PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

"ANÁLISIS DE LOS MECANISMOS DE ENCRIPTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN EN REDES DE COMUNICACIONES"

PAOLA MARITZA VELASCO SÁNCHEZ

Quito – Abril, 2015

Contenido

1. Introducción

Las tecnologías de la información y las comunicaciones (TIC) son cada vez más utilizadas en todos los ámbitos de la sociedad –educación, salud, comercio, investigación,..– . Según la Unión Internacional de Telecomunicaciones (UIT), más de 3000 millones de personas están en línea y las TIC crecen progresivamente en casi todos los países del mundo [1]. Sin embargo, este incremento trae como consecuencia el inconveniente de controlar la interacción entre usuarios a través de Internet, ya que al ser una red de comunicación no regulada, se constituye en un medio apto para actividades ilegales, poniendo en riesgo la seguridad en la transmisión de la información. [2]

La información que circula por la red está expuesta a varias formas de ataques informáticos – suplantación de identidad, falsificación y alteración de documentos, hurto o destrucción de información, virus,..–, siendo necesario considerar mayor seguridad en el diseño, configuración y operación de los sistemas. Por lo que el análisis de la seguridad informática permitirá que toda información almacenada sea confiable y no pueda ser manipulada por personas no autorizadas. [3]

El presente trabajo, contempla el estudio de los mecanismos de encriptación en redes de comunicaciones. Dicho estudio examina y analiza los trabajos relacionados con el tema de seguridad informática, criptografía, normas y estándares internacionales, para recomendar, de acuerdo a las características y requerimientos, el mecanismo idóneo a ser aplicado en una red de telemedicina.

2. Justificación

En la actualidad la información de una empresa o institución ya no se encuentra únicamente en el computador personal del administrador o de los trabajadores de la organización, con el avance tecnológico y el uso de los medios de comunicación masiva, esta información tiende a viajar a través de la red [4], en consecuencia el derecho a la privacidad se ha visto vulnerado. En este contexto, es importante analizar la seguridad informática, la misma que se basa en mecanismos para proteger datos, aplicaciones, tiempo de procesamiento, ancho de banda, sistemas operativos; y, así garantizar el nivel de confidencialidad e integridad en la transmisión de la información [5].

En las redes de comunicaciones, la información está expuesta a un sinnúmero de eventos que pueden ser provocados por quienes buscan apropiarse y conocer la información que se transmite. Según Gutiérrez, Jaime (2003) "La seguridad de la información es la que va a permitir que muchas empresas u organizaciones sigan existiendo" [6], por ello es necesario considerar diferentes mecanismos para proteger la información que circula a través de la red. No obstante, Cano, Jeimy (2004) manifiesta "no es posible evitar la inseguridad informática pues es una propiedad inherente a los objetos" [7], por lo que cada vez se hace más importante el análisis de nuevas formas de implementar seguridad a los sistemas informáticos, así como procurar que las ya existentes estén acorde a los nuevos retos tecnológicos.

Por lo que la realización del presente estudio es importante debido a que el manejo de la información es confidencial y compromete la integridad de una persona, organización, institución e incluso gobiernos, quienes en los últimos años se han visto afectados por divulgación de cierta información considerada "secreta". Siendo fundamental analizar y establecer los parámetros de seguridad al momento de implementar una red de comunicaciones.

3. Antecedentes

La seguridad informática, analiza a la criptografía como la ciencia en la cual se fundamentan los protocolos y métodos de seguridad que buscan garantizar la confidencialidad e integridad de los datos que circulan por una red de comunicaciones, y el Internet es el medio que ha permitido esta interconectividad [5]. En el último año se ha incrementado el número de usuarios de Internet a nivel mundial (6,6% siendo el 3,3% los países desarrollados y 8,7% los países en desarrollo) [1], Hamadoun I. Touré, (2014) manifiesta que las TIC son un potencial relevante pues contribuyen en el desarrollo y mejora del entorno social, tanto para los más pobres y privados de derechos –mujeres– como para los jóvenes y personas con discapacidad [1].

Para cumplir con este propósito se han desarrollado diferentes proyectos en los cuales se hace de las TIC el medio para aprovechar todos los recursos tecnológicos que existen en la actualidad –comunicaciones inalámbricas, dispositivos móviles,..–[8]. Al mismo tiempo se han ido incrementando los ataques hacia diferentes medios en busca de vulnerar su seguridad y hacer uso de la información que se está transmitiendo [9]. No obstante, la encriptación sigue siendo el mecanismo utilizado para proteger los datos que transitan a través de la red.

El principio de la teoría de la información de Claude Shannon, permitió que a mediados de los años 70 se presente el primer algoritmo criptográfico, el mismo que debido a su estructura es parte de la criptografía simétrica. A partir de éste se han desarrollado un sinnúmero de algoritmos, los mismos que van buscando mejorar el tipo de seguridad del anterior. Fue así que *Whitfiel Diffie* y *Martin Hellman*, desarrollaron un método diferente para la encriptación de los datos, y es conocido como criptografía asimétrica o de clave pública [10].

4. Objetivos

4.1 Objetivo General:

Analizar los mecanismos de encriptación para la seguridad de la información en una red de comunicaciones.

4.2 Objetivos Específicos:

1. Establecer los riesgos de seguridad en el intercambio de información en redes de comunicaciones.
2. Identificar los mecanismos de encriptación utilizados en seguridad de información.
3. Establecer las fortalezas y debilidades de los mecanismos de encriptación.
4. Definir el mecanismo de encriptación idóneo para aplicarlo en la seguridad de una red de telemedicina.
5. Realizar un artículo referente al análisis de los mecanismos de encriptación.

5. Análisis de los Mecanismos de Encriptación para la Seguridad de la Información en Redes de Comunicaciones

5.1 Seguridad en la transmisión de información en redes de comunicaciones

A medida que se expanden las redes de comunicación, la inseguridad en los sistemas informáticos también aumenta. El término seguridad –que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente– [11], se ha convertido en una necesidad para todos quienes son parte del mundo de las comunicaciones; en cualquiera de los ámbitos en los que se desarrolle una aplicación, la prioridad siempre será mantener segura la información que se transmite [12]. Para ello se establece una diferencia entre seguridad de la información y seguridad informática.

- **Seguridad de la información:** Conjunto de reglas y procedimientos para asegurar la confidencialidad, integridad y disponibilidad de la información.[5]
- **Seguridad informática:** Conjunto de políticas y mecanismos que permitan proteger los recursos de un sistema (memoria, tiempo de procesamiento, ancho de banda, información en el sistema,..). Esta a su vez considera a la seguridad según la función que va a realizar, así: [5]
  - *En función de lo que se quiere proteger*: seguridad física – protección ante causas físicas y desastres naturales (incendios, inundaciones, robos,..)– y seguridad lógica – protección al sistema lógico (datos, aplicaciones,..) –.
  - *En función del momento en que tiene lugar la protección*: seguridad activa – medidas preventivas ante incidentes en los sistemas informáticos – y seguridad pasiva – técnicas para minimizar las consecuencias de un incidente de seguridad –.

La Unión internacional de Telecomunicaciones (UIT-T), en el proceso de normalización respecto a seguridad en las comunicaciones, en 1980 elaboró la recomendación *Rec. UIT-T X.800* para arquitectura de sistemas abiertos. A partir de ello, la UIT-T ha venido trabajando conjuntamente con ISO en el desarrollo de nuevas recomendaciones, que permitan abordar los servicios y mecanismos de seguridad en otras arquitecturas. La recomendación *Rec. UIT-T X.805*, complementa las necesidades planteadas en las de la serie X.800 y aporta con nuevos parámetros para garantizar la seguridad en sistemas de comunicación extremo a extremo. Estas dimensiones de seguridad son [13]:

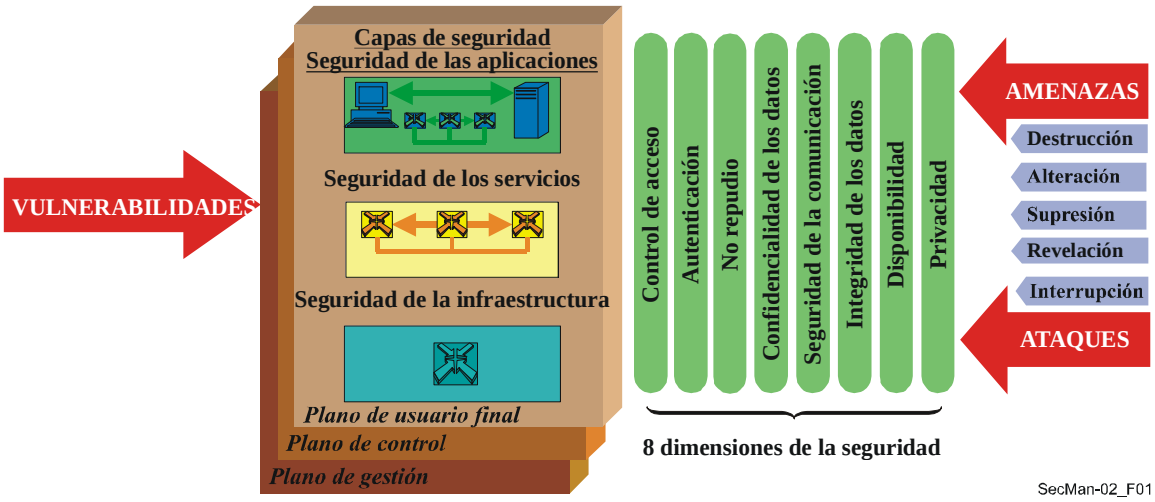


Figura 1: Elementos de la arquitectura de seguridad de la Rec. UIT-T X.805 [13]

1. **Control de acceso.-** Verifica que los recursos sean utilizados por quien tiene autorización para hacerlo. Garantiza que solo las personas y los dispositivos autorizados pueden acceder a los elementos de red –información almacenada, flujos de información, servicios y aplicaciones –

2. **Autenticación.-** Verifica la fuente de los datos – identidad –. Garantiza que ninguna entidad – persona, dispositivo, servicio o aplicación – ha usurpado una identidad o está reproduciendo una comunicación anterior sin autorización.

3. **No repudio.-** Consiste en que una persona o entidad nieguen haber realizado una acción. Utiliza firmas digitales.

4. **Confidencialidad de los datos.-** Garantiza que solo las personas autorizadas tengan acceso a la información. Utiliza métodos como la criptografía, listas de control y permisos de acceso para garantizar la confidencialidad de datos.

5. **Seguridad de la comunicación.-** Garantiza que los flujos de información solo tienen lugar entre puntos extremos autorizados (la información no puede desviarse ni ser interceptada cuando fluye entre estos dos puntos extremos).

6. **Integridad de los datos.-** Garantiza que los datos que son enviados por el transmisor no se alteren hasta su llegada al receptor.

7. **Disponibilidad.-** Garantiza que ningún evento que pueda ocurrir en la red impedirá el acceso autorizado a los elementos, la información almacenada, los flujos de información, los servicios y las aplicaciones de la red.

8. **Privacidad.-** Impide conocer información observando las actividades de la red.

5.1.1 Seguridad en redes inalámbricas

Según Madrid, J. (2004) las redes inalámbricas de área local (WLAN), debido a su potencial acceso han alcanzado estándares de popularidad a nivel mundial. Sin embrago, en cuanto a seguridad se refiere, una gran mayoría son vulnerables y están expuestas a plagio por personas –*hackers*– no autorizadas. De hecho, "cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica" (Madrid, 2004: 15). En efecto, la existencia de puntos de acceso (AP) inalámbrico en la red posee ciertas implicaciones negativas para una determinada empresa o compañía, es decir, una persona –*empleado o transeúnte*– que se encuentre

dentro de ese rango podría conectarse a una red inalámbrica –*empresa*– fácilmente sea de manera intencional o no y obtener información exclusiva, lo que posibilitará navegar gratis en la web, usar la red de la compañía como punto de ataque para otras redes y desconectarse para no ser identificado, introducir virus, entre otros problemas de inseguridad.

Asimismo, una empresa o institución protege adecuadamente el acceso a sus redes con un firewall apropiado, sin embargo, al interior de la red existen puntos de acceso inalámbricos sin seguridades. Por lo tanto, un punto de acceso inalámbrico mal configurado se convierte en un completo potencial vulnerable para la seguridad –*informática*– de una empresa. Así, *Fisher*, D. (2003) en un estudio publicado por *RSA Security* Inc. encontró que de 328 puntos de acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP, por lo que cien de estos puntos de acceso estaban divulgando información que permitía identificar la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica.

