin ningún medio de seguridad (cifrado).

Figura 38 Sniffeo de página HTTP



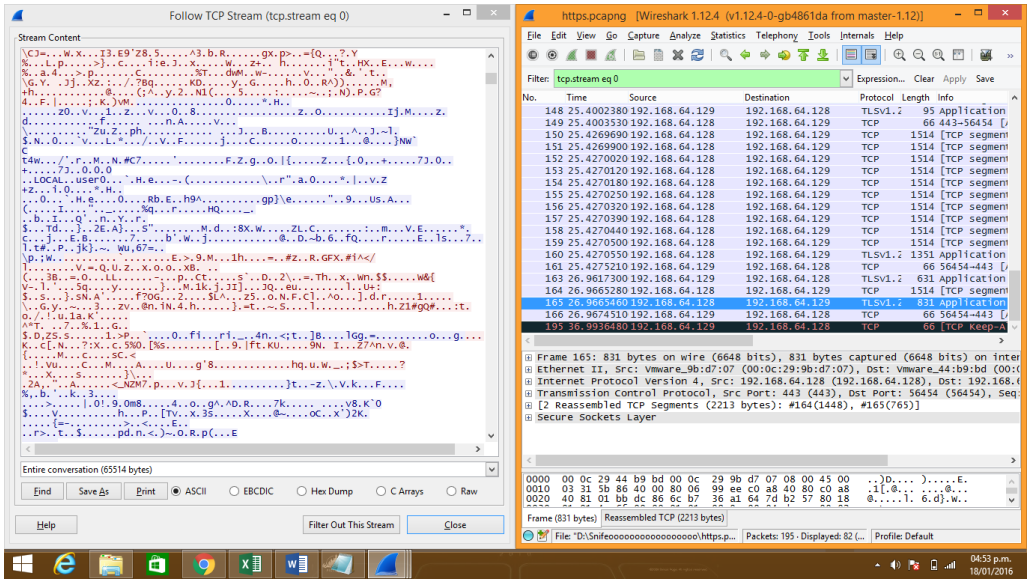
Fuente: propia

En la figura 38 se puede apreciar que la cantidad de datos sin cifrar en la comunicación HTTP es de 55248 bytes.

4.1.8 Datos con cifrado

Evaluando el tráfico en una comunicación vía HTTPS se demostró que todos los datos son enviados por un medio seguro (cifrado).

Figura 39 Sniffeo página HTTPS



Fuente: propia

En la figura 39 se puede apreciar que la cantidad de datos con cifrado en la comunicación HTTPS es de 65514 bytes.

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

4.1.9 Proporción de tamaño entre datos con cifrado y datos sin cifrado

Evaluando el tráfico en las comunicaciones vía HTTP, HTTPS se determinó que los datos cifrados son 1.1858 veces más grandes.

$$\frac{datos\ con\ cifrado}{datos\ \text{sin}\ cifrado}$$

Haciendo la comparación del tráfico con cifrado y sin cifrado, se determinó que el tamaño de los datos al aplicar cifrado aumento un 18.58%.

$$\frac{(dcc - dsc)}{dsc} \times 100\%$$

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

4.2 Discusión de resultados.

Mediante el análisis e interpretación de los resultados se obtuvieron datos específicos, en la cual se implementó en una infraestructura de PKI de un solo nivel con 3 ámbitos (cliente – servidor – Entidad Certificadora).

Analizando la siguiente tesina (Hernández Ortiz , Peña Blanco, Ramírez Amaya, Rodríguez Baños, & Acosta Gil , 2010) cuya finalidad es que mediante el uso de software libre como OpenSSL, Stunnel y rsyslog se respalden las bitácoras de servidores remotos en un servidor central de bitácoras, pero que los mensajes de syslog viajen cifrados, y dentro de un túnel ya que la conexión entre ellos puede ser vía una red pública de datos y se quiere garantizar la confidencialidad, autenticidad e integridad de los datos.

Teniendo en cuenta que dicha implementación se desarrolló en dos máquinas con procesador Intel Xeon E5320 con 2Gbytes en RAM y versión Linux 2.6.27 de la distribución Ubuntu 8.10.

Este desarrollo utilizó RSA 2048 bits para llave pública la cual permitirá el cifrado del mensaje, acorde a ello nuestra investigación realizada en la tabla N°4 muestra el tiempo de procesamiento de dicha llave y a la vez en la figura N°31, podemos comprobar que con el algoritmo de clave pública RSA con key de 2048 bits es el más utilizado por las páginas web analizadas. Desafortunadamente Stunnel y OpenSSL tienen sus limitaciones, Stunnel solo soporta Proxy transparente y solo puede ser implementado en servicios que solo utilicen un solo puerto, OpenSSL por su lado puede ser complicado en la generación de los certificados. Finalmente se concluye dicha contrastación que el campo en aplicación fue en VPNs.

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

Según (Ordeñez Calero, 2013) desarrollaron un sistema web para la gestión de información de la empresa TELALCA S.A, a la vez se implementó seguridad mediante el cifrado SSL del protocolo HTTPS, para ello se utilizó un servidor Apache Tomcat 6.0 y la generación del certificado digital con una key public RSA 2048 que permitirá el acceso al sistema a través del cifrado SSL del protocolo HTTPS. En la tabla N°4 muestra el tiempo de procesamiento de dicha llave y a la vez en la figura N°31, podemos comprobar que con el algoritmo de clave pública RSA con key de 2048 bits es el más utilizado por las páginas web analizadas. Nuestra investigación genera los certificados digitales mediante la "entidad de certificación (Active Directory Certificate Services) de Windows server 2012" mientras que para esta investigación utilizan la herramienta Keytool que viene dentro de la plataforma de Java.

Prosiguiendo con las discusiones de resultado analizaremos la siguiente investigación (Villegas Gómez, 2010) en la cual hicieron comparaciones de algoritmos de llave publica como lo son RSA, ElGamal, y ECES, los cuales proveen el servicio de confidencialidad. Esto, género que el más óptimo sea RSA debido al nivel de seguridad y madurez que tiene, programándolo en java y a la vez recomendaron que el tamaño de la llave publica sea mayor a 1024 bits.

En la tabla N°4 muestra el tiempo de procesamiento de dicha llave que en esta tesina se investigó y a la vez en la figura N°31, podemos comprobar que con el algoritmo de clave pública RSA con key mayor a 1024 bits (2048 bits) es el más utilizado por las páginas web analizadas. Dicha investigación fue base para la

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

nuestra, mediante la cual se tomó como buenas prácticas para hacer el análisis de los algoritmos RSA y DSA mostrada en la tabla N°4 y la tabla N°5.

En el mundo actual de las telecomunicaciones la transmisión de datos enviados por la red es cada vez más frecuente por medio de intranet o internet, perder parte de los datos que se envían es un problema que se puede suscitar en la red, generado por una congestión o porque se perdió la ruta que se tenía prevista para el envío de los datos.

Esto, nos lleva al análisis de la siguiente investigación (Chapaca Garzón & Rojas Bustamante, 2013) cuyo objetivo principal es Analizar, diseñar y desarrollar un prototipo de protocolo de transporte basado en comunicación TCP con capacidad de cubrir las necesidades de transferencia de datos seguros, confiables y de alta disponibilidad. Dicha tesina se tomó como buenas prácticas para la conexión cliente – servidor – CA en nuestra investigación realizada, la cual nos ofrece una conexión segura en 3 máquinas virtuales.

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

4.3 Contrastación de Hipótesis

La contrastación de la hipótesis se realizó teniendo en cuenta los indicadores de la variable dependiente.

Formulación de Hipótesis

H_0 : Hipótesis Nula.

$$H_0: \quad \mu_{dcc} - \mu_{dsc} = 0$$

El tamaño de datos con cifrado es igual al tamaño de datos sin cifrado.

H_A: Hipótesis Alterna.

$$H_A: \quad \mu_{dcc} - \mu_{dsc} > 0$$

El tamaño de datos con cifrado es mayor al tamaño de datos sin cifrado.

Donde
dcc: datos con cifrado
dsc: datos sin cifrado

Tabla 6 Tamaño de datos

Datos transmitidos	Datos con cifrado	Datos sin cifrado
Tamaño de datos (bytes)	65514	55248

Fuente: propia

$$\mu_{dcc} - \mu_{dsc} > 0$$

65514 – 55248 = 10266

Decisión

$10266 \in$ a la región crítica. Por tanto se rechaza la hipótesis nula y se acepta la hipótesis alterna.

Conclusión

Se estima el tamaño de los datos con cifrado es mayor que el tamaño de los datos sin cifrado

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

CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN

5.1 Reunir requisitos y expectativas

a) Quienes son las personas que utilizan la red:

Los bachilleres Renzo Augusto Ariansen Moncada y José Iván Rojas Díaz

b) Datos críticos de la organización
Los datos críticos se encontraban en el servidor web (IIS), el servidor de entidad certificadora (CA).

c) Que operaciones han sido declaradas críticas por la organización

La comunicación entre el servidor Web y el usuario final

d) Protocolos permitidos en la red

Red LAN

a) Sistema de nombres de dominio (DNS): TCP/UDP 53.
b) Protocolo de transferencia de hipertexto (HTTP), TCP 80.
c) Protocolo de transferencia de hipertexto seguro (HTTPS), TCP 443.

e) Cuantos hosts son soportados y cuáles son los tipos

Se hará uso de 3 hosts, un servidor será la entidad certificadora de tipo root, un servidor web (IIS) que alojara una página web y un cliente para acceder a la página web.

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

f) Quien es el responsables de las direcciones, la denominación, el diseño de topología y la configuración de las LAN.

Los Bachilleres: Renzo Augusto Ariansen Moncada y José Iván Rojas Díaz

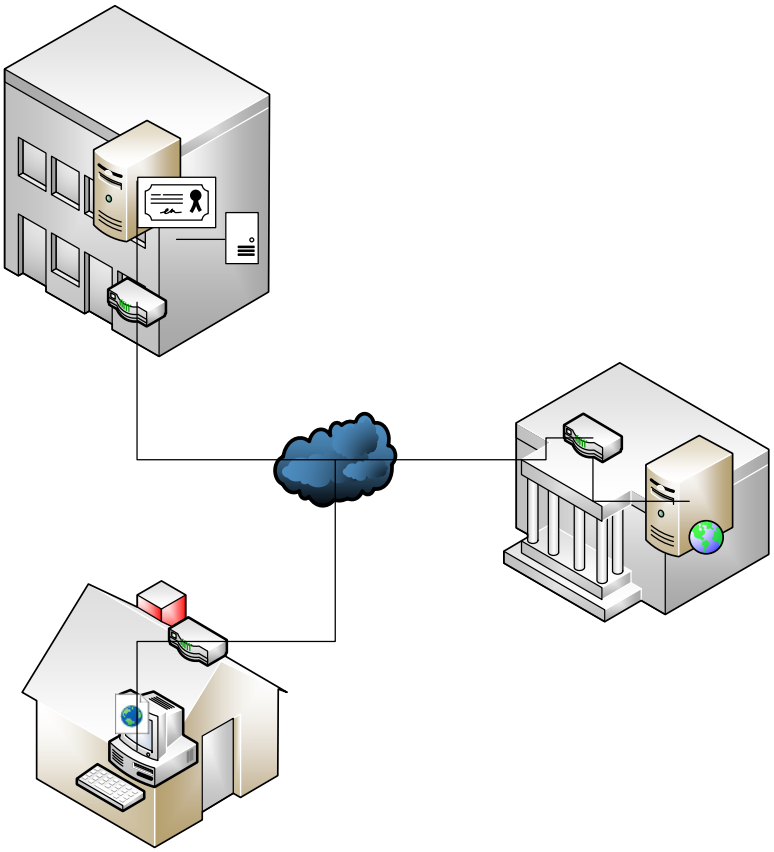
g) Cuáles son los recursos humanos organizacionales, de hardware y de software

Recursos de hadware: (1) Computadora con procesador core i5-3230m a 2.60Ghz y (1) computadora con procesador core i5 – 4200U a 2.30 GHz.
Recursos de Software: (1) Servidor Windows Server 2012 R2 (Root CA), (1) Servidor Windows Server 2012 R2 (IIS, user) y (1) Ubuntu (user)

