Criptografía en la Seguridad de la Red en Sudamérica

Cryptography in Network Security in South America

Angely Mendez Cruz
Universidad Nacional de Trujillo. Perú
t052701020@unitru.edu.pe
https://orcid.org/0000-0002-9256-8044

Ciara Mendez Cruz
Universidad Nacional de Trujillo. Perú
t022700920@unitru.edu.pe
https://orcid.org/0000-0002-8232-5188

Angie Recalde Monzón
Universidad Nacional de Trujillo. Perú
t512700720@unitru.edu.pe
https://orcid.org/0000-0002-1553-8212

Valentina Padilla Leyva
Universidad Nacional de Trujillo. Perú
t032700320@unitru.edu.pe
https://orcid.org/0000-0002-9560-4565

Resumen

La existencia de redes de comunicación, específicamente de Internet, ha abierto nuevas posibilidades para el intercambio de información y al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite. Es necesario entonces, crear diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, todo ello es parte de una nueva tecnología denominada Criptografía. El presente artículo es una revisión sistemática referente al problema que existe de seguridad de redes donde se asevera que la criptografía es una de las herramientas más importantes y poderosas dentro del área de la Seguridad de Red que aporta gran valor y seguridad a nuestra sociedad. Este artículo se inicia con la seguridad en la red, sus tipos, protocolos y niveles para reconocerlos frente a un ataque en la red. Posteriormente, se centra en la Criptografía, su clasificación, protocolos y principios para salvaguardarla. Luego, se describen aplicaciones desarrolladas acerca de la Criptografía en la Seguridad de la Red en distintos países de Sudamérica. Finalmente, se describen brevemente las conclusiones.

Palabras clave

Criptografía; Datos; Informática;Red; Seguridad.

Abstract

The existence of communication networks, specifically the Internet, has opened new possibilities for the exchange of information and at the same time, the threats to the

security of the information transmitted are increasing. It is therefore necessary to create different mechanisms aimed at guaranteeing the confidentiality and authenticity of electronic documents, all of which is part of a new technology called cryptography. This article is a systematic review of the existing problem of network security where it is asserted that cryptography is one of the most important and powerful tools in the area of network security that brings great value and security to our society. This article starts with network security, its types, protocols and levels to recognize them in the face of a network attack. Next, it focuses on Cryptography, its classification, protocols and principles to safeguard it. Then, applications developed about Cryptography in Network Security in different countries of South America are described. Finally, conclusions are briefly described.

Keywords
Cryptography; Data; Security; Computing; Network.

Introducción
Desde que el internet apareció brinda servicios esenciales de comunicación entre decenas de millones de personas y está siendo cada vez más utilizado como una herramienta para la educación, el comercio, por lo que la seguridad se convierte en un tema importante a tratar. Y surge la inseguridad de los sistemas informáticos y de las redes, que va más allá de los virus informáticos conocidos.

Así lo indica [1] que, la protección es una *prioridad* para cualquier empresa o institución. Los atacantes a una red no necesitan estar en contacto físico con la víctima; los datos pueden ser fácilmente copiados, transmitidos, modificados o destruidos cuando son transmitidos por la red, si no se dispone de los mecanismos de protección adecuados. Según [6], existen muchos aspectos de la seguridad y muchas aplicaciones, que van desde comercio seguro, pagos a las comunicaciones privadas y la protección de contraseñas. Un aspecto esencial para las comunicaciones seguras es a través de criptografía.

El objetivo principal de este documento es proporcionar una revisión sistemática con enfoque territorial en Sudamérica de la criptografía en la seguridad de la red, con especial atención y énfasis en los trabajos aplicativos predecesores. La justificación y elaboración del presente trabajo es porque queremos informar, orientar e instruir a profesionales, estudiantes y público lego respecto al tema a desarrollar, tal como lo señala [10] que, la criptografía es una herramienta que juega un papel vital en la seguridad de la red, asegurando la confidencialidad e integridad de los datos y proporcionando autenticación.

En cuanto al contenido del documento cuenta con dos orientaciones principales. El primero, definir algunos términos relacionados con la criptografía y seguridad de la red. El segundo, proporcionar algunos antecedentes (resúmenes de estudios previos), en sudamérica, reales de la criptografía en la seguridad de redes.