Según Andreu, F. (2006) las amenazas a una red inalámbrica se dividen en: a) ataques pasivos cuyo objetivo es hacer uso ilegal e inadecuado de los recursos encontrados mediante el análisis de red, la intercepción y el análisis de tráfico; y, b) ataques activos, que tienen dos objetivos diferentes: crear un punto de acceso personal para que los usuarios de la red se conecten con el intruso y comiencen a transmitir información; o, "colapsar los servicios que presta la red"(Andreu, 2006: 31).

a) Ataques pasivos

- **Espionaje/*Surveillance*.-** Consiste en acceder a las instalaciones de la red y seleccionar información respecto a la topología de la red, de ésta forma planificar posteriores ataques.
- **Escuchas/*Sniffing*.-** Consiste en monitorear el tráfico de la red para capturar información como direcciones MAC o IP, claves, contraseñas, entre otras. Por ejemplo *Wardriving,* el mismo que consiste en localizar puntos de acceso inalámbricos, con el uso de dispositivo inalámbrico, GPS, antena y software de rastreo.
- **Ataque por fuerza bruta.-** Son aquellos ataques que pretenden romper la clave de un algoritmo de encriptación, usando todas las combinaciones posibles. Es un método que requiere de tiempo y recursos.
- **Ataque de diccionario.-** Este tipo de ataque utiliza un archivo con una cadena de palabras factibles que luego pueden ser utilizadas para descubrir una clave. Se aplica para ataques a los protocolos WPA/WPA2 PSK, produciendo una denegación de servicio, de ésta forma el cliente debe volver autenticarse produciendo un intercambio de paquetes con el AP incluyendo las claves, y así darse el ataque de diccionario [14].
- **Ataque Hole 196.**- Este tipo de ataque afecta al protocolo de seguridad WPA2 utilizado en Wi-Fi, debido a que el estándar IEEE 802.11, permite que los clientes de la red reciban tráfico *broadcast* desde el AP con una clave común. Dando lugar a ataques "*man-in-the-middle*", pudiendo desencriptar datos de otros usuarios o provocar tráfico malicioso [14].

b) Ataques activos

- **Puntos de acceso no autorizados.-** Estos puntos de acceso son llamados *Rogue AP* y no son administrados por los propietarios de la red, por lo que los mecanismos de seguridad pueden ser vulnerados.

- **Suplantación.-** Consiste en suplantar la identidad de un usuario, en este ataque generalmente se usa la dirección MAC para identificarse como un cliente autorizado en la red.
- **Reactuación.-** En este caso se capturan mensajes legítimos para repetirlos y así producir un efecto no deseado, por ejemplo el envío masivo de correos electrónicos.
- **Denegación de servicio.-** Se da cuando los usuarios legítimos se ven impedidos de usar los servicios y recursos de los que dispone la red, pues el ataque consiste en hacerla inaccesible. Para lo cual se modifican parámetros del estándar, donde se envían mensajes sin esperar los intervalos de guarda necesarios [15].

5.2 Mecanismos de seguridad

Los mecanismos de seguridad son técnicas que poseen características específicas, se utilizan para implementar un servicio y proporcionar el nivel de seguridad necesario al sistema [16]. El tema de seguridad en comunicaciones es muy amplio y existen mecanismos que son utilizados en la mayoría de aplicaciones, entre los que se puede señalar los siguientes:

- ***Firewall*.-** Es un dispositivo que realiza un filtrado de los paquetes que circulan entre las redes de datos. Examina las direcciones IP y los puertos, además de las cabeceras TCP/IP de las capas de red y de transporte. De esta forma analiza las comunicaciones entrantes y salientes, y dependiendo del tipo de servicio permite o no las transmisiones entre las redes.[9]
- **VPN (*Virtual Private Network*).-** La Red Privada Virtual permite hacer una extensión de la red local sobre una red pública – Internet o una red WAN (*Wide Area Network*) –. Se pueden realizar conexiones para usuarios remotos – uso de *router* para el proceso de conexión –, para acceso a Internet – utiliza el protocolo HTTPS – [16].

- **Protocolo SSL (*Secure Sockets Layer).-*** Es un protocolo de propósito general permite establecer conexiones seguras a través de internet, fue propuesto por *Nestscape Communications Corporation* en 1994. Proporciona servicios de encriptación de datos, autenticación de servidores, integridad de mensajes, opcionalmente autenticación de cliente. Por lo que este protocolo garantiza la confidencialidad e integridad de la información que transita desde el navegador hasta el servidor [8].
- **Protocolo SSH (*Secure Shell*).-** Utiliza criptografía de clave pública, y permite acceder a terminales remotos de forma segura. Además gestiona claves RSA y proporciona seguridad para FTP (*File Transfer Protocol*)[8].
- **Protocolo TLS (*Transport Layer Security).-*** Es un protocolo basado en SSL, que presenta seguridad a las comunicaciones por Internet, especialmente a los ataques de los intermediarios. Utiliza criptografía asimétrica y fue actualizado por última vez en marzo 2011 (RFC 6176).[9]
- **Protocolo IPSec (*IP security*).-** Es una versión del protocolo IP, que proporciona autenticación, confidencialidad e integridad de la información y así protegerla de los ataques cuando ésta transita por la red. IPSec puede ser utilizado con otros dispositivos de protección de redes (redes privadas virtuales, firewall,..)[8]
- **WEP (*Wired Equivalent Privacy*).-** Es aplicado en el estándar 802.11, en la mayoría de dispositivos inalámbricos. Utiliza el algoritmo de criptografía simétrica RC4, con claves de 64 bits o de 128 bits. Fue diseñado para garantizar la confidencialidad, el control de acceso y la integridad de los datos [17]. Sin embargo se han presentado algunas debilidades respecto a WEP, como el inconveniente de utilizar el mismo vector de inicialización en las transmisiones, la distribución manual de las claves, la falta de protección a mensajes repetitivos, un débil sistema de autenticación. Por lo que se considera no seguro para una red inalámbrica. Para lo cual, se proponen alternativas como el uso de RADIUS, para distribución de claves y autenticación de usuarios, o el uso

de VPNs que son consideradas seguras, el problema que se puede presentar es la "falta de interoperabilidad con dispositivos de distintos fabricantes" [18].

- **WPA (*Wi-Fi Protected Access*).-** "Es un mecanismo de control de acceso a una red inalámbrica" [19]. Desarrollado para corregir las debilidades presentadas en WEP, utiliza un servidor de autenticación, distribución dinámica de claves y un vector de inicialización más robusto. Al momento se cuenta con WPA2, éste incluye un algoritmo de encriptación AES, el mismo que involucra un *hardware* más potente [18], implementa la mayoría del estándar IEEE 802.11i.

5.3 Análisis de los mecanismos de encriptación

La criptografía es tan antigua como la escritura, etimológicamente proviene del griego κρυπτο (**Kryptos)** = secreto y ΓΡΑΦΕΙΑ (**Graphos)** = escribir, y se traduce como el arte de escribir de manera secreta. [20]. Los autores Menezes, Van Oorschot y Vanstone, manifiestan:

> *"Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques"* [21]
>
> Lo que se traduciría como: "La criptografía es el estudio de técnicas matemáticas relacionadas con los aspectos de la seguridad de la información tales como la confidencialidad, la integridad de datos, la autenticación de entidad y de origen. La criptografía no comprende solo a los medios para proveer seguridad de información, sino a un conjunto de técnicas"

En 2006 Jorge Ramio Aguirre, define a la criptografía como:

> “Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves” [22]

La criptografía clásica establece dos procedimientos para encriptar información: sustitución y transposición.

- **Sustitución**.- Consiste en sustituir los símbolos del mensaje original por otros, de tal forma que el receptor hace la relación entre el símbolo recibido y el asignado previamente según lo acordado entre las partes. [23]
- **Transposición.-** Consiste en alterar el orden de los símbolos del mensaje original, el receptor con la ayuda de la clave reordena los símbolos para conocer el mensaje enviado[24].

Por lo que se considera a la criptografía como una ciencia que se fundamenta en las matemáticas discretas y la teoría de la información; y, a pesar de que por mucho tiempo su uso estuvo destinado al campo militar y gubernamental, hoy en día su aplicación es una necesidad de los sistemas informáticos, pues está encaminada a procurar la confidencialidad, autenticación, integridad y no repudio en la transmisión de la información [23]. Tiene como objetivo proteger la tanto información almacenada, como la que se trasmite por un medio de comunicación. Su aplicación se basa en el uso de protocolos criptográficos – tareas o pasos para alcanzar un objetivo – y algoritmos criptográficos – especificaciones concretas y detalladas para alcanzar un objetivo –, los mismos que están desarrollados a través de funciones matemáticas.[10]

5.3.1 Protocolos criptográficos

5.3.1.1 Protocolos de criptografía simétrica

Consiste en la distribución de una misma clave para la comunicación entre el emisor y el receptor, la clave asignada se utiliza para encriptar y desencriptar el mensaje [25]. El nivel de

seguridad tiene relación con el tamaño de la clave [26]. Las vulnerabilidades en el protocolo de criptografía simétrica están en mantener secreta la clave asignada a las partes, para que ésta no pueda ser usada por personas no autorizadas, o que sea interceptada en el momento de la distribución; y, al existir mayor número de destinatarios del mensaje todos deberán conocer la clave secreta, por lo que se debe calcular la cantidad de claves a distribuirse utilizando la fórmula: $n(n-1)/2$, siendo n el número de destinatarios [10], siendo un inconveniente el resguardo de tantas claves, pudiendo existir problemas como: suplantación de identidad, falsificación, entre otras. Para que pueda ejecutarse una transmisión, el protocolo de criptografía simétrica sigue el siguiente proceso.[27]

- *Asignación de Claves*: Se asigna la clave secreta a las partes y se las transmite a través de cualquier forma de comunicación (telefónica, correo electrónico, personal, entre otras).
- *Encriptación del texto*: Para esto se aplica un algoritmo de encriptación previamente establecido por las partes utilizando la clave secreta.
- *Desencriptación del texto*: Para esto se aplica un algoritmo de desencriptación previamente establecido por las partes, utilizando la misma clave secreta que se usó para la encriptación.

5.3.1.2 Funciones Hash

También conocidas como huellas digitales *(finger-prints)*, son funciones de una vía que se basan en operaciones matemáticas para tomar a la entrada un conjunto de datos de longitud variable; y, convertirlos en información de longitud fija a la salida. La función hash debe cumplir los siguientes requisitos: imposibilidad de obtener el texto original a partir de la huella digital, imposibilidad de encontrar un conjunto de datos diferentes que tengan la misma huella digital,

transformar un texto de longitud variable en una huella de tamaño fijo, facilidad de empleo e implementación. A continuación se muestra algunos ejemplos de funciones de una vía:

1. **Algoritmo MD5.-** Es una función hash de 128 bits. Este algoritmo se usa para firmas digitales, más no para encriptar mensajes. La información original no se puede recuperar ya que hay pérdida de datos.
2. **SHA-1**.- En una función de 160bits, la compresión es más compleja que la función de MD5, por lo que es más lento que MD5; sin embargo el contar con una mayor longitud (160bits contra 128bits), hace que SHA-1 sea más robusto y seguro.
3. **SHA-2.-** En esta función los rangos de salida han sido incrementados: SHA-224, SHA-256, SHA-384, y SHA-512. Convirtiéndose en el más seguro SHA-512, pues cuenta con mayor número de bits a la salida.

5.3.1.3 Protocolos de criptografía asimétrica

Los protocolos de criptografía asimétrica usan dos claves (pública y privada) para el envío de mensajes, las mismas que pertenecen al receptor del mensaje. La clave pública se puede entregar a cualquier persona, la clave privada únicamente a la persona autorizada y debe guardarla para que nadie más tenga acceso a ella. El emisor usa la clave pública del destinatario para encriptar el mensaje, y solo la clave privada del receptor podrá desencriptarlo [10].