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

5.2 Diseño de Capa física

Figura 40 Diseño Capa Física propuesta



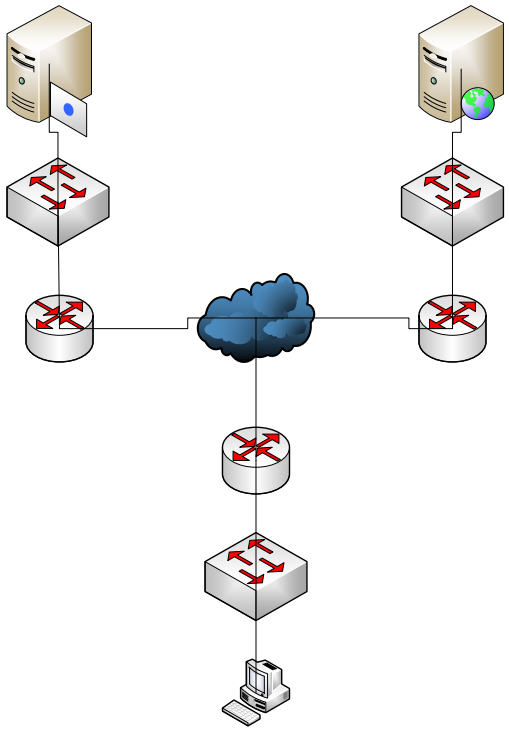
Fuente: propia

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

5.3 Diseño de la estructura física y lógica de la red

5.3.1 Estructura física

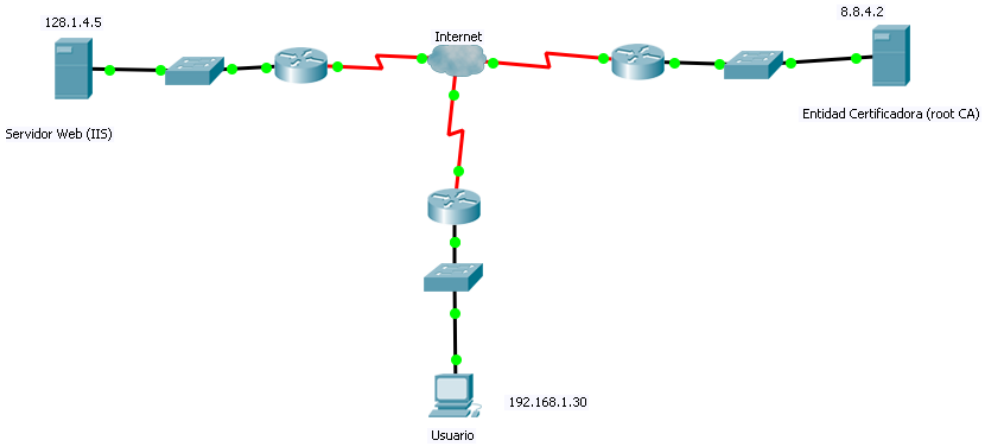
Figura 41 Estructura física



Fuente: propia

5.3.2 Estructura lógica

Figura 42 Estructura lógica

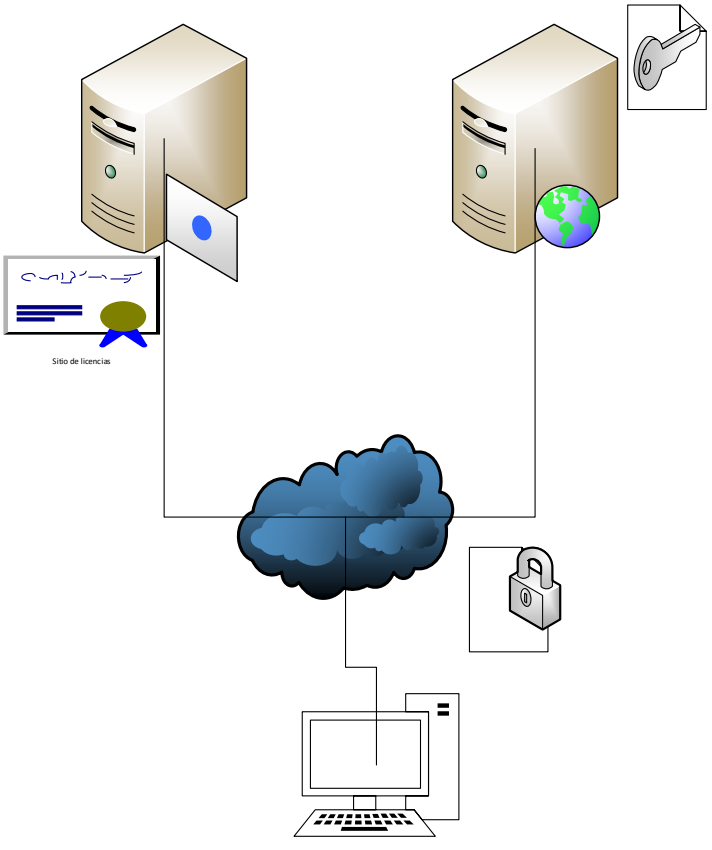


Fuente: propia

5.4 Implementación de protocolo de cifrado - prototipo

Se usó una infraestructura de PKI para hacer uso del protocolo de cifrado TLS en una página web, esta consiste en un servidor de CA (entidad certificadora) y un servidor Web IIS, ambos serán Windows Server 2012 R2, pues en esta versión del sistema operativo podemos encontrar la combinación de algoritmos de cifrado correspondientes a TLS 1.2.

Figura 43 Infraestructura de PKI



Fuente: Propia

El uso de esta infraestructura de PKI es de Root CA, con la cual directamente solicitaremos a la CA la firma digital de nuestro

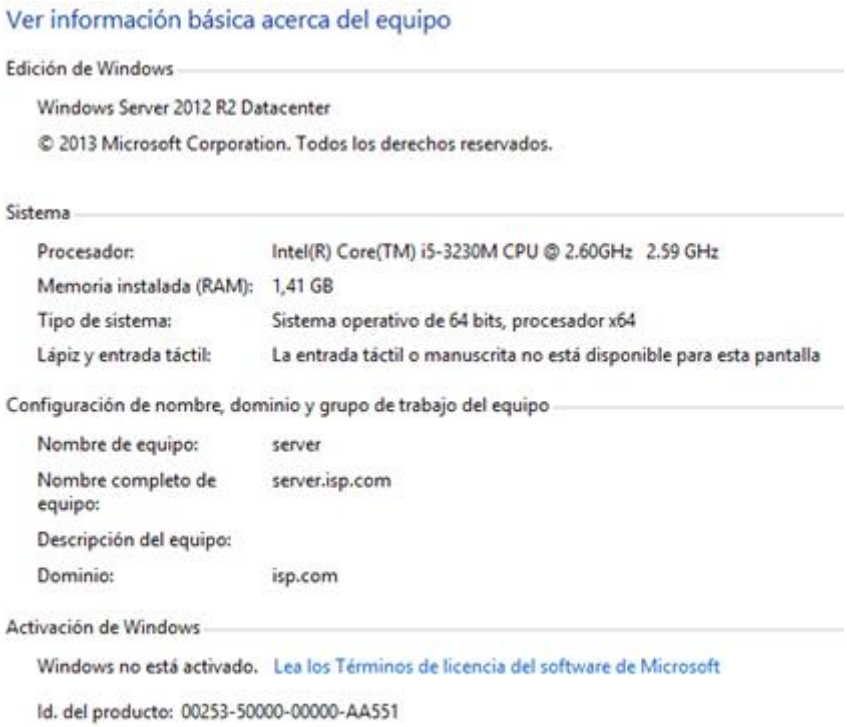
servidor Web.

Se implementará un servidor Web el cual usará HTTPS como protocolo de transferencia de hipertexto, para ello usaremos una entidad certificadora de tipo Root para emitir el certificado que luego será instalado en nuestro servidor Web

Componentes a usar

1. Servidor Windows Server 2012 R2 (Root CA)
2. Servidor Windows Server 2012 R2 (IIS, user)
3. Ubuntu (user)

Figura 44 Nombre del servidor

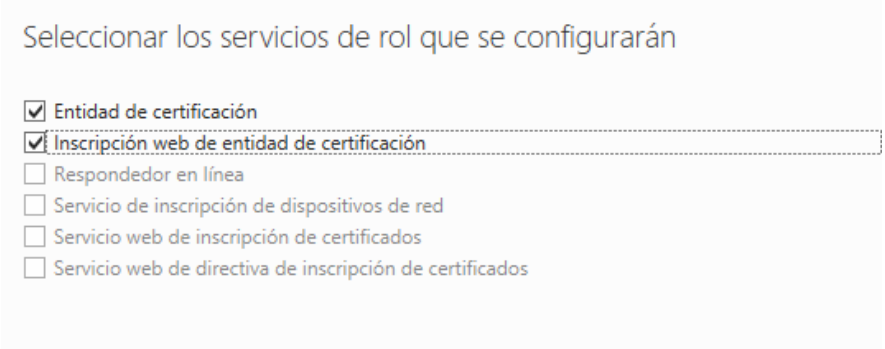


Fuente: Propia

Creamos un dominio para crear nuestra entidad certificadora y nuestra página Web, en este caso le llamamos isp.com, y nuestro servidor web se llama server, nuestra entidad certificadora se llama SERVER-CA, ambos se encuentran dentro del dominio isp.com.

Instalamos el servicio de entidad certificadora de Active Directory

Figura 45 Servicios de Rol



Fuente: Propia

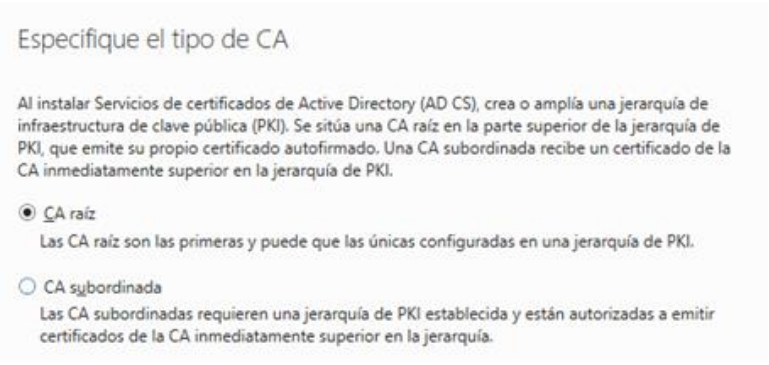
Seleccionaremos los servicios del rol que configuraremos, en nuestro caso tenemos la entidad de certificación que es la que nos permitirá emitir, revocar los certificados desde el servidor y la inscripción Web de entidad de certificación la que nos permitirá conectarnos a nuestra entidad certificadora desde cualquier explorador web para descargar los certificados de la CA, o solicitar certificados, en nuestro caso lo usaremos para hacer la solicitud de un certificado para server Web

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

Figura 46 Tipo de instalación de CA

Fuente: Propia

Figura 47 Tipo de CA



Fuente: Propia

Tras instalar los servicios de entidad certificadora de Active Directory (ADCS) podemos configurar el tipo de entidad certificadora que tenemos, en nuestro caso por tener un dominio, y emitiremos directamente los certificados, haremos uso de una CA empresarial de tipo Root.

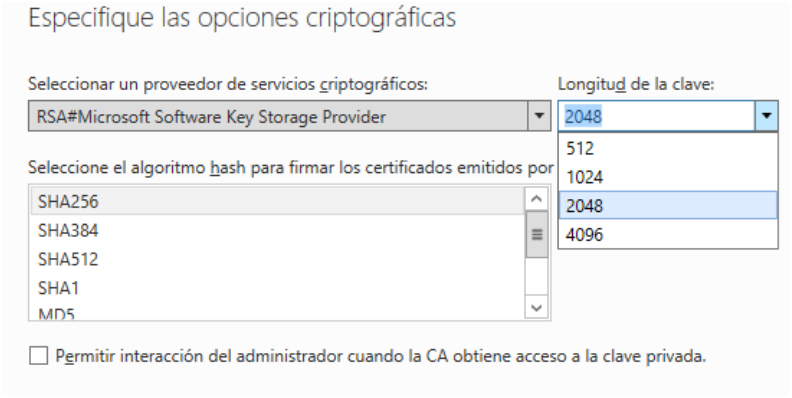
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 48 Tipo de Clave privada

Fuente: Propia

Lo siguiente es configurar la clave privada que usaremos, para lo cual creamos una nueva clave privada.

Figura 49 Opciones Criptográficas



Fuente: Propia

Seleccionamos un proveedor de servicios criptográficos, el tamaño de la clave pública, y el algoritmo de Hash.

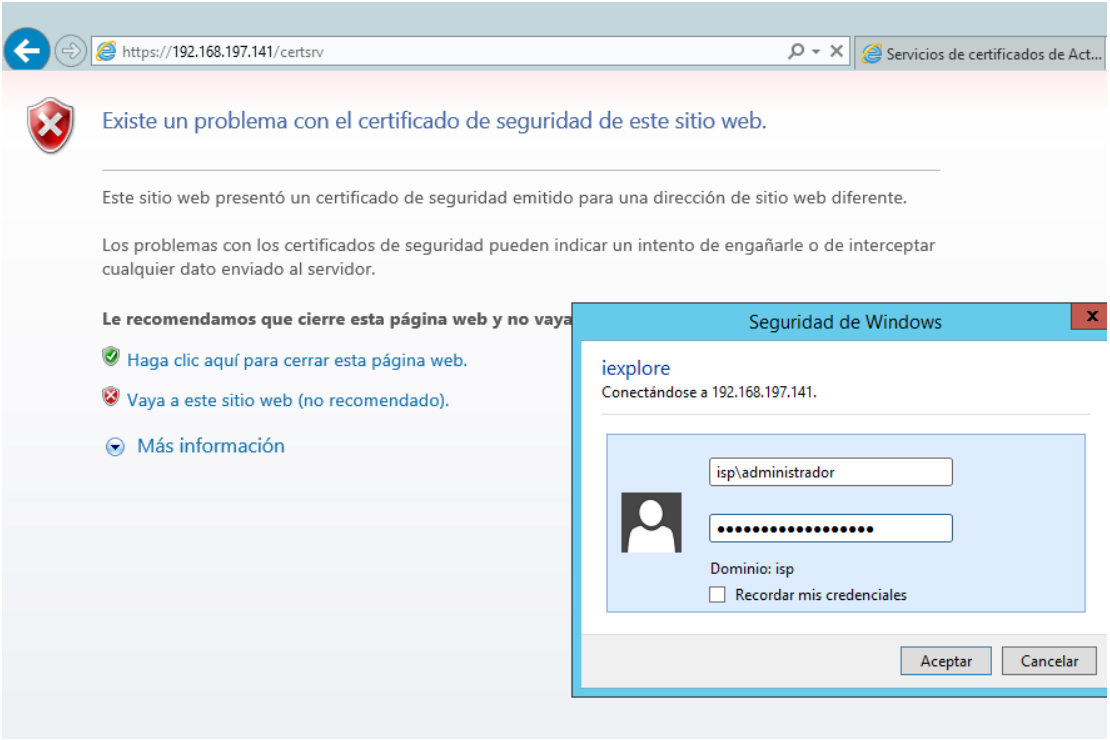
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 50 Inscripción Web de Entidad Certificadora

Fuente: Propia

Comprobamos que podemos acceder desde el navegador a la inscripción web de la entidad certificadora.