Criptografía y Seguridad de la Red

Sobre el tema de estudio se realizó una revisión bibliográfica. La revisión se realizó en dos niveles: primero, desde la perspectiva de la seguridad de redes en general y segundo, dirigida particularmente al tema de la criptografía en la seguridad de la red. Así, mediante una búsqueda, se obtuvo una gran cantidad de documentación general y específica que permitieron ubicar y comprender mejor al objeto de estudio particular, es decir, la Criptografía en la Seguridad de Redes en Sudamérica.

1. Seguridad de la Red

1.1. Definición

La definición y el objetivo de la seguridad en redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado.[3]

Es la operación de proteger datos, aplicaciones, dispositivos y sistemas conectados a una red. Se encarga de proteger los sistemas de malware/ransomware, ataques distribuidos de denegación de servicio (DDoS), intrusiones, entre otros, de manera que utilicen una plataforma segura para los usuarios.

1.2. Tipos de Seguridad de Red

1.2.1. Protección Firewall

El Firewall es un programa de software o de un dispositivo que evita que otros usuarios no autorizados puedan acceder a su red, impiden el tráfico sospechoso y permite que fluya el tráfico permitido.

1.2.2. Detección de intrusiones (IDPS)

Estos sistemas se implementan mediante un firewall como una segunda capa de defensa, un sistema IDPS avanzado puede utilizar aprendizaje automático para analizar los datos entrantes continuamente y así activar un proceso automatizado.

1.2.3. Control de acceso a la red (NAC)

Utilizado para examinar un dispositivo como una laptop o smartphone asegurándose de que cuente con la protección antivirus, el nivel de actualización del sistema y configuración adecuada antes de que ingrese a la red y pueda acceder a archivos o datos.

1.2.4. Seguridad en la nube

Protege los recursos en línea, es decir, datos, aplicaciones, IP virtualizados y servicios en caso de filtración, pérdidas o robo de esta información, la seguridad en la nube incluye otros método de seguridad como la arquitectura de firewall, los controles de acceso, las redes privadas virtuales (VPN), la encriptación o enmascaramiento de

datos, el software de inteligencia de amenazas y los programas de recuperación de desastres.

1.2.5. Redes privadas virtuales (VPN)

Es un software encargado de proteger la identidad del usuario mediante un cifrado de datos y el enmascaramiento de la dirección IP y la ubicación, al usar una VPN, se conecta a un servidor seguro, el cual se conecta a Internet.

1.2.6. Prevención de pérdida de datos (DLP)

Son herramientas que garantizan que usuarios entre sí no compartan información confidencial intencionalmente o no fuera de una red corporativa, de manera que monitorean y controlan la actividad en una red corporativa o en la nube.

1.2.7. Gestión unificada de amenazas (UTM)

Los dispositivos UTM permiten que una organización reduzca costo y empleando firewalls, VPN, IDS y otras herramientas mejora la capacidad de protección y monitoreo de la red.

1.2.8. Puerta de enlace web segura

Este tipo evita el tráfico de red no autorizado a la red interna, además protege al usuario al acceder a sitios web maliciosos que contengan virus o malware.

1.3. Protocolos de Seguridad

1.3.1. El protocolo de Internet 6

El Protocolo de Internet en su versión 4 (IPv4) fue creado cuando se pensaba que su número máximo de direcciones posibles que es de alrededor de 4 mil millones de direcciones; pero al ritmo que ha avanzado la tecnología y dadas las facilidades para tener una computadora conectada a la red esta cifra se alcanzará en esta misma década, entonces se pensó también que el sucesor del IPv4 debería tener capacidades para poder asegurar la transferencia de paquetes para evitar los principales ataques que se gestan en la red. A manera de solucionar todas estas dificultades que se han presentado con el paso de los años un nuevo protocolo, el IPv6. [11]

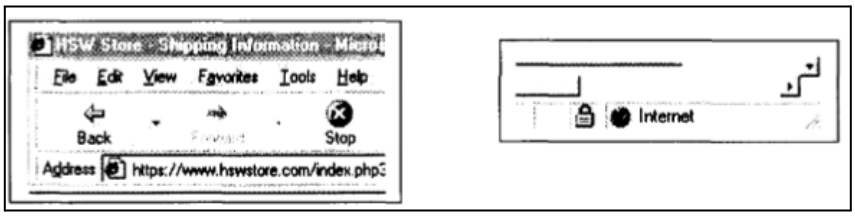
Cisco Systems ha diseñado ruteadores IOS (Internetworks Operating Systems) los cuales también incluyen el soporte para IPv6, este es un hecho muy importante ya que los ruteadores de Cisco portan el 80% del tráfico principal de Internet. La compañía Microsoft también ha incluido un previo de tecnología de desarrollador IPv6 en el Service Pack para Windows 2000 y el soporte del IPv6 de igual manera está presente en la versión del Explorador de Internet para Windows XP.