La asignación de la clave pública se hace a través de certificados digitales –documento electrónico que contiene la clave y la identidad del destinatario y está avalado por una entidad certificadora –, ya que de esta forma se asegura que una determinada clave pertenece a un solo usuario [27]. El proceso que utiliza el protocolo de criptografía asimétrica es el siguiente:

- *Generación de las claves*: Cada usuario debe contar con sus propias claves, para esto se utilizan algoritmos de generación de claves públicas y privadas.

- *Asignación de las claves públicas*: Este proceso se basa en una Infraestructura de Clave Pública (PKI, *Public Key Infrastructure*) donde la identidad del usuario conjuntamente con su clave pública son almacenados en un Certificado Digital.

- *Hash o huella digital*: Consiste en aplicar la función matemática unidireccional.

- *Firmado del mensaje:* Encriptación del *Hash* del documento con la clave privada del emisor para adjuntarlo al mensaje original.

- *Validación de la Integridad:* Cuando el receptor recibe el mensaje y su firma digital asociada, se debe calcular el *Hash* del documento recibido y desencriptar la firma digital con la clave pública del emisor y comparar ambos *Hash*, de esta forma garantiza que el mensaje recibido fue el correcto, en caso de que al comparar los hash, éstos no coincidan se considera que la información fue alterada.

5.3.1.4 Protocolo de firma digital

La firma digital o firma electrónica, es un método que generalmente utiliza criptografía asimétrica o de clave pública para encriptar y desencriptar información, su aplicación garantiza: la autenticidad de quién dice ser el emisor de un mensaje, la integridad de los datos transmitidos y el no repudio, pues existe una entidad certificadora responsable del proceso. [28]

En el Ecuador la Ley 2002-67 de Comercio Electrónico, firmas electrónicas y mensajes de datos, el art.13 *Firma Electrónica*, señala: “Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos” [29].

5.3.1.5 Certificado Digital

Un certificado digital es un documento electrónico que permite validar la identidad de una persona o institución a quien se le asignará unas claves asimétricas. Dicha validación es emitida por una entidad certificadora siendo ésta la Autoridad de Certificación (AC). Pueden ser almacenados en tarjetas inteligentes ("*Smart Card*"), *Tokens*, memorias USB o en el computador del usuario. Los certificados digitales tienen un período de duración determinada, por lo que una vez concluido este tiempo deben ser revocados. [16]

En Ecuador el Consejo Nacional de Telecomunicaciones (CONATEL) es el estamento gubernamental encargado de autorizar a empresas o personas jurídicas que presten servicios para emitir certificados de firma electrónica. Así también se establece sus obligaciones y responsabilidades en la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos. (Ley 2002-67, Art. 29, 2002). El 8 de octubre de 2008, se acreditó al Banco Central del Ecuador como Entidad Certificadora (Resolución N° 481-20-2008); y, el 22 de octubre de 2010 a la compañía SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. como Entidad de Certificación de Información y Servicios Relacionados (Resolución N° 640-21-2010) [30].

La recomendación UIT-T X.509 versión 3, establece el formato normalizado de certificados digitales, el mismo que contiene la siguiente información [31]:

Versión
Titular
Emisor
Firma (ID de algoritmo)
Número de serie de certificado
Periodo de validez
Atributos
ID único de emisor
Extensiones

Figura 2. Estructura de un certificado de atributo X.509 [13]

a. *Versión.* Contiene el número de versión del certificado encriptado.
b. *Número de serie del certificado.* La autoridad certificadora emite un único número de serie.
c. *Identificador del algoritmo de firmado.* Identifica el algoritmo empleado para firmar el certificado.
d. *Nombre del emisor.* Identifica a la autoridad certificadora.
e. *Período de validez.* Indica el período de validez del certificado, debe contener la fecha de emisión y de renovación.
f. *Nombre del sujeto.* Identifica el nombre de la entidad a la que se va a emitir el certificado.
g. *Información de llave pública del sujeto.* Especifica los parámetros de la clave pública, así como el algoritmo empleado.
h. *Identificador único del emisor.* Es un campo opcional que permite reutilizar nombres de emisor.
i. *Identificador único del sujeto.* Es un campo opcional que permite reutilizar nombres de sujeto.

5.3.2 Algoritmos de criptografía

Los algoritmos criptográficos son funciones matemáticas estructuradas como un conjunto finito de pasos, que permiten encriptar y desencriptar datos, se basan en tres principios: teoría de la información, teoría de los números, teoría de la complejidad. [10]. Basados en éstos se han establecido dos métodos de encriptación: encriptación en bloque y encriptación en flujo [32].

1. **Encriptación en bloque**.- Consiste en tomar un bloque de texto original como entrada y aplicando la clave secreta, producir un bloque de texto encriptado de igual tamaño que el de entrada. Para desencriptar el texto se realiza el mismo proceso,

es decir se ingresan bloques de texto encriptado y se producen bloques de texto original.

2. **Encriptación en flujo.-** Este método convierte un texto original en un texto encriptado bit a bit, para esto se genera un algoritmo de secuencias pseudoaletaorias para el flujo de clave, el mismo que se combina con el flujo de datos mediante la operación XOR.

Así también los algoritmos criptográficos presentan 4 modos de operación: [25]

1. **ECB (*Electronic Codebook*)**.- Se subdivide el texto original en bloques de tamaño apropiado y se encriptan todos ellos utilizando la misma clave.
2. **CBC (*Cipher Block Chaining*).-** En este modo se utiliza una retroalimentación, ya que el bloque encriptado es utilizado a través de una operación XOR para el proceso de encriptación del siguiente bloque. Para el primer bloque se aplica un vector de inicialización (VI).
3. **CFB (*Cipher Block Feedback*).-** Este modo puede encriptar información en tamaños menores al bloque. El bloque de entrada se divide en varios paquetes pequeños, y éstos se combinan con el último bloque encriptado mediante una operación XOR. Aplica un vector de inicialización al inicio.
4. **OFB (*Output Feedback*).-** Se aplica para métodos de encriptación por flujo, ya que genera bits independientemente del texto. Para luego combinarse bit a bit mediante una operación XOR y la salida del algoritmo.

5.3.2.1 Algoritmos de criptografía simétrica

5.3.2.1.1 Algoritmo DES (Data Encryption Standard)

Es el más desarrollado a nivel mundial, en 1976 fue considerado como estándar de comunicaciones no clasificadas por el gobierno de los Estados Unidos [25], y en 1981 fue

aprobado por el *American National Standards Institute* (ANSI). En 1999 se hizo un ataque a DES utilizando alrededor de 2^{56} posibles claves, por lo que se restringe para aplicaciones de alta seguridad [33]. Este algoritmo tiene una clave de 64 bits, siendo 8 usados como bits de paridad, por lo que la clave es de 56 bits reales [24]. DES aplica un tipo de encriptación en bloque, utiliza la sustitución seguida de una permutación, como secuencias repetitivas, a este tipo de operaciones se les denomina rondas. El algoritmo consiste en aplicar a un bloque de 64 bits de longitud de texto original, 16 rondas en la encriptación y usa el mismo procedimiento para desencriptar el texto.[10]

5.3.2.1.2 Algoritmo Triple DES

Aparece por la necesidad de conseguir una versión fortalecida del algoritmo DES, consiste en realizar 3 veces consecutivas el proceso DES, de tal forma que su clave sea el conjunto de las tres claves DES aplicadas [12].

5.3.2.1.3 Algoritmo AES (Advanced Encryption Standar)

Aparece en 2001 y fue creado por Joan Daemen y Vicent Rijmen, por lo que también es conocido como Rijndael. Es un algoritmo con una longitud de bloque de 128 bits, y una clave de 128, 192 o 256 bits [10]. Consiste en procesar el bloque de 128 bits y la clave en matrices cuadradas, en cuatro fases: “la sustitución de bits, desplazamiento de filas, mezcla de columnas, suma de la clave usando una operación XOR bit a bit del bloque original con una porción de la clave extendida”. [34]

5.3.2.1.4 Algoritmo IDEA (International Data Encryption Algorithm)

Fue diseñado por Xuejia Lai y James L. Massey en el Instituto Tecnológico federal Suizo. [35].Trabaja con bloques de 64 bits de longitud y una clave de 128 bits. Realiza tres operaciones: XOR, suma en módulo de 2^{16} y multiplicación en módulo $2^{16}+1$.[5]

5.3.2.1.5 Algoritmo Blowfish y Twofish

Desarrollado por Bruce Schneier en 1993, con encriptación por bloques y clave de longitud variable (448 bits). Es un algoritmo rápido y robusto, sin embargo no fue seleccionado para estandarización.[10]

5.3.2.1.6 Algoritmo RC4

Fue desarrollado por Ron Rivest para la compañía RSA Data Security Inc. por lo que es conocido como ARC4 o Alle-ged-RC4. Es un algoritmo de encriptación por flujo [36], usado por los protocolos SSL y WEP, el flujo de claves se genera seudo-aleatoriamente a partir de una clave de 40 y 256 bits [10].

5.3.2.2 Algoritmos de criptografía asimétrica

5.3.2.2.1 Algoritmo RSA

Toma su nombre debido a las iniciales de sus creadores Ron Rivest, Adi Shamir y Leonard Adleman, es considerado uno de los algoritmos más seguros y su popularidad lo hace de entre los favoritos para aplicaciones de encriptación, permite la generación de firmas digitales. Su seguridad radica en la dificultad de factorar números grandes, puesto que la clave pública y privada son generadas en función de números primos entre 100 y 300 dígitos [36].

5.3.2.2.2 Algoritmo ElGamal

Basado en el algoritmo Diffie-Hellman, fue presentado por Taher Elgamal en 1984, se usa para encriptación y desencriptación de información, así como para firma digital. Este algoritmo tiene la seguridad en la dificultad que significa el calcular logaritmos discretos en un campo finito. Es una versión más robusta del RSA [10].

5.3.2.2.3 Algoritmo DSA (Digital Signature Algorithm)

Es un estándar para firmas digitales. Expuesto en 1991, no es utilizado para encriptar información. El tiempo que requiere el algoritmo es mayor que el de RSA [20].

5.3.2.2.4 Algoritmo Diffie-Hellman

Es el primer algoritmo de clave pública, desarrollado por Whitfield Diffie y Martin Hellman. Se caracteriza porque el algoritmo es utilizado para la distribución de las claves, más no para encriptar o desencriptar mensajes [23]. “La seguridad se basa en la dificultad de calcular logaritmos discretos en un campo finito” [10].

5.3.2.2.5 Algoritmos de Curvas Elípticas

Fueron propuestos en 1985 desarrollados por Neil Nobalitz y Victor Millar de manera independiente. Este sistema se basa en el logaritmo discreto, y en lugar de números enteros utiliza coordenadas cartesianas, sobre las cuales se definen las propiedades: conmutativa, asociativa, elemento neutro y elemento simétrico, y las operaciones suma y multiplicación. En la actualidad aún no se ha encontrado ningún sistema capaz de romper el algoritmo en un tiempo razonable, ni siquiera para claves pequeñas. Los procesos de encriptación y desencriptación son bajos, lo que reduce los costos de implementación.[20]

Una vez establecidas las características de los protocolos de criptografía simétrica y asimétrica, se presenta en la tabla 1 un resumen de las ventajas y desventajas de cada uno de éstos. Así también, se destacan los algoritmos más utilizados como mecanismos de encriptación, incluyendo el tamaño de las claves que se aplican. No obstante, en la siguiente sección se realizará un análisis comparativo que permita destacar particularidades de los algoritmos de cada uno de las criptografías mencionadas.

Tabla 1: Comparación entre criptografía simétrica y asimétrica [37]

	Ventajas	Desventajas	Algoritmos más utilizados	Tamaño de clave
Criptografía Simétrica	Eficiente en grupos reducidos, debido a que requiere una única clave	La clave se debe compartir entre el emisor y el receptor, por lo que el medio de comunicación puede resultar inseguro	DES	56 bits
	No se requiere de una tercera parte confiable	No es posible autenticar al emisor	TripleDES	de 128 bits a 256 bits
	Tiene una infraestructura sencilla	Requiere de un número elevado de claves (n(n-1))⁄2, donde n es el número de destinatarios	Blowfish	de 128 bits a 256 bits
			AES	de 128, 192 o 256 bits
Criptografía Asimétrica	Debido a que utiliza la clave pública y la privada, el número de claves es reducido	La generación de claves implica un alto proceso computacional	RSA	mayor o igual a 1024 bits
	La clave privada no se trasmite entre el emisor y el receptor	Necesita de una Autoridad Certificadora	DSA	de 512 a 1024 bits
	Se realiza la autenticación de la clave privada	Requiere una infraestructura mayor para el proceso.	El Gamal	de 1024 a 2048 bits

5.3.3 Comparación de los algoritmos de criptografía simétrica

5.3.3.1 Velocidad de proceso de encriptación y desencriptación

En esta sección se hace una comparación de la velocidad de proceso de encriptación y desencriptación de los algoritmos de criptografía simétrica. Para lo cual se aplican herramientas de código abierto [32], que permitan realizar dicha comparación. Las mismas que se detallan a continuación:

1. *OpenSSL*[1].- Es una implementación de los protocolos SSL y TLS, utiliza lenguaje de programación C. Tiene versiones disponibles para los sistemas operativos Linux y

[1] https://www.**openssl**.org/

Microsoft Windows, y los algoritmos criptográficos que implementa son: AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, TDES, GOST 28147-89, RSA y DSA.