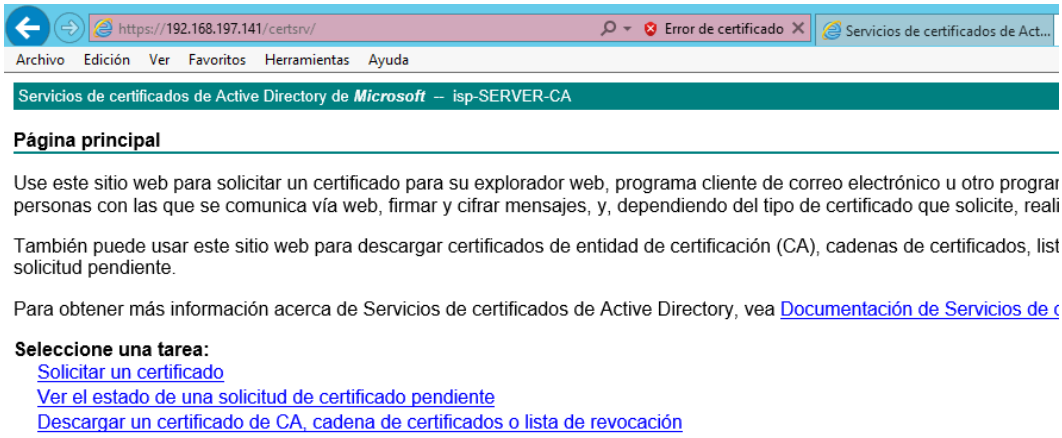
Figura 51 Ingreso de Usuario



Fuente: Propia

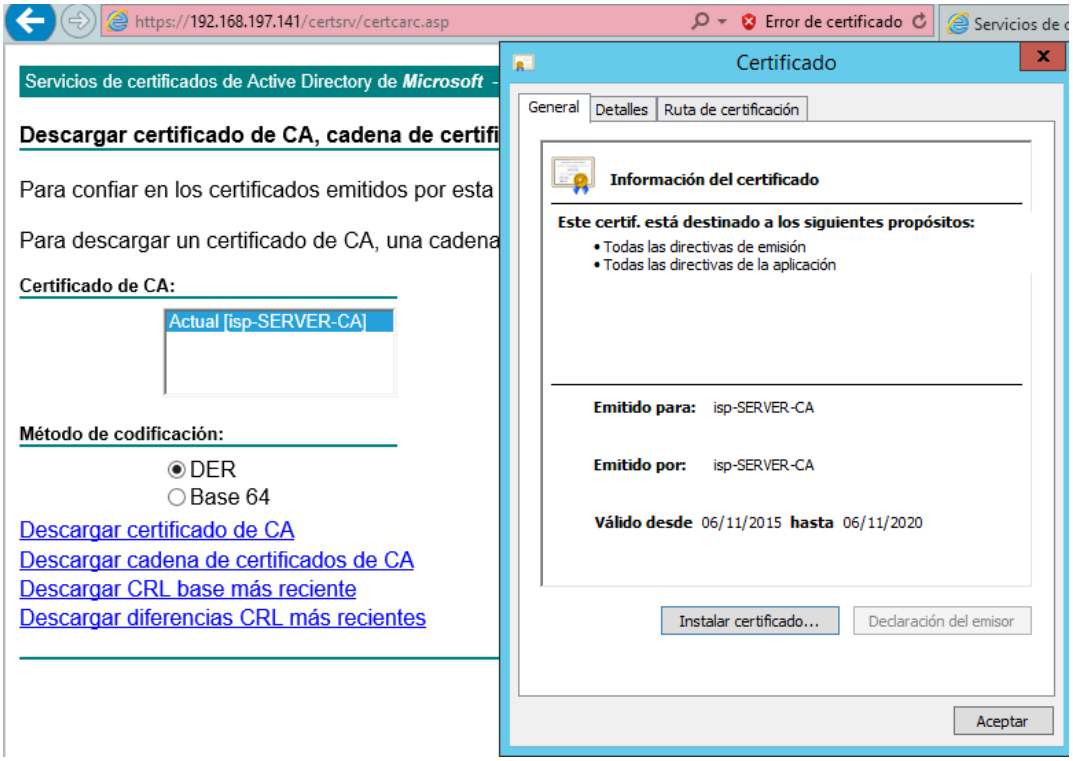
Desde el servidor de IIS Web Server accedemos desde nuestro navegador a la inscripción web de la entidad certificadora

Figura 52 Inscripción web de entidad certificadora en modo HTTPS



Fuente: Propia

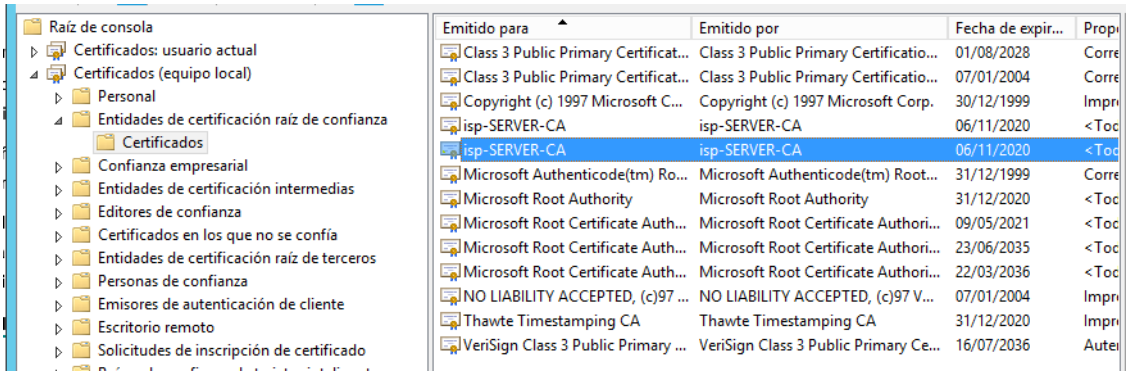
Figura 53 Descarga de Certificado de Entidad Certificadora



Fuente: Propia

Vamos a descargar el certificado de la CA para que nuestro servidor IIS confíe en la entidad certificadora, posteriormente lo instalamos.

Figura 54 Entidades de certificación raíz de confianza

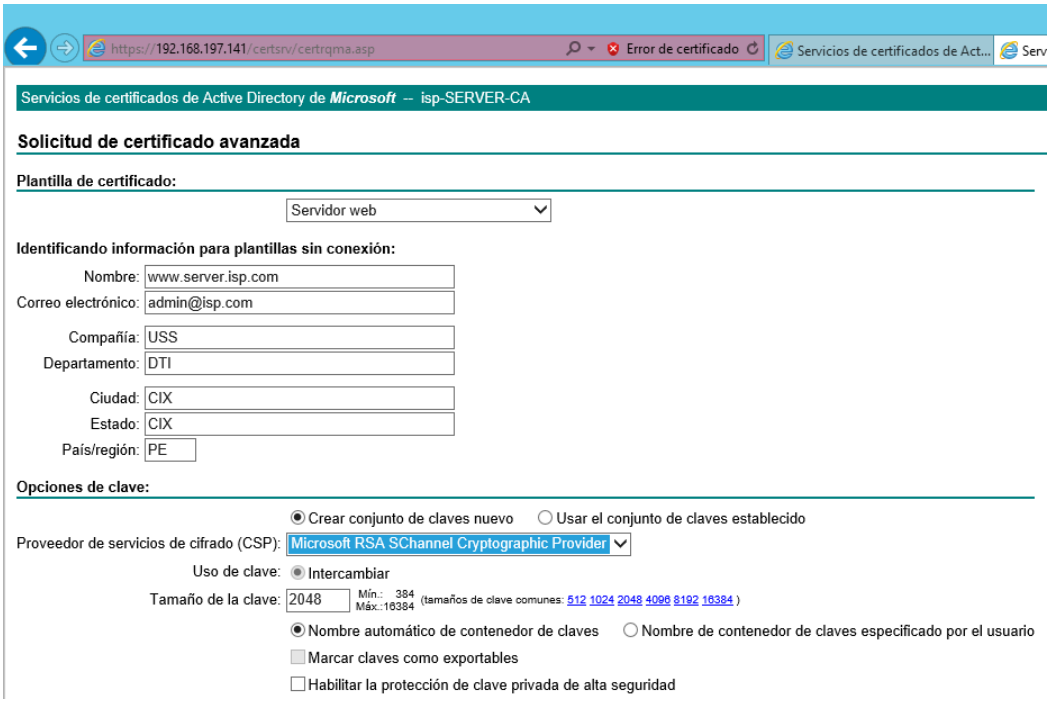


Fuente: Propia

Vemos que se instaló en las entidades de certificación de raíz de confianza, con ello podemos hacer que nuestro servidor IIS confíe en la entidad certificadora y no arroje ningún posterior error.

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

Figura 55 Solicitud de certificado avanzada



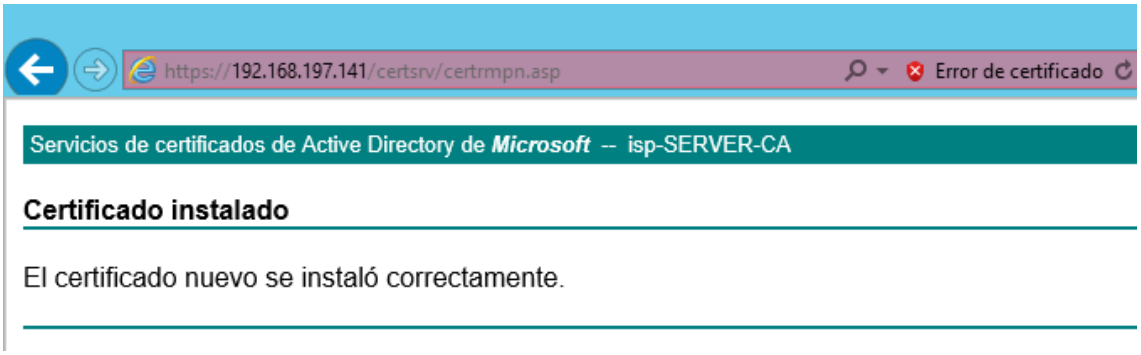
Fuente: Propia

Hacemos la solicitud del certificado para el servidor web, para la configuración de nuestra entidad certificadora hemos permitido que automáticamente se emitan los certificados