2. *TrueCrypt*[2].- Es una aplicación disponible para los sistemas operativos Linux y Windows. Permite crear volúmenes encriptados a los que se puede acceder si se conoce la contraseña y/o archivo clave que se utilizó para su creación. Trabaja con los siguientes algoritmos: Twofish, AES y Serpent –es un algoritmo de cifrado simétrico de bloques, utiliza un tamaño de bloque de 128 bits, tamaños de llave de 128, 192 y 256 bits y consta de 32 rondas–, y las posibles combinaciones entre ellos.
3. *DiskCryptor* [3] .- Soporta algoritmos de encriptación AES, Twofish, Serpent, y las combinaciones entre ellos. Realiza un *benchmarking* de la velocidad de encriptación de los algoritmos. Disponible para los sistemas operativos Windows.

Para la elección del *hardware*, en el cual se instaló cada una de las herramientas, se realizó una prueba entre tres computadores, aplicando el *software OpenSSL*, que tiene un mayor número de algoritmos para procesar; y, de esta forma comparar el rendimiento entre los equipos, que poseen sistema operativo Windows 7 de 64 bits, y las siguientes características:

Tabla 2: Características de los equipos

	Computador 1	Computador 2	Computador 3
Procesador	Intel Core i7 2.1GHz	Intel Core i5 2.67GHz	Intel Core i3 1.89 GHz
Memoria RAM	8.00 GB	4.00GB	4.00GB

Una vez ejecutada la prueba se obtuvo como resultado que para todos los tamaños de bloque (16, 64, 256, 1024 y 8192 bytes) que se compararon, el rendimiento del computador 1 fue el

[2] www.**truecrypt**.org/downloads

[3] https://**diskcryptor**.net/

mejor. En la figura 2 se muestra la evaluación de los algoritmos para un tamaño de bloque de 8192 bytes en función de las tres computadoras.

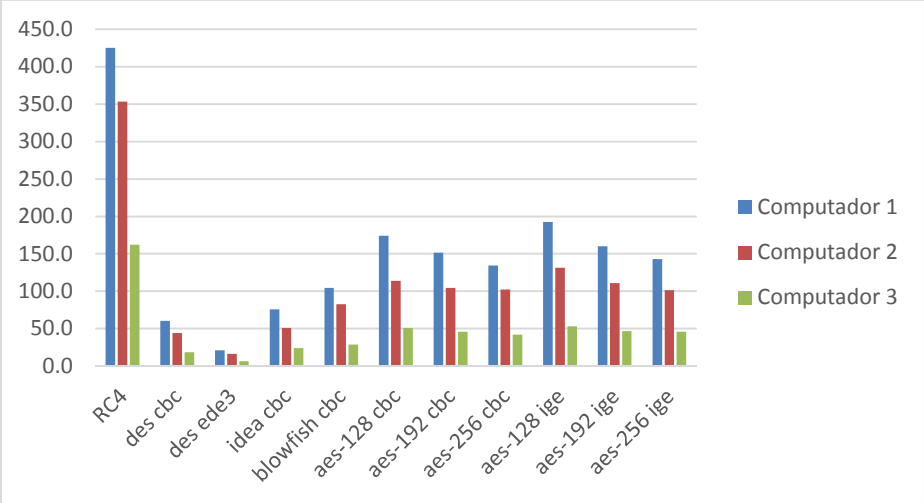


Figura 2: Rendimiento de las tres computadoras utilizando OpenSSL

Es así como se determinó que debido al tiempo de ejecución en el procesamiento, la evaluación de los algoritmos se debía realizar en el computador 1, el mismo que tiene memoria RAM de 8 GB y procesador de 2,1 GHz.

5.3.3.1.1 Evaluación de los algoritmos de encriptación utilizando OpenSSL:

Para realizar esta evaluación se utilizó el comando *speed* del *software,* con el cual el sistema hace una prueba de la velocidad de encriptación de cada algoritmo en diferentes modos de operación (cbc, ige), variando el tamaño del bloque (16, 64, 256, 1024 y 8192 bytes) que se va a encriptar; y, en algunos casos el tamaño de la clave (AES de 128, 192 y 256 bits). Los resultados son presentados en la tabla 3 y de manera gráfica en la figura 3, y están en megabytes por segundo (MB/s). Con este software se comparó los algoritmos: RC4, DES, IDEA, Blowfish y AES.

Tabla 3: Velocidad de proceso en MB/s para diferentes tamaños de bloques utilizando OpenSSL

Algoritmo	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
RC4	493,3	431,8	416,4	357,4	425,1
des cbc	58,1	59,6	60,2	58,9	60,3
des ede3	22,0	20,8	21,1	21,3	21,2
idea cbc	72,7	74,6	75,5	76,7	76,0

blowfish cbc	96,4	100,7	102,8	104,0	104,4
aes-128 cbc	155,5	169,0	171,8	175,8	174,1
aes-192 cbc	139,3	147,8	149,6	150,1	151,6
aes-256 cbc	124,5	131,6	133,6	134,0	134,2
aes-128 ige	172,4	182,9	185,6	185,1	192,4
aes-192 ige	151,8	161,6	155,8	158,1	160,2
aes-256 ige	133,7	140,0	140,0	140,7	142,8

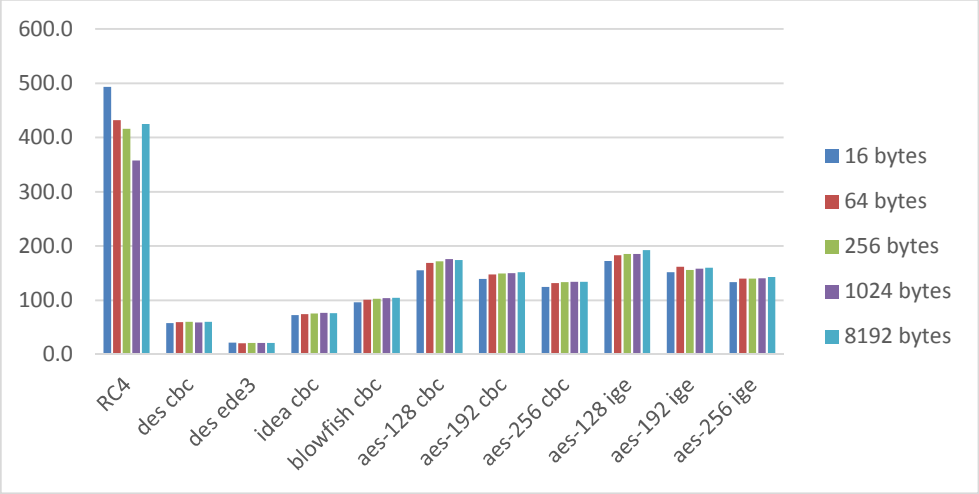


Figura 3: Velocidad de proceso en MB/s para diferentes tamaños de bloques utilizando OpenSSL

De los resultados obtenidos se puede establecer que independientemente del tamaño de bloque, el algoritmo RC4 tiene una velocidad de proceso mayor que los otros algoritmos. En segundo lugar se encuentra AES en modo de operación ige y con tamaños de clave de 128 bits, seguido de AES en modo cbc y tamaño de clave de 128 bits. En tercer lugar se encuentra Blowfish en modo cbc.

5.3.3.1.2 Evaluación de los algoritmos de encriptación utilizando TrueCrypt:

El *software TrueCrypt* permite generar un *benchmark* con los algoritmos que contiene y las combinaciones entre ellos. En esta comparación se puede elegir el tamaño del *buffer* a encriptar; y, presenta las velocidades en el proceso de encriptación y desencriptación en gigabytes por segundo (GB/s) y megabytes por segundo (MB/s), además del promedio entre ellas. Para esta

evaluación se han considerado los algoritmos AES, *Twofish* y *Serpent* y se ha variado el tamaño de *buffer*. En la figura 4 se presenta un ejemplo de la pantalla del *software* al aplicar el *benchmark* de encriptación con un tamaño de *buffer* de 50 MB.

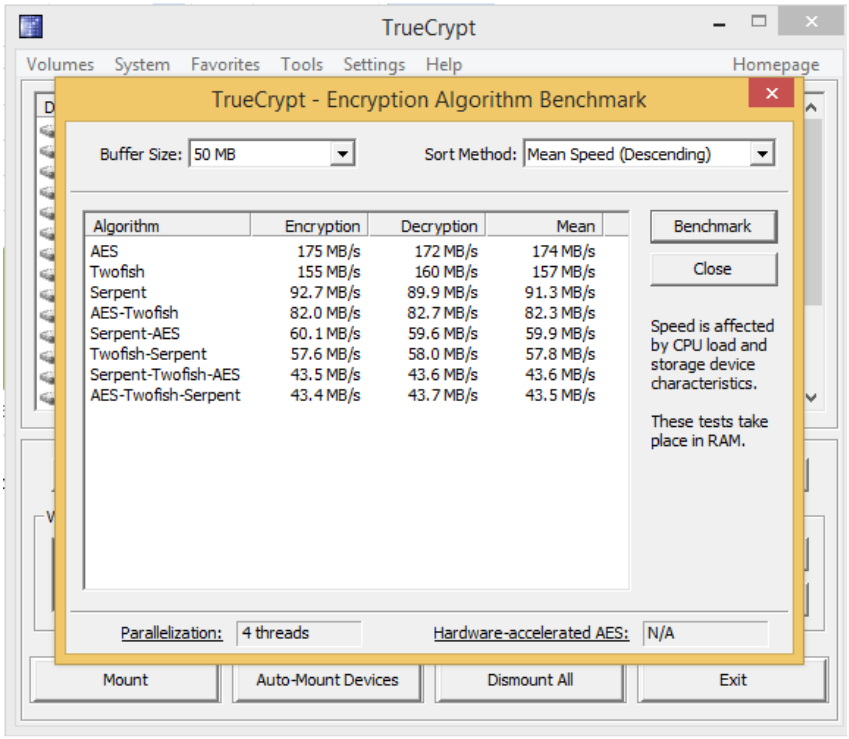


Figura 4: Ejemplo del Encryption Algorithm Benchmark para un tamaño de buffer de 50 MB utilizando TrueCrypt

En la tabla 4 se presentan los resultados obtenidos en la evaluación de los algoritmos para tamaños de *buffer* de: 100KB, 500KB, 1MB, 50MB, 200MB; y, de forma gráfica en la figura 4.

Tabla 4: Promedio en MB/s para diferentes tamaños de buffer utilizando TrueCrypt

Algoritmo	100 KB	500 KB	1 MB	50 MB	200 MB
AES	68,9	78,9	79,5	174	177
Twofish	67,1	71	71,4	157	159
Serpent	37,4	39,3	41,3	91,3	93,6

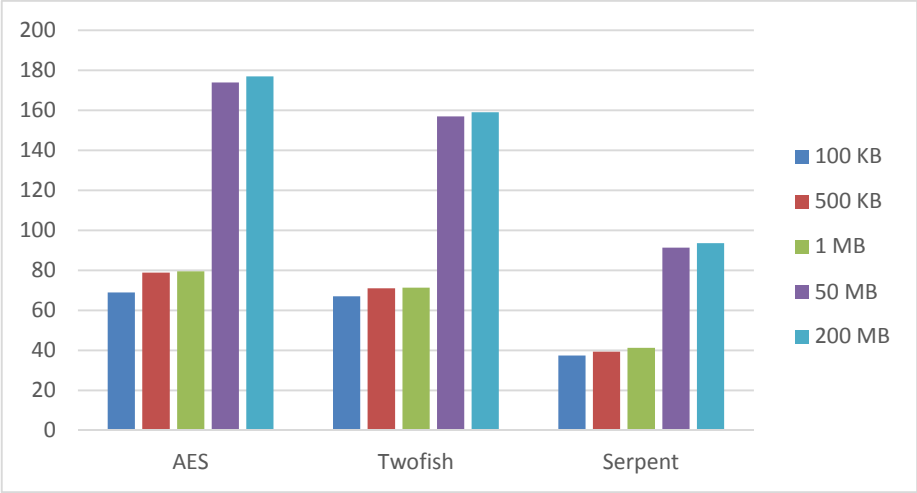


Figura 5: Promedio en MB/s para diferentes tamaños de buffer utilizando TrueCrypt

De los resultados se ha determinado que el algoritmo AES tiene una mayor velocidad de proceso de encriptación y desencriptación para cualquiera de los tamaños de *buffer* comparados, seguido por Twofish y finalmente Serpent. Se puede diferenciar que cuando el tamaño del *buffer* está entre 100 KB y 1 MB, los valores de la velocidad no sobrepasan los 80 MB/s, mientras que cuando el tamaño está entre 50 MB y 200 MB, la velocidad se incrementa notablemente.

5.3.3.1.3 Evaluación de los algoritmos de encriptación utilizando DiskCryptor:

Este *software* presenta entre sus herramientas un "Encryption Benchmark", este proceso permite determinar la velocidad de encriptación y desencriptación en megabytes por segundo (MB/s) de los algoritmos disponibles AES, Twofish y Serpent y las combinaciones entre ellos. Mediante este proceso se puede tener una referencia para seleccionar el algoritmo que se desee utilizar. Ya que en esta prueba no es factible manipular otra variable para la comparación, lo que se realizó es un *benchmark* con las unidades de disco. En la figura 6 se muestra un ejemplo de la pantalla del *software* al evaluar el disco D con un tamaño de 454GB.

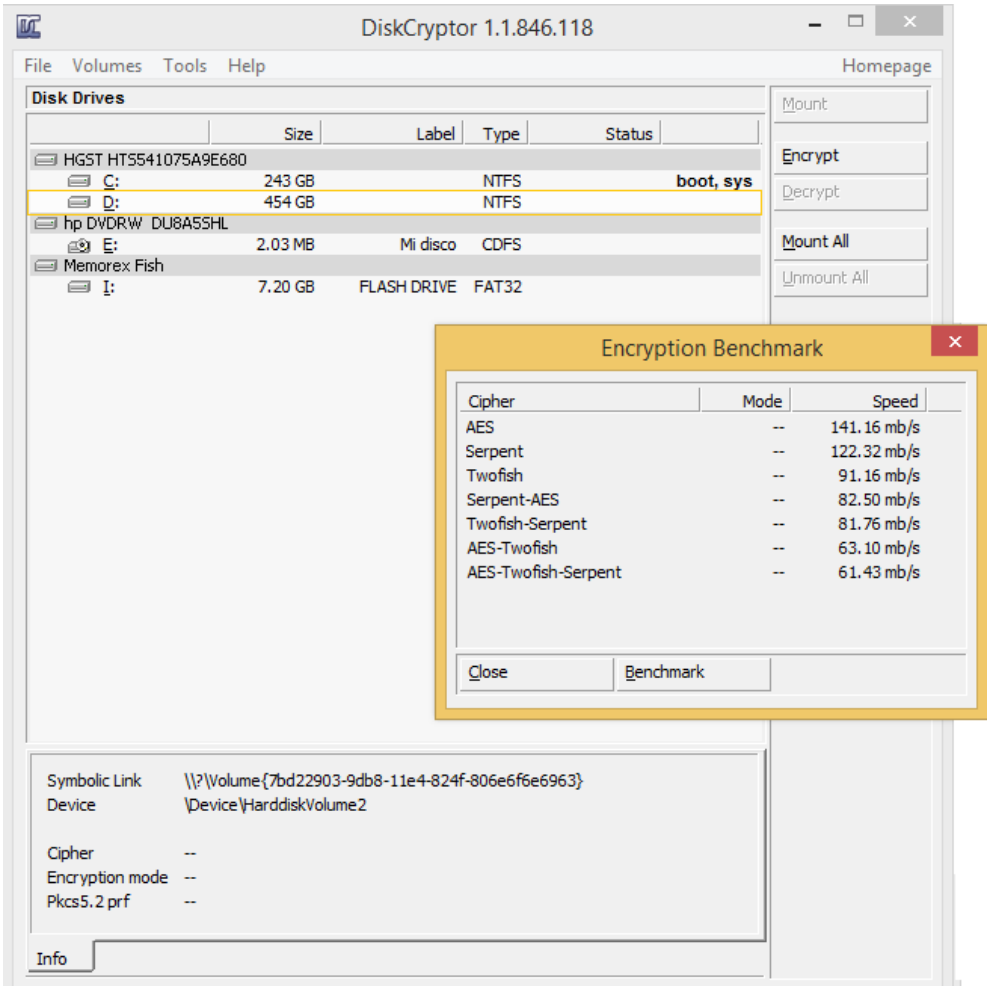


Figura 6: Ejemplo del Encryption Benchmark para la unidad de disco D utilizando DiskCryptor

Para la evaluación se comparó cada uno de los algoritmos con el tamaño de las unidades de disco (C: 243 GB, D: 454 GB, E: 2.03MB, I: 7.2GB). Los resultados obtenidos se muestran en la tabla 5 y de manera gráfica en la figura 7.

Tabla 5: Velocidad en MB/s para diferentes tamaños de unidad de disco utilizando DiskCryptor

Algoritmo	243 GB	454 GB	2.03 MB	7.2 GB
AES	130,55	141,16	137,54	138,66
Twofish	111,29	122,32	118,92	116,07
Serpent	85,04	91,16	94,45	93,24

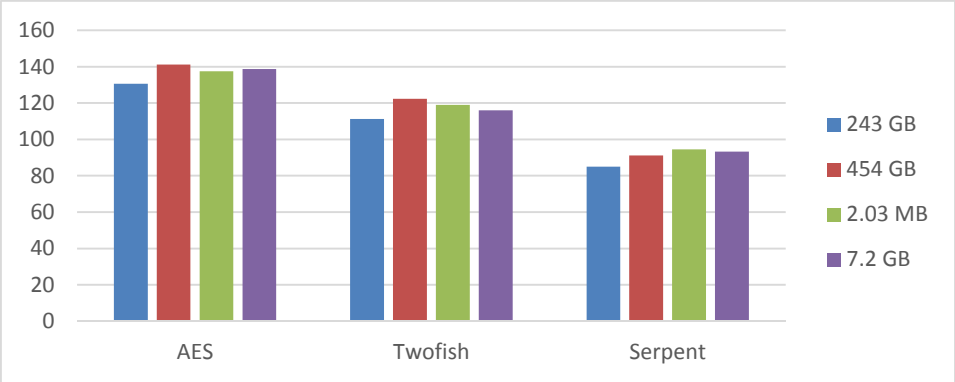


Figura 7: Velocidad en MB/s para diferentes tamaños de unidad de disco utilizando DiskCryptor

Con los resultados obtenidos, se puede observar que en este caso AES es el algoritmo con mayor velocidad de encriptación y desencriptación para todas las unidades de disco, seguido por *Twofish* y *Serpent*.

5.3.3.2 Análisis de resultados

De los resultados presentados, se establece que los algoritmos RC4 y AES, son los que tienen una mayor velocidad en el proceso de encriptación y desencriptación. Por lo que el análisis para recomendar uno de éstos dos algoritmos como mecanismo de encriptación, se sustentará en otro factor para la elección del algoritmo. En este caso se expondrán argumentos respecto a la robustez.

El nivel de seguridad en la encriptación de datos, también depende de la robustez del algoritmo [38]. En el caso de RC4, las investigaciones de *Scott Fluhrer, Itsik Mantin y Adi Shamir*, mostraron las debilidades del algoritmo, las mismas que radican en el vector de inicialización [39], si bien existen aplicaciones que utilizan el algoritmo RC4 como mecanismo de encriptación, es importante destacar que éste ya ha tenido problemas respecto a su seguridad, es el caso del mecanismo WEP donde las claves han sido descubiertas con facilidad [18], por lo que es

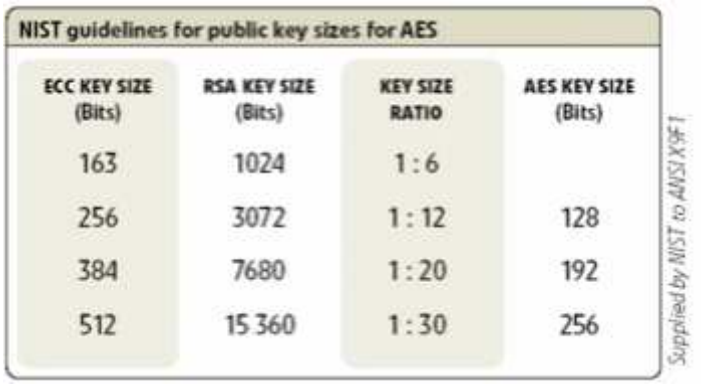
considerado como un sistema de criptografía simétrica inseguro [32], y aceptado para usuarios domésticos y aplicaciones no críticas [39].

En el año 2011, *Andrey Bogdanov, Christian Rechberger y Dmitry Khovratovich, de Microsoft Research*, descubrieron una vulnerabilidad en el algoritmo AES [40]. Sin embargo, el ataque no tiene relevancia práctica debido a que es necesaria una estructura computacional que permita probar 10 millones de claves por segundo [37]. Este algoritmo es utilizado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA), para el resguardo de información *"Secret"* con una longitud de clave de 128 bits; y, *"Top Secret"*, con claves de 192 o 256 bits, consideradas suficientemente seguras [41]. Por lo que es un algoritmo de criptografía simétrica que garantiza un alto nivel de seguridad por su robustez, y es utilizado en diversas aplicaciones.

5.3.4 Análisis de los algoritmos de criptografía asimétrica

Para este análisis se han considerado, los estudios, aplicaciones e investigaciones realizadas respecto a la comparación de algoritmos de criptografía asimétrica Carbonell (2007), Maldonado (2009), Bonilla (2012), Alfaro (2014). Exponiendo diferentes parámetros que permitan seleccionar al algoritmo de encriptación asimétrico con mejores características de desempeño y seguridad. En algunos casos se incluye en el análisis a AES, debido a los resultados de la evaluación que se realizó en los algoritmos de criptografía simétrica.

- El *National Institute of Standards and Technology* (NITS), muestra una tabla comparativa entre el tamaño de la clave de los algoritmos de criptografía asimétrica de Curvas Elípticas (ECC) y RSA; y, el algoritmo AES de criptografía simétrica. Esto debido a que en las aplicaciones se utilizan los dos tipos de algoritmos en el intercambio de claves y luego en la encriptación de la información [42].



NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Figura 8: Comparación entre el tamaño de clave de los algoritmos de Curva Elíptica, RSA y AES [42]

La figura 8 muestra la relación que existe entre el tamaño de la clave en ECC y el tamaño RSA, y se puede observar una amplia diferencia entre ellas. Además se observan datos respecto a la relación de tamaño de la clave (*key size ratio)*. Por ejemplo si en AES se requiere una clave de 192 bits para el resguardo de información, se puede alcanzar el mismo nivel de seguridad usando una clave de 384 bits utilizando el algoritmo ECC, o una clave de 7680 bits al aplicar el algoritmo RSA, teniendo una proporción de 1:20 entre el tamaño de ambas.

- La empresa *Certicom*[4] ha desarrollado investigaciones respecto al algoritmo de Curvas Elípticas (ECC), a continuación se muestra una comparación respecto al tiempo de respuesta de un servidor que utiliza algoritmos RSA (con claves de 1024 y 2048 bits) y ECC (con claves de 160 y 224 bits) expresado en milisegundos (ms), las operaciones por segundo, el *ratio* –relación– de *performance* –rendimiento– y el *ratio* de tamaño de clave [42].