Figura 56 AutoEmisión del certificado

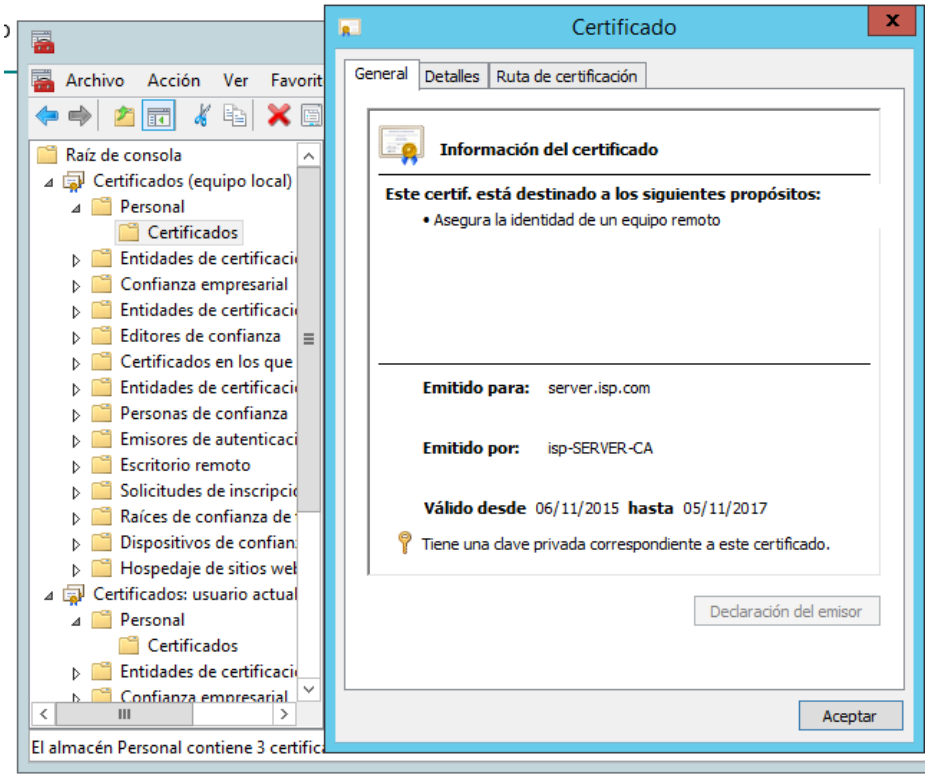
Fuente: Propia

Figura 57 Instalación del certificado



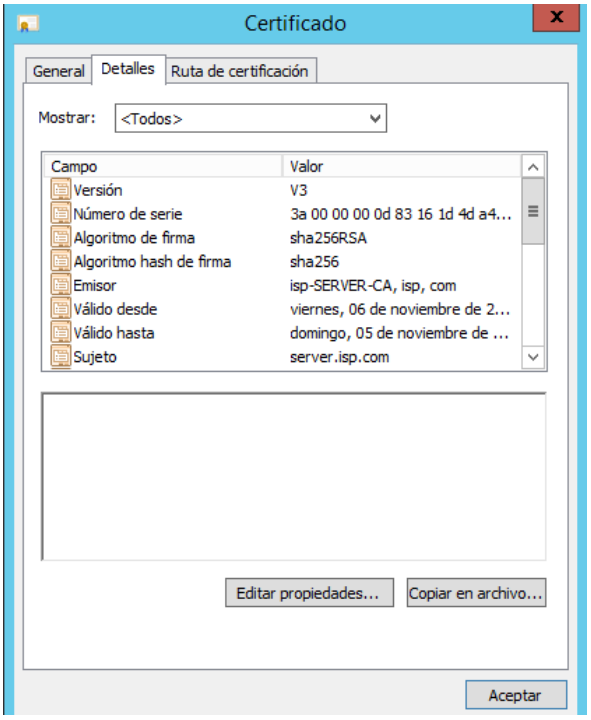
Fuente: Propia

Figura 58 Certificado emitido por CA para Web Server



Fuente: Propia

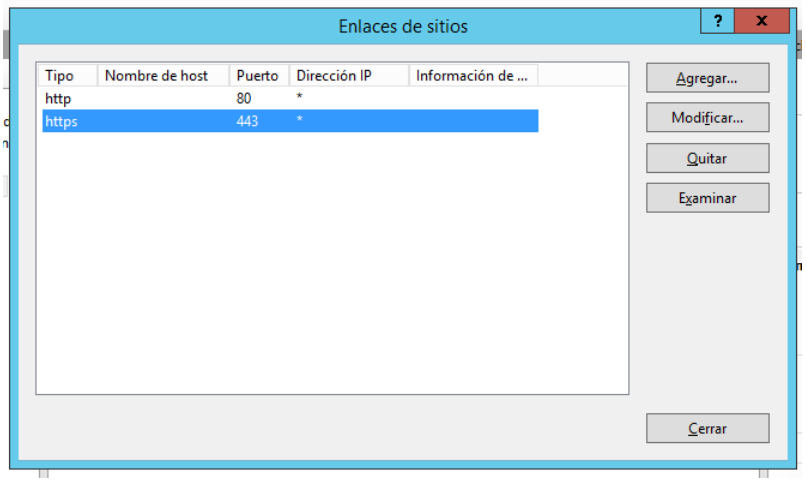
Figura 59 x.509 v3 Certificado



Fuente: Propia

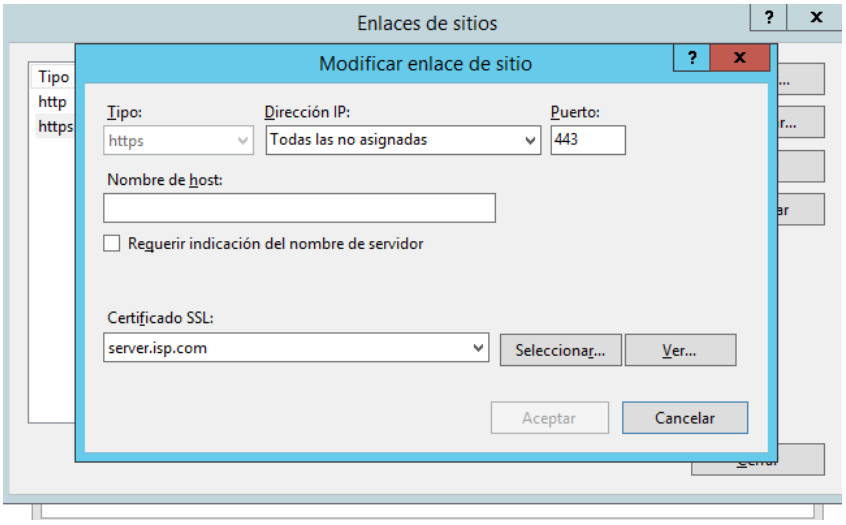
Instalamos el certificado emitido por la entidad certificadora para que podamos hacer uso de este en nuestro servidor web

Figura 60 Configuración Enlace de sitio en IIS



Fuente: Propia

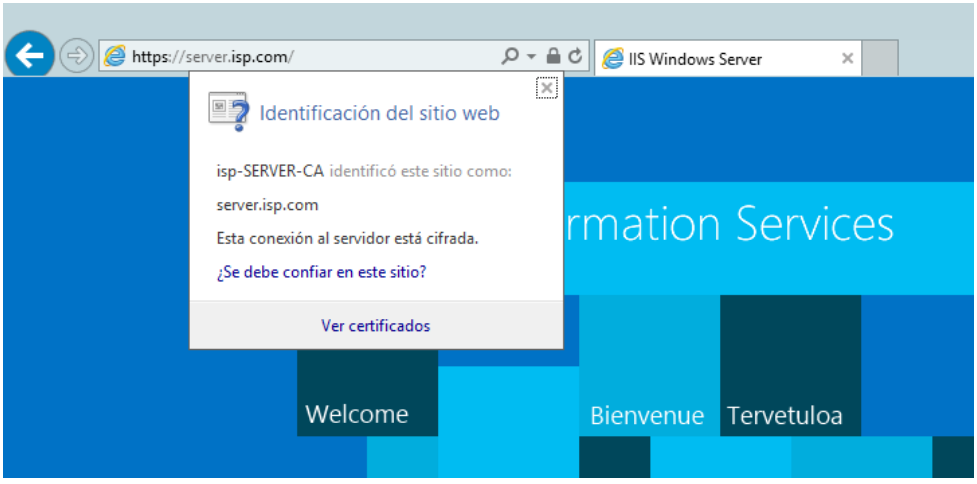
Figura 61 Selección del certificado SSL para el Servidor Web



Fuente: Propia

En nuestro servidor IIS hacemos la integración del certificado emitido por la entidad certificadora (CA), con esto ya podemos hacer uso de la página Web segura con HTTPS.

Figura 62 Comprobación del sitio por CA

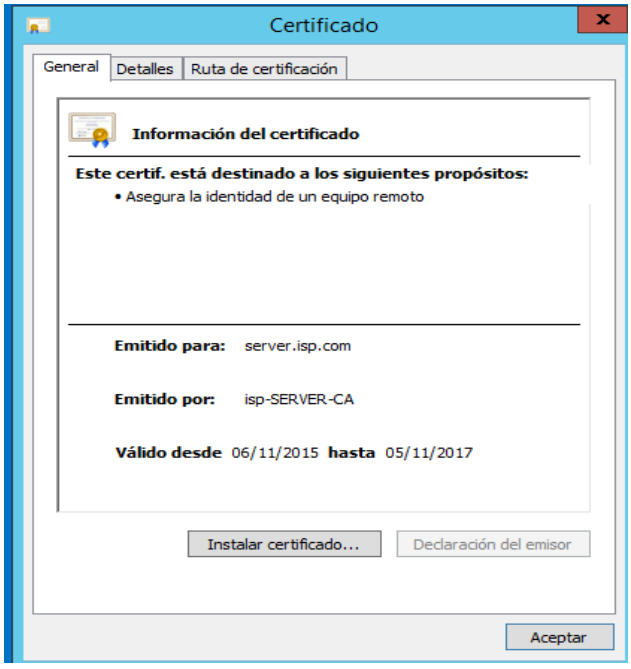


Fuente: Propia

Accedemos desde otro navegador a nuestro servidor IIS y podemos ver que la entidad certificadora identifica al sitio y que la conexión con el servidor está cifrada.

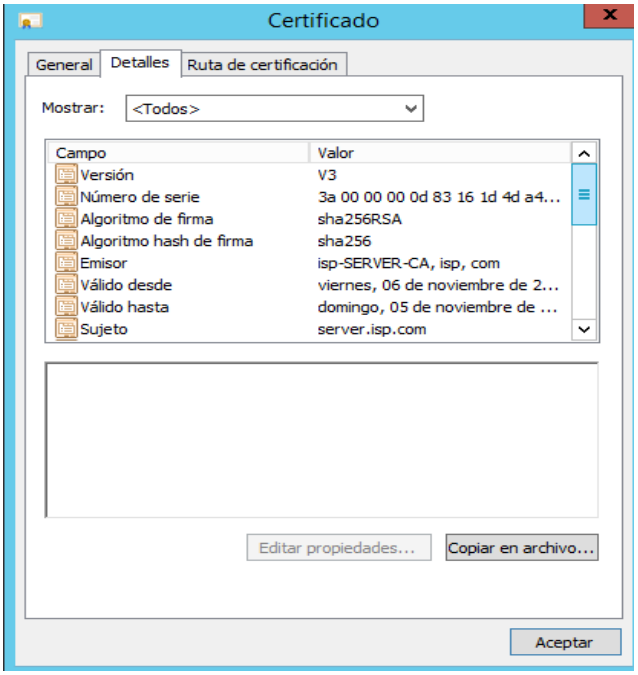
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 63 Certificado de la página Web