[4] *Certicom principal empresa comercial de algoritmos de Curvas Elípticas ECC* - http://www.*certicom*.com

Tabla 6: Comparación de performance de RSA y Curvas Elípticas [42]

	ECC-160	RSA-1024	ECC-224	RSA-2048
Tiempo (ms)	3.69	8.75	5.12	56.18
Operaciones/seg	271.3	114.3	195.5	17.8
Ratio de Performance	2.4 : 1		11 : 1	
Ratio de tamaño de clave	1 : 6.4		1 : 9.1	

De los datos expuestos en la tabla 6 se puede establecer que el algoritmo ECC tiene tiempos de respuesta y operaciones por segundos mejores que los presentados para RSA. Se observa que al relacionar los tamaños de las claves, ECC sigue siendo mejor que RSA, puesto que el tiempo de respuesta de un RSA-1024 es de 8.75 ms, mientras que ECC-160 tiene una respuesta de 3.69 ms. En el caso del *performance* se aprecia una mayor diferencia cuando RSA-2048 realiza 17.8 operaciones/seg; y, ECC-224 ejecuta 195.5 operaciones/seg.

- Considerando el ancho de banda, *Certicom* presenta un análisis entre los algoritmos ECC, ElGamal y RSA, respecto al tamaño del texto encriptado considerando para el proceso un mensaje de tamaño de 100 bits [43]. Los resultados que se muestran en la tabla 7.

Tabla 7: Tamaño de textos encriptados [43]

Algoritmo	Tamaño de texto encriptado (bits)
RSA	1024
ElGamal	2048
ECC	321

Esta comparación permite determinar que el algoritmo ECC tiene un tamaño de texto encriptado menor al del algoritmo ElGamal, lo que se refleja en un ahorro de ancho de banda utilizado al momento de la transmisión de mensajes encriptados.

- Respecto a los niveles de seguridad *Certicom,* presenta una curva de respuesta donde se compara dicho parámetro entre ECC, RSA y DSA [42] .

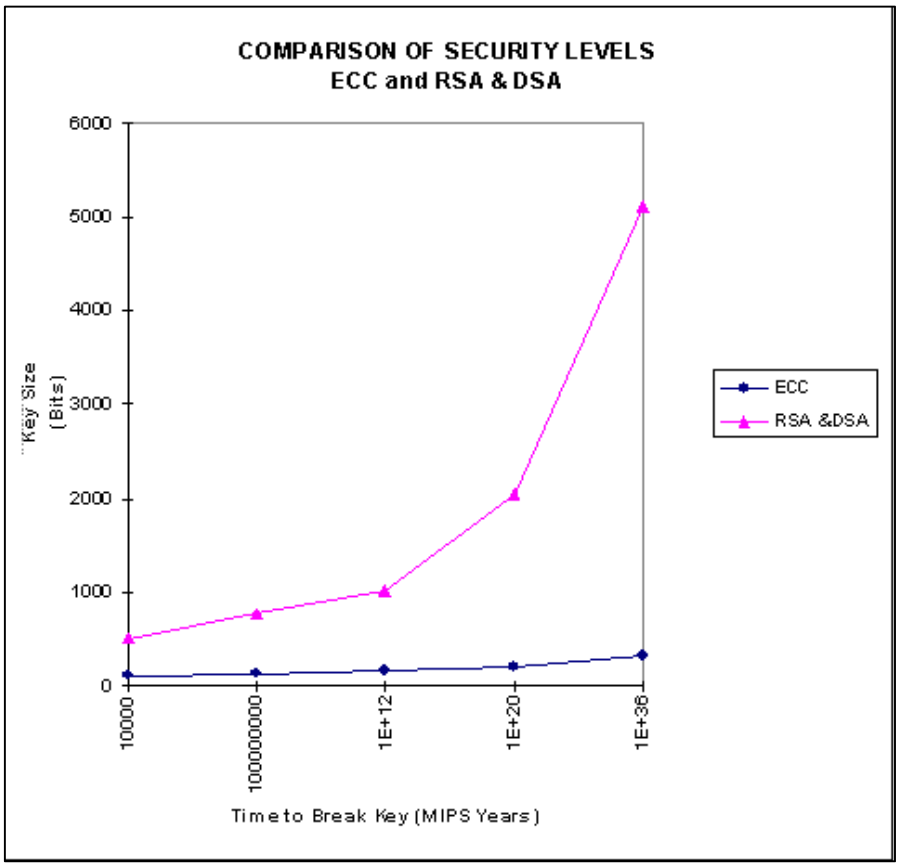


Figura 9: Comparación de los niveles de seguridad entre ECC, RSA y DSA [42].

La figura 9 muestra una curva de respuesta que relaciona el tiempo requerido para romper una clave (medido en MIPS[5] años) y el tamaño de la clave de los algoritmos. El nivel de seguridad aceptable para romper una clave es aproximadamente 10^{12} MIPS-años. Según la gráfica el algoritmo ECC, es más seguro en relación a RSA y DSA [42].

[5] *MIPS representa un tiempo de cálculo de un año en una máquina capaz de realizar un millón de instrucciones por segundo.*

- Respecto a la La Complejidad Ciclomática[6] , facilita una medición cuantitativa de la complejidad lógica de un algoritmo, la misma que compara tres algoritmos de encriptación ECC, RSA y AES [44].

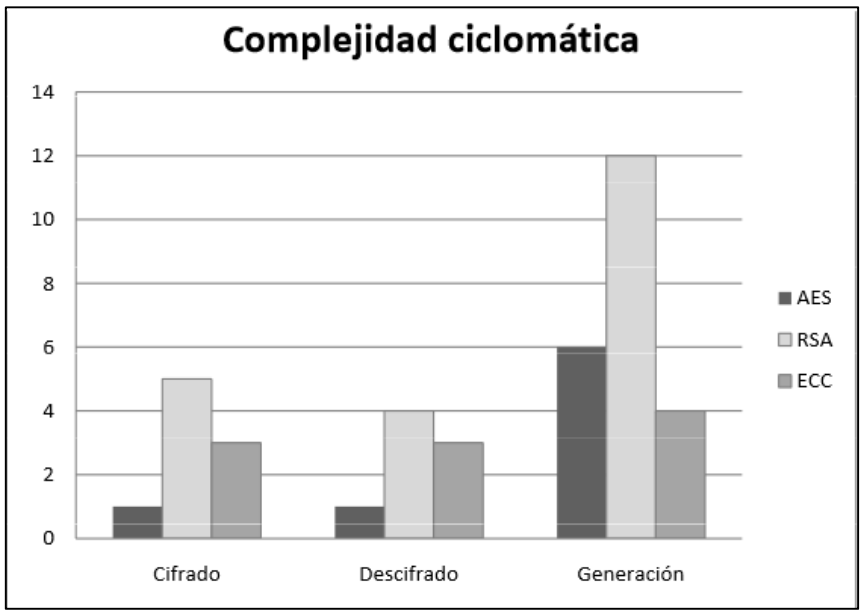


Figura 10: Comparación de la complejidad de AES, RSA y ECC [44]

La figura 7 muestra que la complejidad lógica del algoritmo RSA es mayor que ECC, tanto en la generación como en el cifrado (encriptación) y descifrado (desencriptación), esto se debe al proceso matemático que realiza al seleccionar números primos grandes y realizar una operación compleja. AES tiene una complejidad menor, por ser un algoritmo de criptografía simétrica y su proceso matemático consiste en elaboración de tablas de sustitución, mezcla de columnas e intercambio de matrices [44].

- Las redes de comunicaciones siguen avanzando en la implementación de medios seguros y protección de información, por ello que el uso de tarjetas inteligentes para accesos seguros, identificación y cualquier servicio que requiera seguridad son cada vez

[6] Complejidad Ciclomática: Es una métrica de software que proporciona una medición cuantitativa de la complejidad lógica de un programa. - http://es.wikipedia.org/wiki/Complejidad_ciclom%C3%A1tica

más comunes [37] . En la figura 9 se muestra una comparación entre la cantidad de compuertas lógicas que los algoritmos RSA y ECC requieren en el diseño electrónico –*chip*–, para su implementación [42]:

Algoritmo	Cant. de compuertas lógicas
RSA – 1024	34.000
ECC – 163	3.260
RSA – 3072	50.000
ECC – 283	6.660

Figura 11: Compuertas lógicas usadas en el diseño electrónico [42]

Se puede apreciar que la diferencia entre el requerimiento del número de compuertas de RSA y ECC es significativo. Esta diferencia permite establecer con claridad que el algoritmo ECC requiere menos tiempo en el procesamiento de señales, lo que significa que al momento de adquirir un procesador el costo no será elevado.

- En el año 2014, un grupo de investigadores entre los cuales se encuentra *Adi Shamir* –uno de los creadores del algoritmo RSA–, presentaron una investigación sobre un ataque para romper el algoritmo de encriptación en base a sonidos. Utilizan técnicas de criptoanálisis acústico para deducir la clave privada a partir del ruido que hace el computador cuando desencripta un mensaje [45]. Con este tipo de ataques denominados de canal lateral, ya no es relevante el tamaño de la clave, puesto que al ser un ataque a nivel de señales eléctricas existen más posibilidades de detectarlas. Siendo una amenaza para otros algoritmos similares a RSA, como son ElGamal y Diffie-Hellman.

5.3.4.1 Evaluación de los algoritmos

Una vez expuestos y analizados los diferentes parámetros de los algoritmos de criptografía asimétrica, se determinó que el algoritmo criptográfico de Curvas Elípticas (ECC), cumple con los parámetros de robustez y seguridad, dejando atrás al algoritmo RSA, que a pesar de ser el más popular de esta criptografía no cumple con las expectativas que la tecnología actual requiere.

5.4 Recomendación del mecanismo de encriptación para la seguridad de una red de telemedicina

La UIT propone que las TIC estén al servicio de las personas, de tal forma que se beneficien a través de servicios de educación, capacitación, salud, comercio,…. En el ámbito de la salud se han ido incrementado las redes de Telemedicina a nivel mundial, contando con personal especializado en cada una de las áreas estratégicas para que puedan prestar servicios de calidad a un sinnúmero de usuarios a través del envío de información médica, que permita al especialista establecer un diagnóstico correcto a pesar de la distancia. Con equipos y redes de comunicación que faciliten la transmisión de información clara y segura, manteniendo de esta forma la privacidad y la confianza entre el médico y el paciente. [46] A continuación se presentan algunas de las amenazas a las que están expuestas las redes de telemedicina:

Tabla 8: Clasificación de las amenazas que pueden producir un problema de seguridad en la organización [47]

Nivel	Clasificación de amenazas	Sanciones Legales[7]
1	Divulgación accidental. El trabajador, sin querer, revela información del paciente a otros. Por ejemplo, mensaje de correo electrónico enviado a la dirección incorrecta	**Art. 179**.-"*La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año".* **Art. 229**.- *"La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años".* ***Art. 181.-*** *"La persona que, con engaños o de manera clandestina, ingrese o se mantenga en morada, casa, negocio, dependencia o recinto habitado por otra, en contra de la voluntad expresa o presunta de quien tenga derecho a excluirla, será sancionada con pena privativa de libertad de seis meses a un año".* **Art. 190**.- "*La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años".*
2	Empleado curioso. Un trabajador con privilegios de acceso a los datos de un paciente accede a ellos por curiosidad o para sus propios fines. Por ejemplo, un profesional sanitario que accede a la información de salud de un compañero de trabajo.	
3	Violación de la privacidad de los datos por un trabajador. Miembro del personal que tiene acceso a la información de un paciente y la transmite al exterior con ánimo de lucro o por algún tipo de animadversión hacia un paciente.	
4	Violación de la privacidad de los datos por un externo con intrusión física. Un externo que entra en la instalación física y de manera forzada accede al sistema	
5	Intrusión no autorizada en la red del sistema. Un externo, ex empleado, paciente o hacker que se introduce en la red del sistema de la organización desde el exterior y accede a la información del paciente o hace que el sistema deje de funcionar (ataque a la disponibilidad)	

[7] Información tomada de la Ley Orgánica Integral Penal (2014)

En la tabla 8 se puede observar la clasificación de las amenazas que comúnmente existen en una organización cualquiera, a las que se ha asignado un nivel, siendo 1 el nivel más bajo y 4 el nivel más alto de amenaza, de ésta forma se establecen los requerimientos del sistema al momento de implementar los mecanismos de seguridad. Así también, cada una de estas amenazas se traduce en un acto ilegal dentro de la organización, por tal razón, se presentan además las sanciones legales que el estado ecuatoriano establece en el Código Orgánico Integral Penal para estos casos.