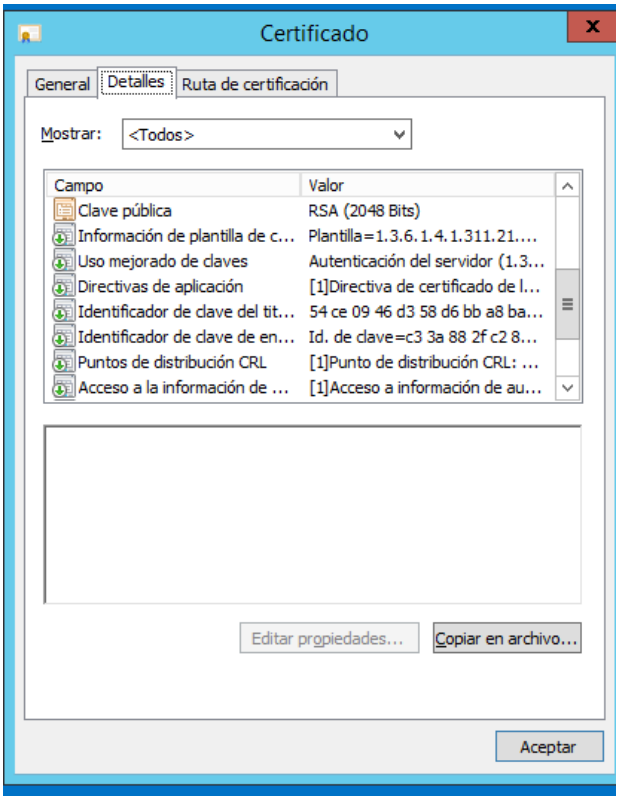
Fuente: Propia

Figura 64 Certificado x.509 v3 de página Web



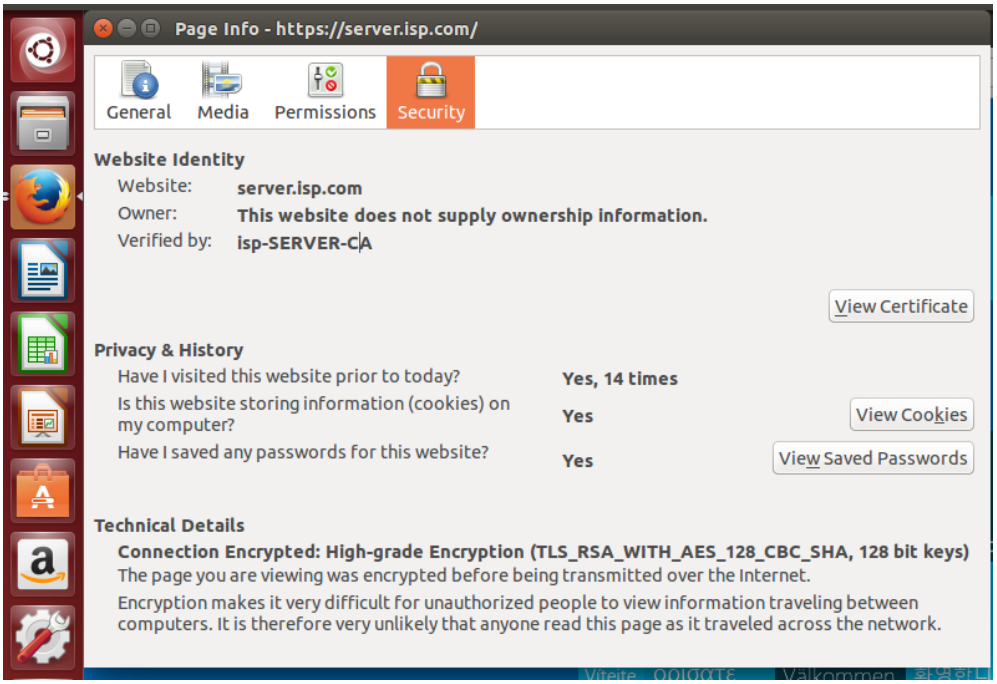
Fuente: Propia

Figura 65 Clave pública en Certificado x.509 v3



Fuente: Propia

Figura 66 Información de Web seguro en Ubuntu



Fuente: Propia

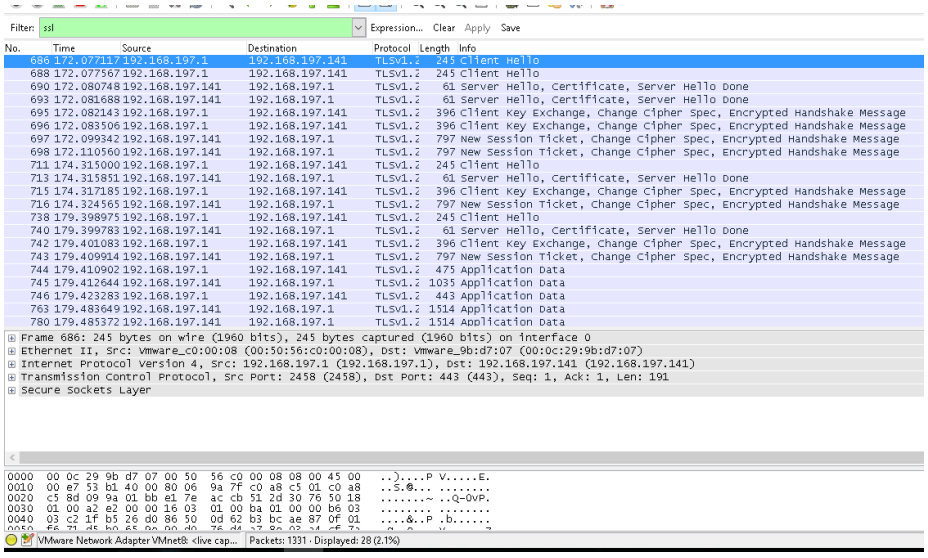
Las combinación que escogimos para nuestro certificado, es la misma que se resultó ganadora en la evaluación de las páginas web más visitadas (Company, 2015), lo que difiere en nuestro caso es que la comunicación secreta se realiza mediante RSA directamente, y no utiliza la variante de Diffie-Hellman, y la autenticación del cifrado en nuestro caso es con CBC que cifra bloques de datos tomando como referencia el bloque actual y el bloque anterior, en cambio en GCM la autenticación del cifrado tiene un contador para cada bloque de datos, lo que ayuda a evitar enviar el mismo bloque dos veces.

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

5.5 Captura de Trafico

El tráfico de la figura 67 corresponde al handshake de SSL que se establece en primera instancia,

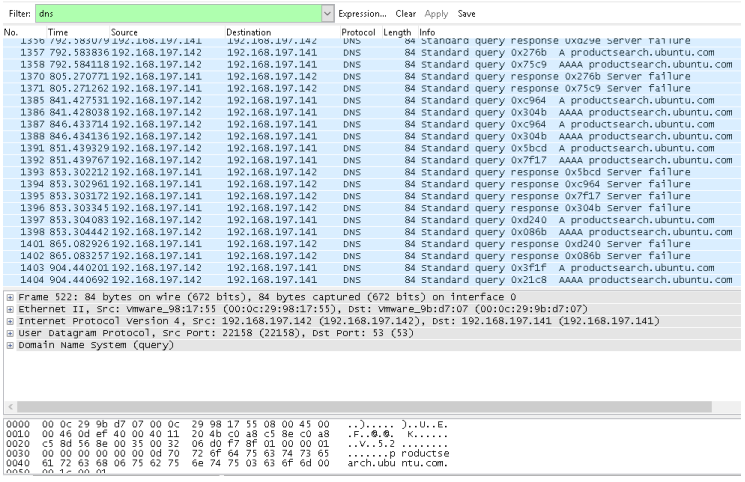
Figura 67 Trafico TLS



Fuente: Propia

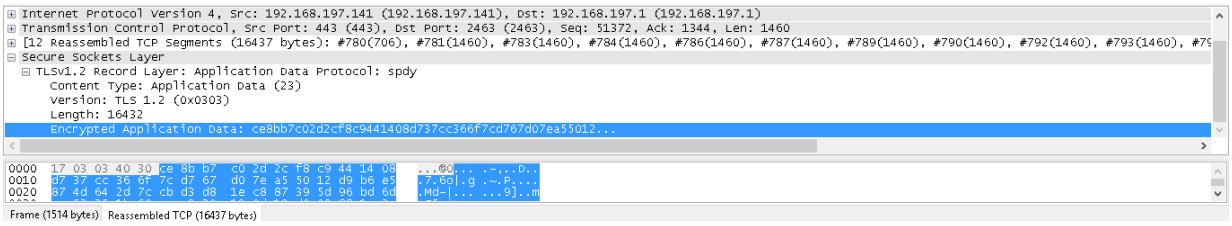
El tráfico de DNS que corresponde a la resolución del nombre que se le dio al servidor Web

Figura 68 Trafico DNS



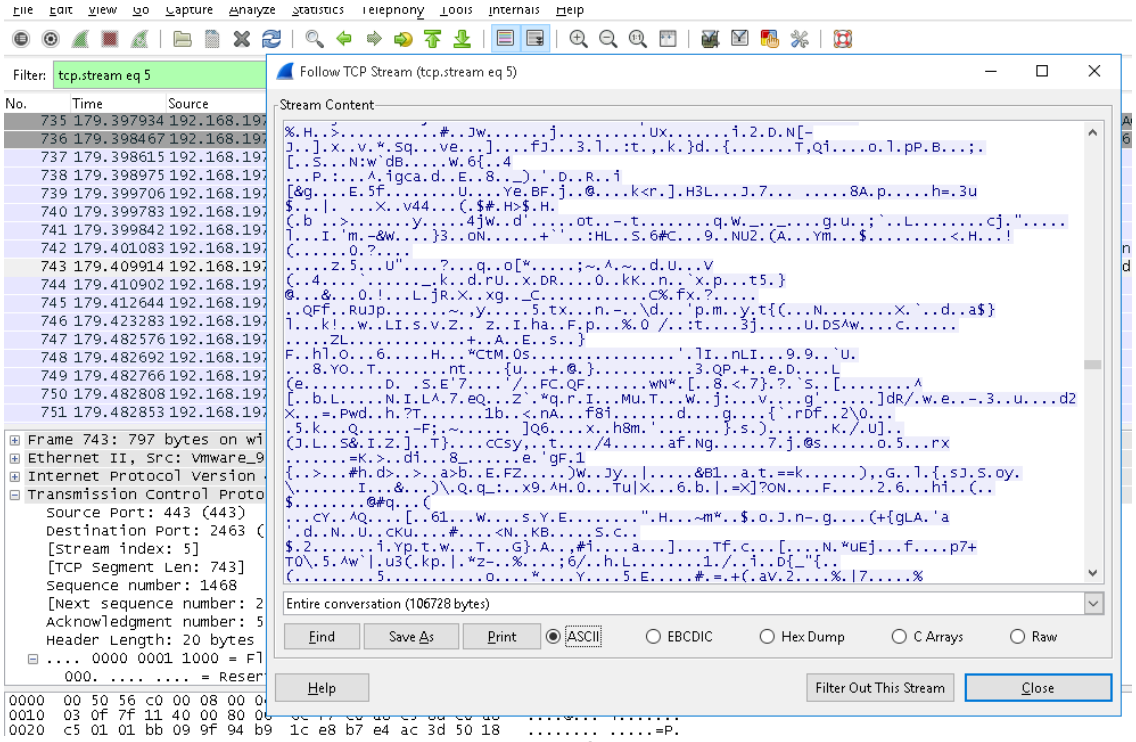
Fuente: Propia

Figura 69 Datos cifrados



Fuente: propia

Figura 70 Datos cifrados



Fuente: propia

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Al objetivo específico 1: Diagnosticar el estado actual de la seguridad de las comunicaciones en la capa de transporte.

Al finalizar la investigación hallamos que los navegadores web más usados tienen compatibilidad con las versiones del protocolo TLS más actuales, dejando de lado las versiones más antiguas. El análisis de los navegadores web arrojo las combinaciones del protocolo TLS que son soportadas, a la vez, se realizó un análisis de un top 100 de páginas más visitadas, de las cuales 53 presentaban seguridad (HTTPS), y se analizó una sin seguridad (HTTP); llegando a la conclusión de que un alto porcentaje de páginas con seguridad utilizan RSA con key 2048 bits para clave pública, y el algoritmo de Hash SHA256 para la integridad de la información. A su vez se vio que sin seguridad al acceder a una página web existe una negociación cliente – servidor, pero esta no garantiza la veracidad de la página, ni la integridad, ni seguridad, ni confidencialidad de los datos, mientras que la negociación cliente – servidor de una página Web segura muestra que verificamos la autenticidad del sitio, se comparte la llave publica con la que podremos cifrar los datos.

Al objetivo específico 2: Analizar los algoritmos de cifrado.

Al término de la investigación se pudo concluir que el algoritmo de Hash SHA256 es usado por su bajo costo computacional, y su alto nivel de seguridad, comparado con otros algoritmos de integridad de datos según la tabla N° 3 su costo computacional se encuentra en el promedio. La clave pública RSA con Key 2048 bits obtuvo buenos números comparado con su par DSA como pudimos ver

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

en la tabla N° 4 y la tabla N°5. En cuanto a la negociación que establecen el usuario y el servidor podemos ver que aumenta el tiempo del procesamiento al tener el protocolo de cifrado implementado.

Al objetivo específico 3: Diseñar un modelo de protocolo de cifrado.

Al término de la investigación se pudo concluir que haciendo un modelo de protocolo de cifrado, usando la infraestructura de PKI como base, nos permite hacer páginas web seguras, siguiendo los lineamientos de RFC 5280 podemos dar una jerarquía de entidad certificadora que permita autenticar múltiples servidores, cifrar o descifrar datos.

Al objetivo específico 4: Implementar algoritmos de cifrado.

Al término de la investigación se pudo realizar la implementación del protocolo de cifrado TLS haciendo uso de una infraestructura de PKI, con lo que podemos concluir que la página Web goza de mayor seguridad, puesto que podemos verificar la comunicación con el servidor, y a su vez cifrar los datos que coloquemos dentro de la página, con la ventaja que podemos recibir múltiples conexiones a nuestro servidor como lo vemos en la tabla N° 4 sin ver afectado el rendimiento de nuestro servidor.

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

6.2 Recomendaciones

En base a las conclusiones generadas, se plantean las siguientes sugerencias:

1. Implementar protocolo de cifrado TLS a sus servidores Web.
2. Conseguir un certificado que contenga las combinaciones más actuales y con compatibilidad en la mayor cantidad de navegadores.
3. Seleccionar una infraestructura de PKI que se adecue a las necesidades y limitaciones hardware/software.
4. Hacer pruebas del protocolo con software libre implementando la infraestructura de PKI.

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

REFERENCIAS:

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

Agulló, D., Guerra, M. C., Silva, F., & Vivanco, R. (2012). Seguridad e integridad de la transferencia de datos. *Conicyt*, 1-13.

Benton, K., & Bross, T. (2013). Timing Analysis of SSL/TLS Man in the Middle Attacks. *Arxiv*, 1-9.

Cabrera Aldaya, A., & Cabrera Sarmiento, A. J. (2013). Diseño e integración de algoritmos criptograficos en sistemas empotrados sobre FPGA. *RIELAC*, 41-51.

Chapaca Garzón, J. E., & Rojas Bustamante, J. D. (2013). *Análisis, diseño y desarrollo de un prototipo de protocolo de transporte basado en comunicación TCP con capacidad de cubrir las necesidades de transferencia de datos seguros, confiables y de alta disponibildad.* Quito: Universidad politécnica Salesiana.

Company, A. (2015). *Alexa - Actionable Analytics for the Web*. Obtenido de http://www.alexa.com/: http://www.alexa.com/topsites

Data, R. (021 de Octubre de 2015). *W3Schools*. Obtenido de http://www.w3schools.com/

Forné, J., Melús, J. L., & Soriano, M. (2011). Criptografia y seguridad en comunicaciones. *Fecyt*, 15-25.

Francisco Diaz, J., & Venosa, P. (2013). Puntos clave para el desarrollo de una aplicación segura usando firma digital. *LINTI*, 1-10.

Gallegos García, G. (2011). *Diseño de protocolos criptográficos para votación electrónica.* Mexico D.F.: Instituto politecnico nacional.

Gil, P. C. (2002). *Introducción a la Criptografía.* AlfaOmega Ra-Ma.

Haro Montero, M. A., & Gavilanes Sagñay, F. M. (2010). *Análisis de funciones criptográficas de código libre en los protocolos ssl y tls aplicado al portal web de la jefatura provincial de tránsito de Chimborazo.* Riobamba: Escuela Superior Politécnico de chimborazo.

Hermida Mondelo, A., & Iglesias Fernández, I. (2014). *Sistemas de archivos y clasificacion de documentos.* España: Ideaspropias.

Hernández Ortiz , R., Peña Blanco, N., Ramirez Amaya, C. M., Rodriguez Baños, V. F., & Acosta Gil , J. (2010). *Implementación de un túnel con cifrado para transporte de datos.* Mexico D.F: Instituto politecnico nacional.