Para la implementación es importante conocer los organismos relacionados con la estandarización de los componentes que intervienen en una red de telemedicina, entre los que tenemos:

- La Comisión Europea y Comité Europeo de Normalización (CEN) a través del Comité Técnico CEN-TC251.
- El Comité Técnico AEN-CTN 139 de Normalización en Tecnologías de la Información y Comunicaciones para la Salud en España.
- *International Standards Organization* (ISO) e *Institute of Electrical and Electronics Engineering* (IEEE), organismos encargados de la estandarización y desarrollo en áreas técnicas.
- La Organización Internacional de Telecomunicaciones (UIT-T), permite garantizar y proteger la infraestructura de Telecomunicaciones y los servicios que prestan.

La estandarización y normalización en estas redes deben cubrir todos los ámbitos, es decir: infraestructura de comunicación, historia clínica, registros médicos, comunicación con dispositivos médicos, transmisión, seguridad y protección de datos. Las normas sobre seguridad

y protección de datos incluyen sistemas de certificados, claves públicas, y firma electrónica. Entre las normas y estándares podemos citar las siguientes [3]:

- El estándar HL7 (*Health Level Seven)*, acreditada por *American National Standards Institute* (ANSI), para el intercambio de datos clínicos en redes de telemedicina.
- Las norma DICOM (*Diggital Imaging and Comunication in Medicine*) para la comunicación de imágenes y su información asociada.
- La normas del IEEE (*Medical Bus*), utilizadas en la conexión en red de los equipos e instrumentos médicos para la automatización y el control, así como la interoperabilidad con los sistemas de información hospitalaria (HIS) y de historia clínica electrónica (HCE).
- Las normas que permiten revisar los requisitos de seguridad en redes de datos, para aplicar en redes de Telemedicina en la recomendación X.805 y X.1051 de la ITU-T.
- Las normas ISO 27000 diseñadas para administrar la seguridad de la información.

La implementación de seguridad en una red de telemedicina, debe cubrir las dimensiones de seguridad de la recomendación X.805 de la UIT-T. Debido a la información que se va a manejar en los centros hospitalarios y considerando el tipo de amenazas a las que se expone una red de telemedicina (Tabla 9), se debe diseñar los mecanismos de seguridad que permitan: control de acceso, autenticación, no repudio, confidencialidad, seguridad de la comunicación, integridad, disponibilidad y privacidad.

Por tal razón, se deben considerar algunas recomendaciones en función de los requerimientos para implementar los mecanismos de seguridad que permitan alcanzar niveles de seguridad adecuados en una red de éste tipo. Una vez evaluados los algoritmos de criptografía simétrica y asimétrica, y analizados parámetros como – velocidad de proceso, tiempo de ejecución, robustez, tamaño de clave,.. –. Se recomienda que para los procesos

de encriptación de los diferentes mecanismos que se apliquen se utilicen el algoritmo simétrico AES; y, el algoritmo asimétrico de curvas elípticas ECC.

Una red de Telemedicina está formada por enlaces de baja velocidad para conexiones dentro del centro hospitalario; y, enlaces de alta velocidad para la conexión entre los centros y sub centros. En la Figura, se muestra de manera general, los principales componentes de una red típica de telemedicina [46].

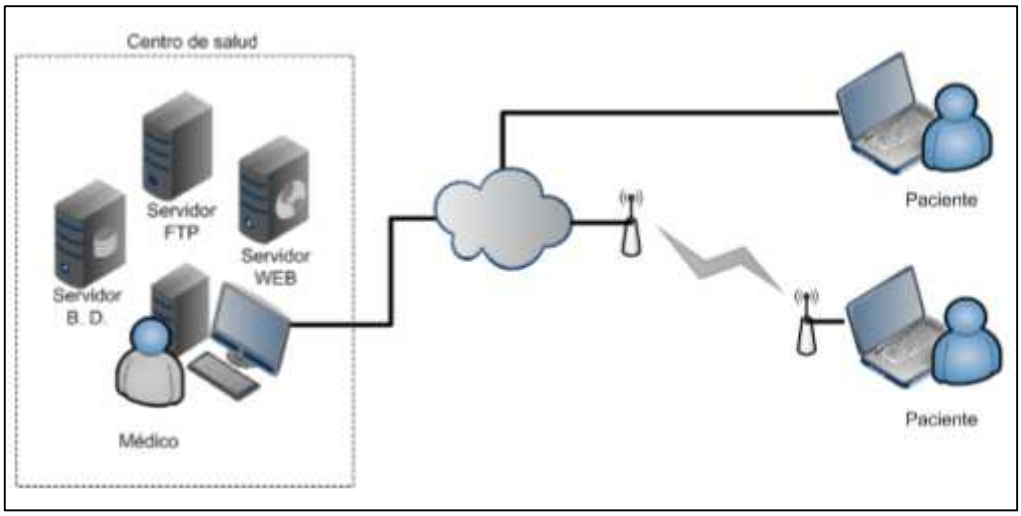


Figura 12: Típica red de telemedicina [46]

Existen varios parámetros que se deben considerar, para mantener los niveles de seguridad entre los que destacaremos los siguientes:

- Uso de contraseñas para la privacidad en el manejo de información. Las mismas que deben ser utilizadas de forma que no puedan ser suplantadas por otro usuario.
- En las redes de telemedicina es necesario utilizar certificados digitales donde se puede identificar al titular del certificado para intercambiar información. Así como la firma digital para mantener la integridad de la información que se envía. En estos casos puede utilizar algoritmo de criptografía asimétrica ECC.

- Para la navegación por Internet es recomendable utilizar el protocolo SSL, firewall y antivirus. Además de que se deben tomar en cuenta, aspectos como no descargar archivos de sitios desconocidos y no entregar datos personales en páginas no seguras.
- Otro aspecto a considerar respecto a la seguridad es el uso de dispositivos extraíbles, es recomendable encriptar con un certificado digital la información que salga del centro hospitalario.
- Para el caso de proteger información que se encuentra en el disco duro, se recomienda el uso de contraseñas, así como encriptar los datos sensibles de los pacientes, para lo que se puede aplicar el algoritmo de criptografía simétrica AES.

5.5 Análisis económico

Los mecanismos de seguridad utilizan algoritmos de encriptación, para garantizar la seguridad informática en las redes de comunicaciones. Para esto es importante establecer el tipo de tecnología que usará la red, la topología, los servicios que prestará, entre otros aspectos, y así establecer el costo de la inversión en seguridad de la red. Sin embargo, existen rubros establecidos por las entidades Certificadoras que permiten realizar una estimación económica en varios aspectos.

Para garantizar la seguridad de la información generada en los centros hospitalarios se manejan certificados digitales, los mismos que utilizan el estándar PKCS#12 (*Personal Information Exchange Syntax Standard*) para el archivo que contiene la información. Dichos archivos pueden ser almacenados en las siguientes tecnologías.

- **Tarjeta inteligente (*Smart Card*).-** Son dispositivos que contienen un chip –conjunto de circuitos integrados–, específicamente un microprocesador que permita almacenar información y usar mecanismos de encriptación y desencriptación como protocolo de comunicación segura[6]. En el caso de una red de telemedicina es aplicable para el

control de acceso en áreas restringidas, computadores, bases de datos, así como para almacenar los datos de pacientes (historia clínica) [27]. Las tarjetas inteligentes utilizan el estándar ISO7816 y son compatibles con las especificaciones EMV (*Europay MasterCArd VISA*) y GSM (Sistema Global para las Comunicaciones Móviles. La especificación EMV está diseñada como una alternativa para incluir criptografía de curvas elípticas [6].

- ***Token.-*** Es un dispositivo electrónico fácil de transportar, se utilizan para almacenar claves criptográficas (certificados digitales, huellas digitales). Pueden ser tokens generadores de contraseñas dinámicas llamados OTP (*One Time Passwords*); y, los conocidos como *tokens* USB, que permiten almacenar contraseñas y certificados digitales [27]. El costo del dispositivo y la emisión de firma electrónica se muestra en la tabla 9:

Tabla 9: Tarifas Emisión de Certificados - Token

Entidad Certificadora	Concepto	Valor en USD
BANCO CENTRAL DEL ECUADOR [8]	Emisión del Certificado de Firma Electrónica (token) - Vigencia 2 años	$ 30,00
	Dispositivo portable seguro – Token	$ 35,00
	Renovación del Certificado (válido por 2 años)	$ 20,00
DATA SECURITY [9]	Emisión del Certificado con Token Epass 3003 - Vigencia 2 años	$ 59,00
	Emisión del Certificado en Token propio - Vigencia 2 años	$ 27,50
	Renovación del Certificado (válido por 2 años)	$ 18,50
	EPASS3003	$ 31,50
	Epass1000	$ 24,00
	Safenet iKey2032	$ 24,00
	Biopass 3000	$ 31,50

[8] www.eci.bce.ec – Tarifas según Resolución Administrativa No.BCE-0038-2014 de 27/06/2014 (Precios no incluyen IVA)
[9] www.securitydata.net.ec

- ***Hardware Security Module (HMS).-*** Es un procesador diseñado para la administración, el procesamiento y el almacenamiento seguro de claves criptográficas. Este tipo de hardware se utiliza para autenticación, firma digital, procesos de encriptación y desencriptación especialmente en transacciones de altos volúmenes. El costo de este servicio se muestra en la tabla 10.

Tabla 10: Tarifas Emisión de Certificados - HSM

Entidad Certificadora	Concepto	Valor en USD
BANCO CENTRAL DEL ECUADOR	Emisión del Certificado de Firma Electrónica (HMS) - Vigencia 3 años	$ 90,00
	Renovación del Certificado (válido por 3 años)	$ 90,00
DATA SECURITY	CERTIFICADO para transacciones en gran volumen - el HSM debe ser soportado por nuestra plataforma	$ 507,00
	PRUEBAS EN HSM nuevo para comprobar soporte en nuestra plataforma	$ 147,00

El Banco Central del Ecuador presenta tarifas para emisión de certificados de firma electrónica en *archivo* –certificado estándar X.509, se puede integrar en cualquier sistema operativo– y, *roaming* –certificado almacenado en servidores ECIBCE, que puede realizar operaciones mediante el aplicativo ESP–.En la tabla 11 se muestran estos valores.

Tabla 11: Tarifas Archivo y Roaming – Banco Central del Ecuador

Concepto	Valor en USD
Emisión del Certificado de Firma Electrónica (Archivo)- vigencia 1 año	$ 20,00
Renovación del Certificado (válido por 1 año)	$ 15,00
Emisión del Certificado de Firma Electrónica (Roaming) - vigencia 2 años	$ 30,00
Renovación del Certificado (válido por 2 años)	$ 20,00
Aplicativo ESP (Entrust Security Provider) - Opcional Usuarios Roaming	$ 25,00

La empresa Data Security posee tarifas para el uso de Servidores con certificados SSL, en la figura se presentan los valores de diferentes tipos de certificados para 1, 2 y 3 años de vigencia.

CERTIFICADOS SSL			
Tipos de certificado	1 año	2 años	3 años
Estándar 256 Bits	$ 919,43	$ 1.654,97	$ 2.234,21
Advantage	$ 965,55	$ 1.737,99	$ 2.346,29
EV Multi dominio	$ 1.980,30	$ 3.564,54	$ -
UC Multi dominio	$ 1.472,93	$ 2.651,27	$ 3.579,22
Wildcard	$ 4.286,55	$ 7.715,79	$ 10.416,32
Firma de código	$ 1.242,30	$ 2.236,14	$ -
CDS Individual	$ 1.380,68	$ 2.485,22	$ 3.355,05
CDS grupo	$ 1.998,75	$ 3.597,75	$ 4.856,96
CDS Enterprise lite	$ 55.350,00	$ 99.630,00	$ 134.500,50
CDS Enterprise Pro	$ 69.187,50	$ 124.537,50	$ 168.125,63
Secure Mail Enterprise	$ 209,10	$ 376,38	$ 508,11
EV SANs Extra (dominios certificados)	$ 596,55	$ 1.073,79	$ -
UC SANs Extra (dominios certificados)	$ 199,88	$ 359,78	$ 485,71

Figura 13: Tarifas Certificados SSL – Data Security

Las entidades certificadoras no únicamente poseen tarifas para los diferentes tipos de certificados, además detallan los valores para un sinnúmero de servicios que ofrecen a los usuarios. En la tabla 12 se muestran algunos de ellos.