Hernandez, L. (2000). *Tecnicas criptrograficas de proteccion de datos.* AlfaOmega Ra-Ma .

Hernández, L. E., Carreto, C., & Menchaca, R. (2012). Modelo de seguridad para redes aplicado a dispositivos moviles. *Risce*, 17-25.

Jiménez Bazán, M. J. (2000). *Implementación de un sistema cliente/servidor para transmisión encriptado de voz y datos sobre una red local utilizando DSP'S.* Lima: Universidad Nacional de Ingenieria.

Lin Rivest, R., Shamir, A., & Adleman, L. (2013). A Method for obtaining digital signatures and Public-Key Cryptosystems. *ACM*, 14-67.

Martinez Garcia, P. F. (2011). *Estudio del algoritmo de encriptamiento RSA y TRIPLE DES para mensajes financieros basados en un módulo de seguridad de*

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

hardware utilizado en las transferencias interbancarias. Lima: Universidad Nacional de Ingenieria.

Metodología del desarrollo con CISCO. (2014). Obtenido de http://metodologiaspararedes.blogspot.com/

Mood, A., & Graybill, F. (1978). *Introduccion a la teoria de la estadistica.* Madrid: Aguilar.

Morales Lara, A. (2010). *Analisis de los algoritmos de cifrado de llave secreta y su uso dentro de una organizacion pública.* Ciudad de México: Instituto politecnico Nacional.

Morin, E. (1990). Introduccion al pensamiento complejo. *ESF*, 100-150.

Movement, T. I. (03 de Septiembre de 2015). *Trustworthy Internet Movement*. Obtenido de Trustworthy Internet Movement: https://www.trustworthyinternet.org/ssl-pulse/

Ordeñez Calero, H. D. (2013). *Desarrollo del modulo de gestión de información técnica para TELALCA S.A. e implementación de seguridad mediante cifrado SSL del protocolo HTTPS.* Quito: Escuela Politénica Nacinal.

Padron Godínez, A., Prieto Meléndez, R., Herrera Becerra, A., & Calva Olmos, G. (2014). Implementación de protocolos de comunicación seguros. *SOMI*, 89-126.

Perales Paz, C. A., & Villajuan Guzmán, F. M. (2003). *Transmisión de datos vía TCP/IP en tiempo real.* Lima: Universidad Nacional de Ingenieria.

Philco Iphilcoa, O., & Rosero Irosero, L. (2014). Los riesgos en transacciones electronicas en linea y la criptografia como modelo de seguridad informatica. *Gaceta Sansana*, 45-54.

Pousa, A. (2011). Análisis de rendimiento de un algoritmo de criptografía. *Instituto de Investigacion en Informatica LIDI*, 10.

Rescorla, E. (2001). *SSL and TLS : Designing and Buillding.* Addison-Wesley.

Salgado, L., Ron, M., & Solis, F. (2010). Analisis de riesgos de las aplicaciones web de la superintendencia de bancos y seguros, utilizando las recomendaciones TOP TEN de owasp. *Flacso*, 2-25.

Shannon , C. (1948). A Mathematical theory of communications. *Bell System Technical Journal*, 656-715.

Shazia Riaz, Shafia, Asma Sajid, & Madiha Kanwal. (2014). Performance analysis of SSL/TLS IJISET. *IJISET*, 2348-7968.

Silva Pérez, J., & Morales Luna, G. (2012). Desarrollo de una plataforma de seguridad en dispositivos moviles de comunicacion, ¿necesidad o paranoia? *UNAM*, 1-16.

Stallings, W. (2008). *Fundamentos de seguridad en redes.* Madrid: Pearson.

Stats, I. L. (15 de Junio de 2015). *http://www.internetlivestats.com/*. Obtenido de http://www.internetlivestats.com

System, C. (2014). *CCNA 5.02.* EE.UU: Pearson Education.

Villegas Gómez, R. (2010). *Comparativa de seguridad de algoritmos de cifrado asimetrico.* Mexico D.F.: Instituto politécnico Nacional.

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

ANEXOS

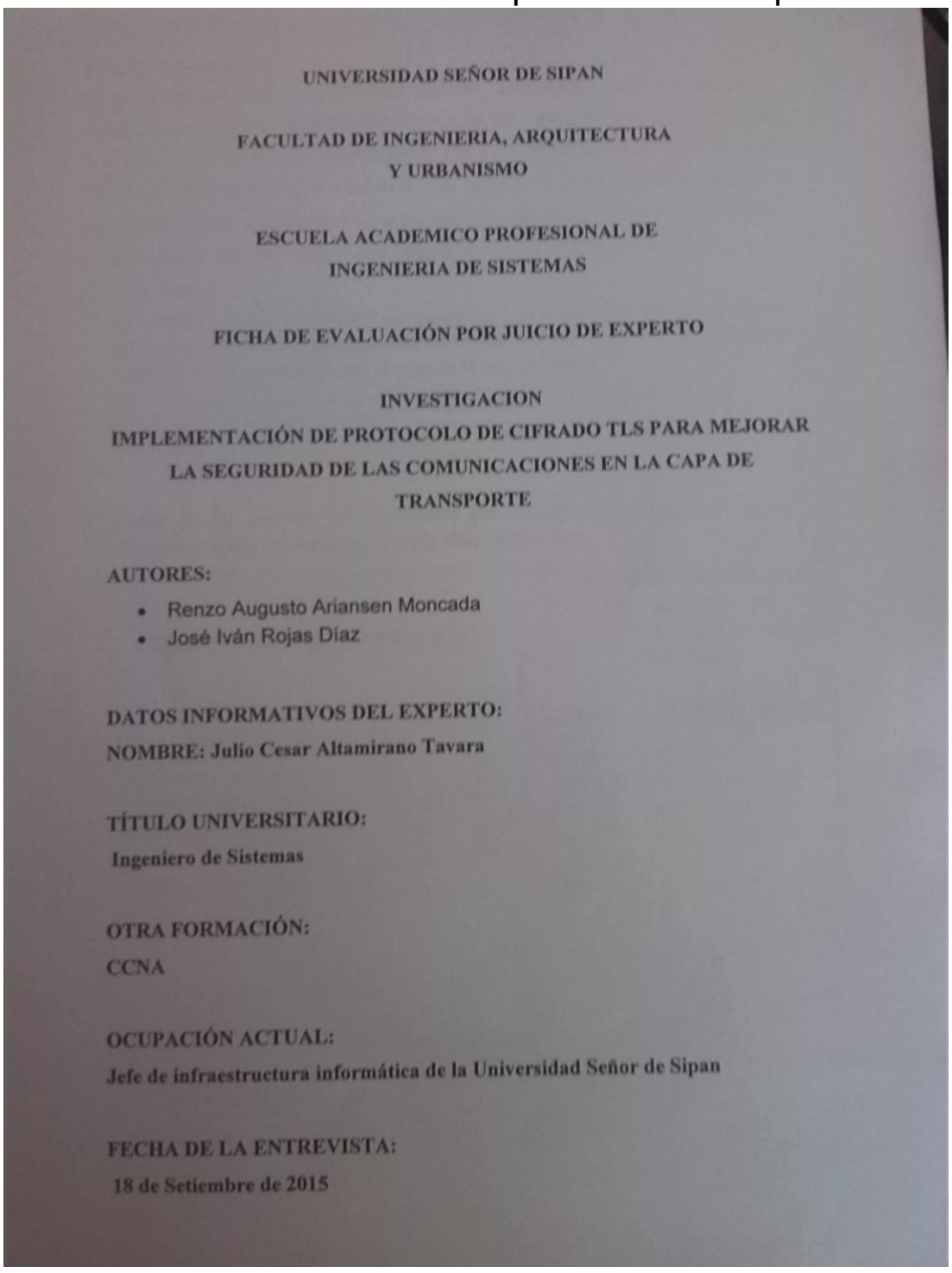
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Anexo 01 Ficha técnica

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

Protocolo TCP/IP	Dominio	Puerto	Algoritmo de firma	Algoritmo Hash de firma	Clave pública	Tamaño clave publica (bits)	Algoritmo de identificación	Handshake (bytes)	Versión	Tipo de Certificado	Tiempo SSL handshake (ms)	Tiempo tcp handshake(ms)	Combinación
http	trademap.org	80	No implementado	No implementado	No implementado	No implementado	No implementado	No implementado	No implementado	No implementado	No implementado	508	No implementado
https	google.com	443	sha256RSA	sha256	RSA	2048	sha1	4109	SSLv3, TLSv1, TLSv1.2	Multi-Domain	871	451	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	facebook.com	443	sha1RSA	sha1	ECC	256	sha1	3741	SSLv3, TLSv1, TLSv1.2	Wildcard	437	223	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
https	youtube.com	443	sha256RSA	sha256	ECC	256	sha1	4890	SSLv3, TLSv1, TLSv1.2	Multi-Domain	425	176	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
https	yahoo.com	443	sha256RSA	sha256	RSA	2048	sha1	5913	SSLv3, TLSv1, TLSv1.2	Wildcard	946	386	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	amazon.com	443	sha1RSA	sha1	RSA	2048	sha1	4976	SSLv3, TLSv1, TLSv1.2	Wildcard	685	250	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	wikipedia.org	443	sha256RSA	sha256	ECC	256	sha1	3615	SSLv3, TLSv1, TLSv1.2	Multi-Domain	669	387	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
https	baidu.com	443	sha1RSA	sha1	RSA	2048	sha1	5168	SSLv3, TLSv1, TLSv1.2	Single-Domain	1266	563	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	qq.com	443	sha256RSA	sha256	RSA	2048	sha1	4841	SSLv3, TLSv1, TLSv1.2	Wildcard	411	298	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	taobao.com	443	sha256RSA	sha256	RSA	2048	sha1	3730	SSLv3, TLSv1, TLSv1.2	Multi-Domain	3557	932	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	live.com	443	sha1RSA	sha1	RSA	2048	sha1	5495	SSLv3, TLSv1, TLSv1.2	Multi-Domain	1186	475	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	linkedin.com	443	sha256RSA	sha256	RSA	2048	sha1	3360	SSLv3, TLSv1, TLSv1.2	Single-Domain	1783	914	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	yandex.com	443	sha1RSA	sha1	RSA	2048	sha1	3788	SSLv3, TLSv1, TLSv1.2	Wildcard	2907	1931	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	hao123.com	443	sha256RSA	sha256	RSA	2048	sha1	5007	SSLv3, TLSv1, TLSv1.2	Multi-Domain	3674	2387	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	vk.com	443	sha256RSA	sha256	RSA	2048	sha1	5749	SSLv3, TLSv1, TLSv1.2	Single-Domain	1535	700	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	bing.com	443	sha256RSA	sha256	RSA	2048	sha1	4567	SSLv3, TLSv1, TLSv1.2	Multi-Domain	1140	512	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	twitter.com	443	sha256RSA	sha256	RSA	2048	sha1	3759	SSLv3, TLSv1, TLSv1.2	Single-Domain	651	258	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	instagram.com	443	sha1RSA	sha1	RSA	2048	sha1	3904	SSLv3, TLSv1, TLSv1.2	Wildcard	474	192	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	msn.com	443	sha256RSA	sha256	RSA	2048	sha1	4001	SSLv3, TLSv1, TLSv1.2	Wildcard	683	295	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	aliexpress.com	443	sha256RSA	sha256	RSA	2048	sha1	4841	SSLv3, TLSv1, TLSv1.2	Single-Domain	1816	746	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	pinterest.com	443	sha256RSA	sha256	RSA	2048	sha1	3581	SSLv3, TLSv1, TLSv1.2	Single-Domain	556	324	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	ask.com	443	sha256RSA	sha256	RSA	2048	sha1	4841	SSLv3, TLSv1, TLSv1.2	Single-Domain	2170	1650	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	blogspot.com	443	sha256RSA	sha256	ECC	256	sha1	4150	SSLv3, TLSv1, TLSv1.2	Multi-Domain	422	175	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	apple.com	443	sha256RSA	sha256	RSA	2048	sha1	4050	SSLv3, TLSv1, TLSv1.2	Wildcard	251	116	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	tmall.com	443	sha256RSA	sha256	RSA	2048	sha1	3730	SSLv3, TLSv1, TLSv1.2	Multi-Domain	3587	2700	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	wordpress.com	443	sha256RSA	sha256	RSA	2048	sha1	5305	SSLv3, TLSv1, TLSv1.2	Single-Domain	2321	1903	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	reddit.com	443	sha256RSA	sha256	RSA	2048	sha1	3504	SSLv3, TLSv1, TLSv1.2	Single-Domain	832	590	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	paypal.com	443	sha256RSA	sha256	RSA	2048	sha1	4207	SSLv3, TLSv1, TLSv1.2	Wildcard	725	385	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	mail.ru	443	sha256RSA	sha256	RSA	2048	sha1	3388	SSLv3, TLSv1, TLSv1.2	Single-Domain	2806	1846	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	tumblr.com	443	sha256RSA	sha256	RSA	2048	sha1	3312	SSLv3, TLSv1, TLSv1.2	Wildcard	953	381	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	sohu.com	443	sha1RSA	sha1	RSA	2048	sha1	5783	SSLv3, TLSv1, TLSv1.2	Single-Domain	2078	885	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	microsoft.com	443	sha256RSA	sha256	RSA	2048	sha1	5005	SSLv3, TLSv1, TLSv1.2	Single-Domain	254	117	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	imgur.com	443	sha256RSA	sha256	RSA	2048	sha1	4011	SSLv3, TLSv1, TLSv1.2	Wildcard	1411	806	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	imdb.com	443	sha256RSA	sha256	RSA	2048	sha1	3236	SSLv3, TLSv1, TLSv1.2	Single-Domain	689	415	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	netflix.com	443	sha256RSA	sha256	RSA	2048	sha1	3734	SSLv3, TLSv1, TLSv1.2	Wildcard	679	384	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	craigslist.org	443	sha1RSA	sha1	RSA	2048	sha1	7678	SSLv3, TLSv1, TLSv1.2	Single-Domain	3156	1926	TLS_RSA_WITH_AES_128_CBC_SHA
https	outbrain.com	443	sha256RSA	sha256	RSA	2048	sha1	4609	SSLv3, TLSv1, TLSv1.2	Single-Domain	2290	876	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	kat.cr	443	sha256RSA	sha256	RSA	2048	sha1	6257	SSLv3, TLSv1, TLSv1.2	Wildcard	1253	539	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	diply.com	443	sha256RSA	sha256	RSA	2048	sha1	3449	SSLv3, TLSv1, TLSv1.2	Wildcard	1380	862	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	dropbox.com	443	sha256RSA	sha256	RSA	2048	sha1	2821	SSLv3, TLSv1, TLSv1.2	Wildcard	950	305	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	github.com	443	sha256RSA	sha256	RSA	2048	sha1	3274	SSLv3, TLSv1, TLSv1.2	Single-Domain	766	294	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	adcash.com	443	sha1RSA	sha1	RSA	2048	sha1	4234	SSLv3, TLSv1, TLSv1.2	Wildcard	716	271	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	popads.net	443	sha256RSA	sha256	RSA	2048	sha1	5317	SSLv3, TLSv1, TLSv1.2	Wildcard	2476	1746	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	dailymotion.com	443	sha256RSA	sha256	RSA	2048	sha1	3260	SSLv3, TLSv1, TLSv1.2	Wildcard	1022	312	TLS_RSA_WITH_AES_128_CBC_SHA
https	pixnet.net	443	sha256RSA	sha256	RSA	2048	sha1	3126	SSLv3, TLSv1, TLSv1.2	Wildcard	4039	2348	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	sogou.com	443	sha256RSA	sha256	RSA	2048	sha1	4386	SSLv3, TLSv1, TLSv1.2	Wildcard	3332	1901	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	bongaca.com	443	sha256RSA	sha256	RSA	2048	sha1	5433	SSLv3, TLSv1, TLSv1.2	Wildcard	734	380	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	booking.com	443	sha256RSA	sha256	RSA	2048	sha1	3194	SSLv3, TLSv1, TLSv1.2	Wildcard	754	267	TLS_RSA_WITH_AES_128_CBC_SHA
https	adnetworkperformance.com	443	sha256RSA	sha256	RSA	2048	sha1	3329	SSLv3, TLSv1, TLSv1.2	Single-Domain	513	206	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	jd.com	443	sha256RSA	sha256	RSA	2048	sha1	3614	SSLv3, TLSv1, TLSv1.2	Multi-Domain	3124	2608	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
https	adobe.com	443	sha256RSA	sha256	RSA	2048	sha1	4742	SSLv3, TLSv1, TLSv1.2	Single-Domain	966	425	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
https	indiatimes.com	443	sha256RSA	sha256	RSA	2048	sha1	4841	SSLv3, TLSv1, TLSv1.2	Multi-Domain	419	298	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Anexo 02 Ficha de Evaluación por Juicio de Expertos



UNIVERSIDAD SEÑOR DE SIPAN

FACULTAD DE INGENIERIA, ARQUITECTURA
Y URBANISMO

ESCUELA ACADEMICO PROFESIONAL DE
INGENIERIA DE SISTEMAS

FICHA DE EVALUACIÓN POR JUICIO DE EXPERTO

INVESTIGACION
IMPLEMENTACIÓN DE PROTOCOLO DE CIFRADO TLS PARA MEJORAR LA SEGURIDAD DE LAS COMUNICACIONES EN LA CAPA DE TRANSPORTE

AUTORES:

- Renzo Augusto Ariansen Moncada
- José Iván Rojas Díaz

DATOS INFORMATIVOS DEL EXPERTO:

NOMBRE: Julio Cesar Altamirano Tavara

TÍTULO UNIVERSITARIO:

Ingeniero de Sistemas

OTRA FORMACIÓN:

CCNA

OCUPACIÓN ACTUAL:

Jefe de infraestructura informática de la Universidad Señor de Sipan

FECHA DE LA ENTREVISTA:

18 de Setiembre de 2015

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

Mensaje al especialista:

En la Universidad Señor de Sipán, km.5 Carretera a Pimentel, se está realizando una investigación dirigida a la IMPLEMENTACIÓN DE PROTOCOLO DE CIFRADO TLS PARA MEJORAR LA SEGURIDAD DE LAS COMUNICACIONES EN LA CAPA DE TRANSPORTE. Por tal motivo, se requiere de su reconocida experiencia, para corroborar que la propuesta de esta investigación genera los resultados establecidos en la hipótesis. Su información será estrictamente confidencial. Se agradece por el tiempo invertido.

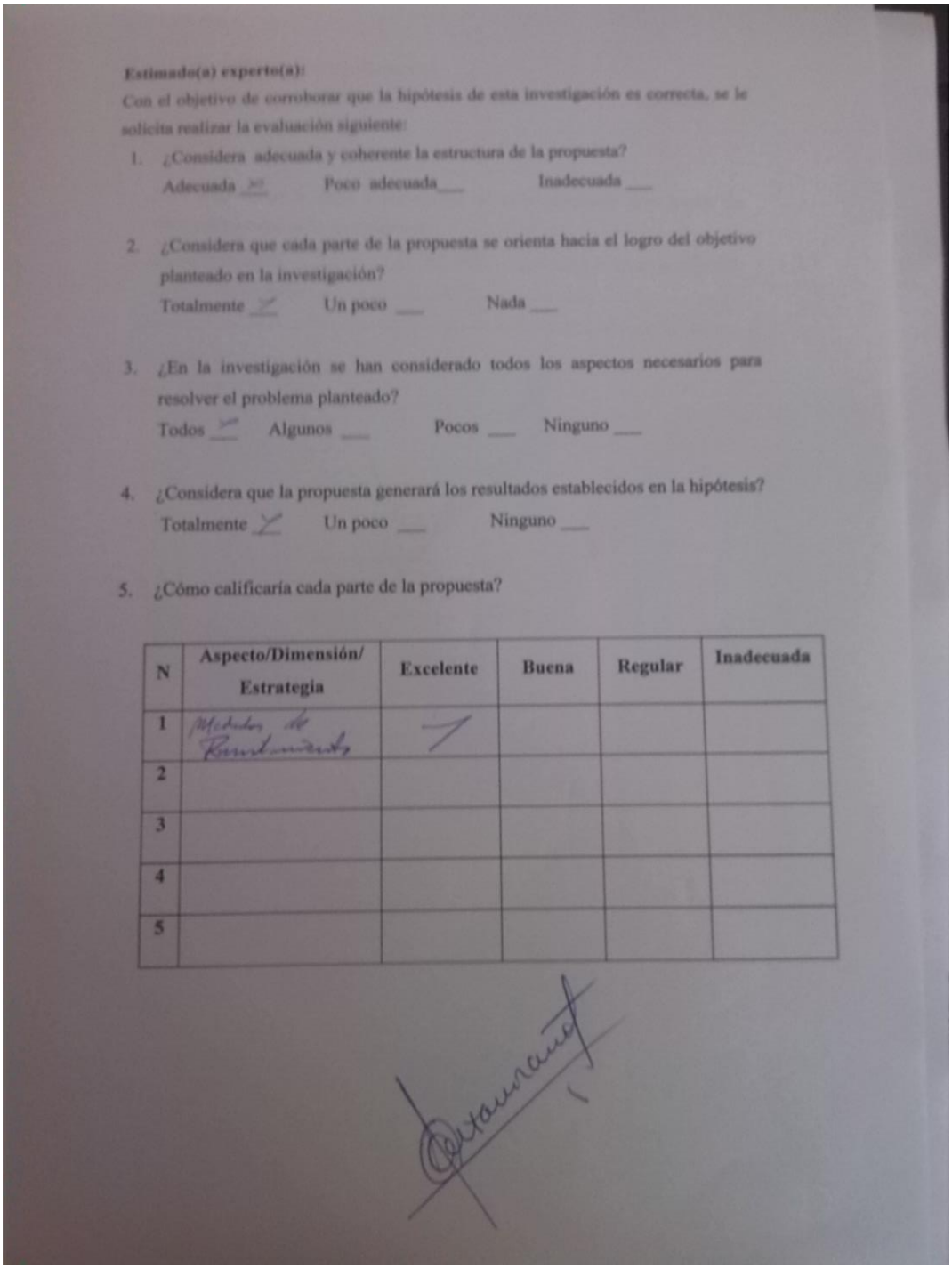
1. En la tabla siguiente, se propone una escala del 1 al 5, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque con una "X" conforme considere su conocimiento sobre el tema de la tesis evaluada.

1	2	3	4	5
Ninguno	Poco	Regular	Alto	Muy alto

2. Sírvase marcar con una "X" las fuentes que considere han influenciado en su conocimiento sobre el tema, en un grado alto, medio o bajo.

FUENTES DE ARGUMENTACIÓN	GRADO DE INFLUENCIA DE CADA UNA DE LAS FUENTES EN SUS CRITERIOS		
	A (ALTO)	M (MEDIO)	B (BAJO)
a) Análisis teóricos realizados. (AT)	X		
b) Experiencia como profesional. (EP)	X		
c) Trabajos estudiados de autores nacionales. (AN)	X		
d) Trabajos estudiados de autores extranjeros. (AE)	X		
e) Conocimientos personales sobre el estado del problema de investigación. (CP)	X		

Firma del entrevistado



Estimado(a) experto(a):

Con el objetivo de corroborar que la hipótesis de esta investigación es correcta, se le solicita realizar la evaluación siguiente:

1. ¿Considera adecuada y coherente la estructura de la propuesta?
   Adecuada ✓ Poco adecuada___ Inadecuada ___

2. ¿Considera que cada parte de la propuesta se orienta hacia el logro del objetivo planteado en la investigación?
   Totalmente ✓ Un poco ___ Nada ___

3. ¿En la investigación se han considerado todos los aspectos necesarios para resolver el problema planteado?
   Todos ✓ Algunos ___ Pocos ___ Ninguno ___

4. ¿Considera que la propuesta generará los resultados establecidos en la hipótesis?
   Totalmente ✓ Un poco ___ Ninguno ___

5. ¿Cómo calificaría cada parte de la propuesta?

N	Aspecto/Dimensión/ Estrategia	Excelente	Buena	Regular	Inadecuada
1	Medidas de Reforzamiento	✓			
2					
3					
4					
5					

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

6. ¿Cómo calificaría a toda la propuesta?

Excelente ___ Buena ___ Regular ___ Inadecuada ___

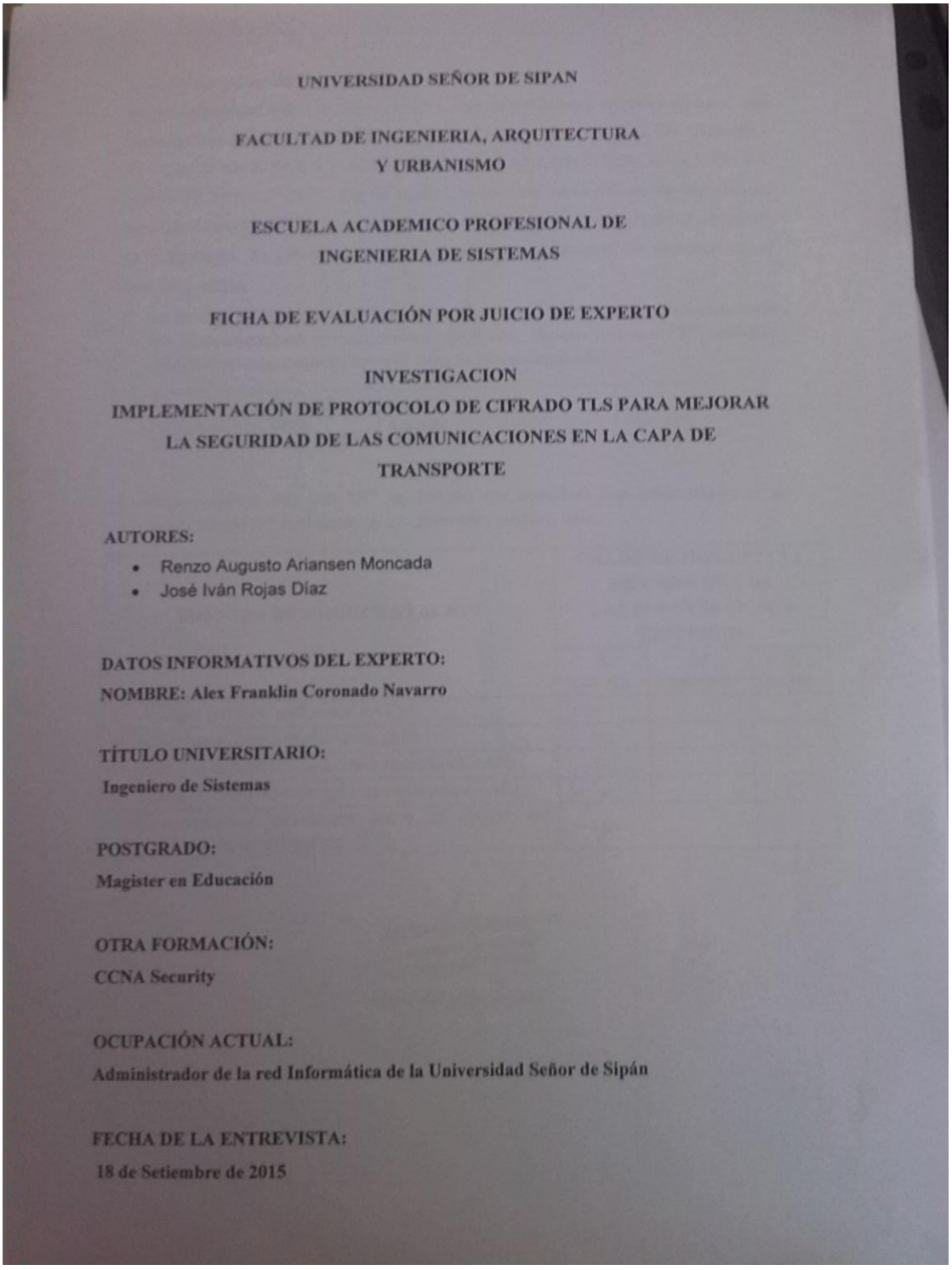
7. ¿Qué sugerencias le haría a los autores de la investigación para lograr los objetivos trazados en la investigación?