Tabla 12: Tarifas de Soporte y Servicios Adicionales de las Entidades Certificadoras

Entidad Certificadora	Tipo de servicio		Valor en USD
BANCO CENTRAL DEL ECUADOR	Sellado de Tiempo - Plan Anual Ilimitado		$ 250,00
	API Intisign para firma y sellado de tiempo		$ 1.000,00
	Aplicativo PDF Automatic Signer - PAS		$ 3.500,00
	Recuperación del certificado		$ 0,00
DATA SECURITY	Atención Express (Costo por persona -No incluye certificado ni token)	Servicio express simple	$ 91,00
		Servicio express plus (simple + soporte)	$ 182,00
	Visita Simple (Valor por máximo dos personas por hora o fracción)	Visita dentro del área urbana	$ 182,00
		Visita fuera del área urbana	$ 364,00
	Visita Plus (Valor por máximo dos personas por hora o fracción)	Visita dentro del área urbana	$ 364,00
		Visita fuera del área urbana	$ 728,00
	Validación de identidad ONLINE (No incluye el valor del certificado de firma electrónica)	Dentro del país	$ 182,00
		Fuera del país	$ 364,00
		En nuestras oficinas	$ 91,00

	Soporte Técnico (Valor por hora o fracción)	En sus instalaciones: Área urbana	$ 182,00
		En sus instalaciones: Fuera del área urbana	$ 364,00
		Soporte Remoto	$ 91,00
	Desbloqueos	Desbloqueo de token en sitio epass3003auto	$ 17,86
		Desbloqueo de token en sitio epass1000auto	$ 7,15
		Desbloqueo de token remoto epass3003auto	$ 31,25
	Actualización de datos	Soporte de actualización de datos	$ 17,86
		Revocación de certificados	$ 0,00

6. Conclusiones y Recomendaciones

6.1 Conclusiones

- La seguridad de la información sigue siendo un aspecto crítico en la redes de comunicaciones, por lo que se requieren de mecanismos que garanticen la confidencialidad, integridad y autenticidad de los datos transmitidos.
- Se ha establecido que el uso de las TIC's y el Internet crecen a pasos agigantados alrededor del mundo, lo que ha permitido que la tecnología esté innovando cada día. Sin embargo, el área de la criptografía ha mantenido sus algoritmos vigentes durante mucho tiempo, a pesar de que algunos de ellos ya han sido atacados, pero la popularidad que han alcanzado los hace difíciles de sustituir.
- En base al análisis de velocidad de encriptación se determinó que los algoritmos AES de criptografía simétrica y el de Curvas Elípticas ECC de criptografía asimétrica, son idóneos para utilizarlos como algoritmos de encriptación en mecanismos de seguridad en redes de comunicaciones.
- El algoritmo asimétrico de Curvas Elípticas posee características altamente seguras en robustez y tamaño de clave. Sin embargo no ha sido difundido adecuadamente por lo que existen muy pocas aplicaciones que lo utilizan.

- Del análisis realizado a los algoritmos asimétricos, se establece que ECC tiene tiempos en el procesamiento más bajos que los otros algoritmos, además de un significativo ahorro en el ancho de banda requerido.
- La comparación de la velocidad de proceso de los algoritmos simétricos, es un parámetro disponible en el software de encriptación que permite realizar una evaluación para establecer el algoritmo a seleccionar para una aplicación. Sin embargo, se ha demostrado que existen otros parámetros que influyen al momento de decidir uno u otro algoritmo.
- Otro aspecto de este análisis es que las investigaciones en los últimos años, han abierto la posibilidad de que los ataques se hagan a través de canales laterales y no únicamente desde la estructura matemática del algoritmo.

6.2 Recomendaciones

- Se recomienda que al momento de seleccionar algún mecanismo de encriptación, se considere que los algoritmos de criptografía asimétrica no reemplazan a los de criptografía simétrica, puesto que la aplicación de éstos dependerá del tipo de seguridad que requiera la red.
- Al momento de aplicar criptografía asimétrica es recomendable aprovechar las ventajas que presentan algoritmos como el de curvas elípticas y analizar la implementación de éste en los software de encriptación de código abierto.
- Antes de elegir un algoritmo de encriptación es necesario establecer si se puede aplicar en cualquier tipo de dispositivo y así facilitar la migración de tecnología cuando sea necesario.

7. Bibliografía:

[1] U. I. d. T. (UIT). (2014). *Índice de Desarrollo de las TIC*. Available: http://www.itu.int/net/pressoffice/press_releases/2014/68-es.aspx#.VSvg_5N1LcY
[2] A. F. M. Giraldoni, E. H. Barrio, T. d. C. R. Izaguirre, J. M. Torres, and A. S. Echevarría, "Problemas éticos y de seguridad asociados al uso de las tecnologías de la información y el conocimiento en Salud," *Medisur*, vol. 6, pp. 85-89, 2008.
[3] P. d. Toledo Heras, "Propuesta de un modelo de sistema de telemedicina para la atención sanitaria domiciliaria," Telecomunicacion, 2003.
[4] J. Cano, *Inseguridad de la Información*. Bogotá: Alfaomega, 2013.
[5] G. Escrivá Gascó, R. M. Romero Serrano, and D. J. Ramada, *Seguridad informática*: Macmillan Iberia, S.A., 2013.
[6] J. Gutiérrez and J. Tena, *Protocolos criptográficos y seguridad en redes*, 1a. ed. ed.: Universidad de Cantabria, 2003.
[7] J. J. Cano, "Inseguridad informática: un concepto dual en seguridad informática," *Revista de Ingeniería*, pp. 40-44, 2004.
[8] G. Álvarez Marañón and P. P. Pérez García, "Seguridad informática para empresas y particulares."
[9] J. F. Roa Buendía, *Seguridad informática*. España: McGraw-Hill España, 2013.
[10] A. Maiorano, *Criptografía. Técnicas de desarrollo para profesionales*, 1 ed. ed. Buenos Aires: Alfaomega Grupo Editor, 2009.
[11] R. A. Española, "Diccionario de la lengua española," ed, 2015.
[12] G. G. Paredes, "Introducción a la Criptografía," *Revista Digital Universitaria*, vol. 7, 2006.
[13] H. Zhao, "La seguridad de las telecomunicaciones y las tecnologías de la información," 2006.
[14] J. M. Luaces Novoa, "Seguridad en redes inalámbricas de área local (WLAN)," 2013.
[15] F. Andreu, I. Pellejero, and A. Lesta, *Fundamentos y aplicaciones de seguridad en redes WLAN*: Marcombo, 2006.
[16] T. d. C. Vivas Ríos, "Aplicacción de mecanismos de seguridad de informción en la red de telemedicina de los municipios de Baruta- El Hatillo," Magíster en Ingeniería Biomédica, Ingeniería Electrónica, Universidad Simón Bolívar, Venezuela, 2010.
[17] S. H. Chiu, "Seguridad en Redes Inalámbricas 802.11," ed: Obtenido de http://www. ciens. ucv. ve.
[18] S. Barajas, "Protocolos de seguridad en redes inalámbricas," *Universidad Carlos III de Madrid*, 2004.
[19] L. E. Hernández, C. Carreto, R. Menchaca, E. S. de Cómputo, and D. México, "Modelo de Seguridad para Redes Aplicado a Dispositivos Móviles," *RISCE Revista Internacional de Sistemas Computacionales y Electrónicos*, p. 21, 2012.
[20] W. Willems and I. Gutiérrez García, *Una introducción a la criptografía de clave pública*, 2a. ed. ed. Colombia: Universidad del Norte, 2010.
[21] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*: CRC Press, 1996.
[22] J. Ramió, *Libro Electrónico de Seguridad Informática y Criptografía versión 4.1*. Madrid-España: Universidad Politécnica de Madrid, 2006.
[23] A. Fúster, D. de la Guía, L. Hernandez, F. Montoya, and J. Muñoz, *Técnicas criptográficas de protección de datos*, 2da ed. ed.: Alfaomega & RA-MA, 2001.
[24] J. M. G. Salas, "Implementación en un FPGA del algoritmo de encriptación Doble Ronda como una solución al Teorema LR," 2008.

[25] M. Lucena López, "Criptografía y Seguridad en Computadoras," *Versión 0.6. 2) Universidad de Jaén*, 2005.
[26] C. D. Carbonell, Rodrigo. Mejías, Pablo., "Eficiencia de la Criptografia de Curva Elíptica y RSA para enfrentar los nuevos requerimientos de Seguridad en Internet," Ingeniero Civil en Computación e Informática., Facultad de Ciencias Físicas y Metemáticas, Universidad Central de Chile, Santiago de Chile, 2007.
[27] T. Vivas, M. Huerta, A. Zambrano, R. Clotet, and C. Satizábal, "Aplicación de Mecanismos de Seguridad en una Red de Telemedicina Basados en Certificados Digitales," in *IV Latin American Congress on Biomedical Engineering 2007, Bioengineering Solutions for Latin America Health*, 2008, pp. 971-974.
[28] H. R. Peñaranda Quintero, "La firma electrónica digital en Venezuela. Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas. Vol 29, No 1 (2011)."
[29] *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de atos*, 2002.
[30] S. N. d. l. A. Pública. (2014, 18/03). *¿Quién emite la firma electrónica?*
[31] H. Zhao, "La seguridad de las telecomunicaciones y las tecnologías de la información."
[32] D. E. M. R. P. ALFARO, "ANÁLISIS Y MEJORA DEL RENDIMIENTO DEL ALGORITMO AES PARA SU UTILIZACIÓN EN TELÉFONOS MÓVILES."
[33] J. d. J. A. Angel, "Criptografía para principiantes," *Obtenido en la Red Mundial el*, vol. 5, 2000.
[34] M. Astilla, "Diseño de un esquema de comunicación utilizando como criptosistema simétrico a TripleDES y asimétrico a RSA," Maestría en Tecnología de Cómputo, Instituto Politécnico Nacional, 2009.
[35] M. Farley, T. Stearns, and J. Hsu, *Guía LAN Times de seguridad e integridad de datos*: McGraw-Hill Interamericana de España, 1997.
[36] R. d. M. García, "Criptografía clásica y moderna."
[37] D. E. M. R. P. Alfaro, "Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles," 2014.
[38] E. d. i. d. E. Latinoamérica. (2014) Tendencias 2014: El desafío de la privacidad en Internet. Available: http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf
[39] G. Lehembre, "Seguridad Wi-Fi–WEP, WPA y WPA2," *Recuperado el*, vol. 9, 2006.
[40] E. Bonilla Palencia, "Implementación del algoritmo AES sobre arquitectura ARM con mejoras en rendimiento y seguridad," 2012.
[41] A. Pousa, V. M. Sanz, and A. E. De Giusti, "Análisis de rendimiento de un algoritmo de criptografía simétrica sobre arquitecturas multicore," in *XVII Congreso Argentino de Ciencias de la Computación*, 2011.
[42] C. Carbonell, R. Díaz, and P. Mejías, "Eficiencia de la Criptografia de Curva Elíptica y RSA para enfrentar los nuevos requerimientos de Seguridad en Internet," Facultad de Ciencias Físicas y Metemáticas, Universidad Central de Chile, Santiago de Chile, 2007.
[43] G. Belingueres, "Introducción A Los Criptosistemas de Curva Elíptica," *Obtenido en la Red Mundial el*, vol. 5, 2000.
[44] F. A. Maldonado López, "Modelo de seguridad para datos y servicios de telecomunicaciones sobre redes de distribución de energía eléctrica - PLT," 2009.
[45] D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology–CRYPTO 2014*, ed: Springer, 2014, pp. 444-461.

[46] E. P. G. Pinto, L. J. R. López, and E. P. E. Cuesta, "ANÁLISIS DE SEGURIDAD PARA EL MANEJO DE LA INFORMACIÓN MÉDICA EN TELEMEDICINA SECURITY ANALYSIS FOR MEDICAL INFORMATION MANAGEMENT IN TELEMEDICINE," 2011.

[47] A. Sánchez-Henarejos, J. L. Fernández-Alemán, A. Toval, I. Hernández-Hernández, A. B. Sánchez-García, and J. M. C. de Gea, "Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria," *Atención Primaria*, vol. 46, pp. 214-222, 2014.