Trabajar más pruebas con monitoreo continuo

Firma del entrevistado

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

Anexo 03 Ficha de Evaluación por Juicio de Expertos



UNIVERSIDAD SEÑOR DE SIPAN

FACULTAD DE INGENIERIA, ARQUITECTURA
Y URBANISMO

ESCUELA ACADEMICO PROFESIONAL DE
INGENIERIA DE SISTEMAS

FICHA DE EVALUACIÓN POR JUICIO DE EXPERTO

INVESTIGACION
IMPLEMENTACIÓN DE PROTOCOLO DE CIFRADO TLS PARA MEJORAR LA SEGURIDAD DE LAS COMUNICACIONES EN LA CAPA DE TRANSPORTE

AUTORES:

- Renzo Augusto Ariansen Moncada
- José Iván Rojas Díaz

DATOS INFORMATIVOS DEL EXPERTO:

NOMBRE: Alex Franklin Coronado Navarro

TÍTULO UNIVERSITARIO:

Ingeniero de Sistemas

POSTGRADO:

Magister en Educación

OTRA FORMACIÓN:

CCNA Security

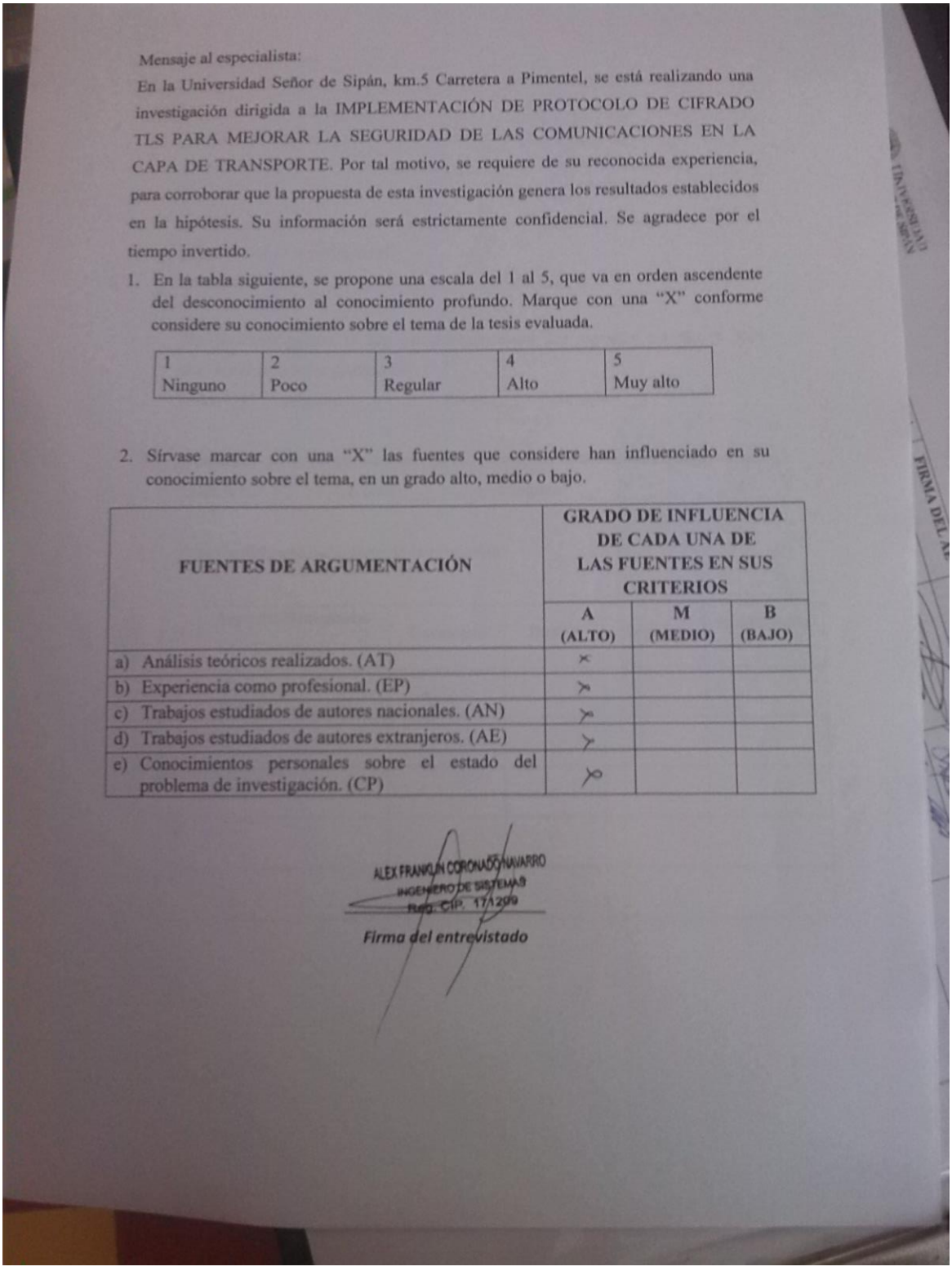
OCUPACIÓN ACTUAL:

Administrador de la red Informática de la Universidad Señor de Sipán

FECHA DE LA ENTREVISTA:

18 de Setiembre de 2015

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



Mensaje al especialista:

En la Universidad Señor de Sipán, km.5 Carretera a Pimentel, se está realizando una investigación dirigida a la IMPLEMENTACIÓN DE PROTOCOLO DE CIFRADO TLS PARA MEJORAR LA SEGURIDAD DE LAS COMUNICACIONES EN LA CAPA DE TRANSPORTE. Por tal motivo, se requiere de su reconocida experiencia, para corroborar que la propuesta de esta investigación genera los resultados establecidos en la hipótesis. Su información será estrictamente confidencial. Se agradece por el tiempo invertido.

1. En la tabla siguiente, se propone una escala del 1 al 5, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque con una "X" conforme considere su conocimiento sobre el tema de la tesis evaluada.

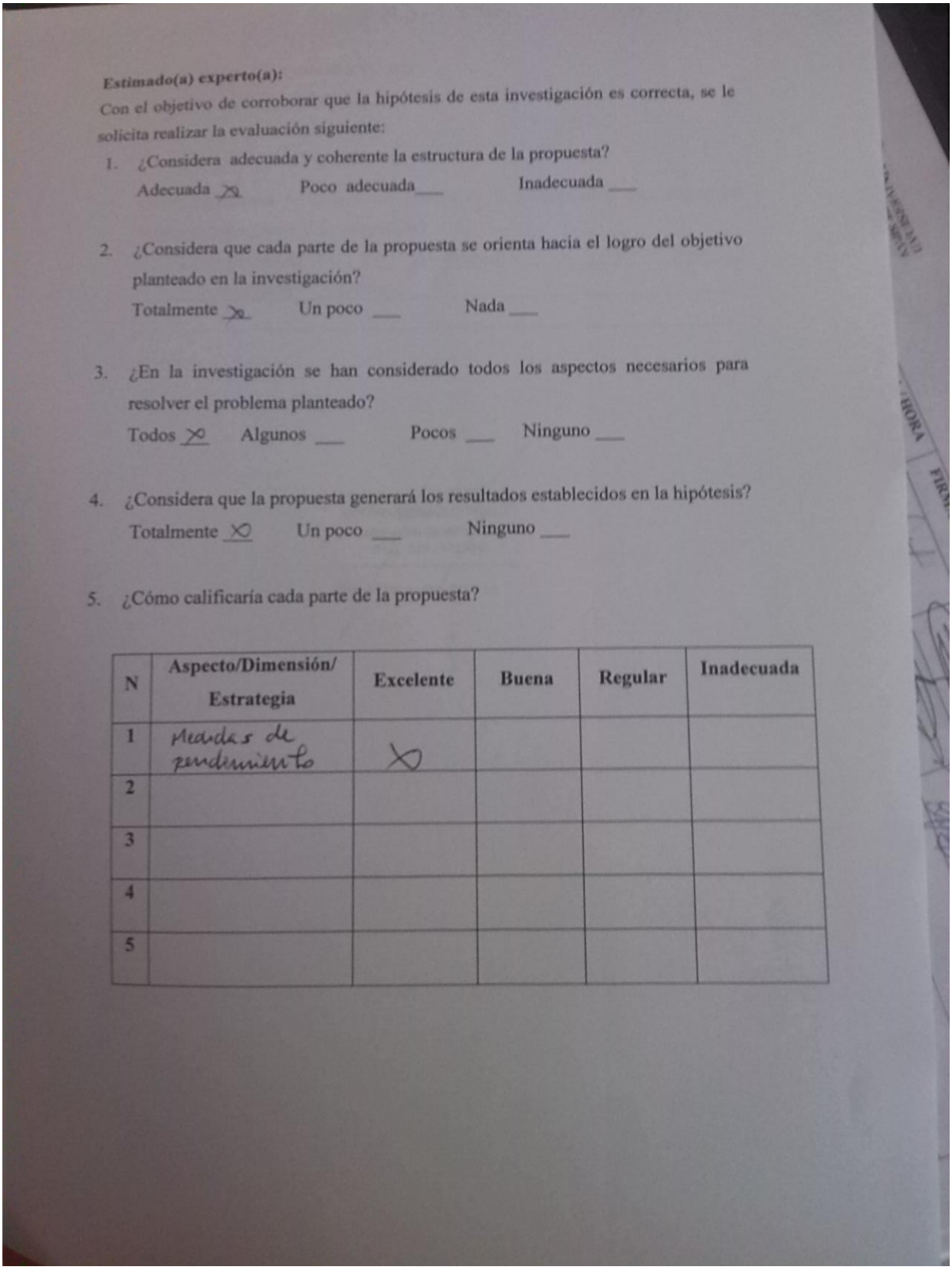
1 Ninguno	2 Poco	3 Regular	4 Alto	5 Muy alto

2. Sírvase marcar con una "X" las fuentes que considere han influenciado en su conocimiento sobre el tema, en un grado alto, medio o bajo.

FUENTES DE ARGUMENTACIÓN	GRADO DE INFLUENCIA DE CADA UNA DE LAS FUENTES EN SUS CRITERIOS		
	A (ALTO)	M (MEDIO)	B (BAJO)
a) Análisis teóricos realizados. (AT)	X		
b) Experiencia como profesional. (EP)	X		
c) Trabajos estudiados de autores nacionales. (AN)	X		
d) Trabajos estudiados de autores extranjeros. (AE)	X		
e) Conocimientos personales sobre el estado del problema de investigación. (CP)	X		

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Firma del entrevistado



Estimado(a) experto(a):

Con el objetivo de corroborar que la hipótesis de esta investigación es correcta, se le solicita realizar la evaluación siguiente:

1. ¿Considera adecuada y coherente la estructura de la propuesta?
   Adecuada X Poco adecuada___ Inadecuada ___

2. ¿Considera que cada parte de la propuesta se orienta hacia el logro del objetivo planteado en la investigación?
   Totalmente X Un poco ___ Nada ___

3. ¿En la investigación se han considerado todos los aspectos necesarios para resolver el problema planteado?
   Todos X Algunos ___ Pocos ___ Ninguno ___

4. ¿Considera que la propuesta generará los resultados establecidos en la hipótesis?
   Totalmente X Un poco ___ Ninguno ___

5. ¿Cómo calificaría cada parte de la propuesta?

N	Aspecto/Dimensión/ Estrategia	Excelente	Buena	Regular	Inadecuada
1	Medidas de rendimiento	X			
2					
3					
4					
5					

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

6. ¿Cómo calificaría a toda la propuesta?

Excelente X Buena ___ Regular ___ Inadecuada ___

7. ¿Qué sugerencias le haría a los autores de la investigación para lograr los objetivos trazados en la investigación?

Implementar la propuesta y llevar un mantenimiento continuo.

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Firma del entrevistado

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