1.3.2. SSL & TLS (Secure Socket Layer & Transport Layer Secure)

Secure Socket Layer es el protocolo de seguridad de internet para conexiones punto a punto. Desarrollado por Netscape, es utilizado por exploradores de Internet y servidores de Red. Ofrece protección contra incursiones, forjado o el tampering. Clientes y servidores son capaces de identificarse uno al otro y establecer un enlace

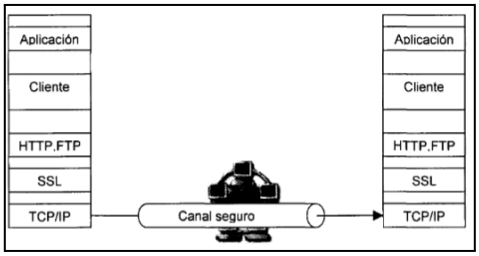
seguro o "tubería" que atraviesa la Internet o una red local para que los datos sean transferidos de manera segura.[11]
En nuestro explorador podemos ver si estamos usando un protocolo de seguridad tal como TLS en diferentes maneras. Se puede apreciar en la línea de dirección es reemplazada con las iniciales "https" y también con un pequeño candado en la barra de estado en la parte de abajo del explorador. En la Figura 1 se ve un ejemplo.

Figura 1
Seguridad en el explorador



El protocolo SSL es análogo a una llamada telefónica en una línea segura entre dos computadoras en cualquier red incluyendo la internet. En SSL la conexión es establecida, las partes autenticadas y la información transferida con seguridad. A la última mejora de este protocolo se le llamó TLS.

Figura 2
Conexión SSL



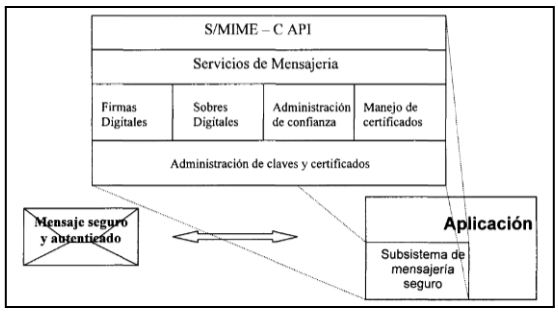
En aplicaciones utilizando SSL, se utilizan fuertes medidas de encriptación para asegurar la confidencialidad. Por medio del uso de certificados digitales, SSL provee de la autentificación transparente de servidores y de manera opcional, de los clientes. SSL utiliza el algoritmo RSA como el algoritmo encargado de manejar la seguridad utilizando firmas digitales y sobres digitales.

1.3.3. S/MIME

S/MIME es el protocolo encargado de ofrecer la privacidad necesaria a los negocios electrónicos de la Red, ofreciendo los servicios de autenticidad y privacidad. S/MIME utiliza la encriptación por llave pública para evitar que los mensajes sean interceptados. La analogía de la protección ofrecida por S/MIME es de un correo postal enviado entre dos lugares de manera segura. El protocolo garantiza la aseguración del mensaje, la autenticación, el almacenamiento y la transmisión de los datos secretos.

Figura 3

Conexión SSL



1.4. Niveles de Seguridad

Se propuso la siguiente clasificación más utilizada a nivel internacional que es el TCSEC Orange Book (Trusted Computer System Evaluation Criteria) por el Departamento de Defensa de los Estados Unidos (DoD), este es un estándar que establece los requisitos básicos que evalúan la eficacia de los controles de seguridad informática integrados en un sistema informático , cada nivel impone ciertos límites y condiciones que un sistema debe tener en cuenta para lograr un esquema de seguridad en Hardware. Software o en Datos[12].

1.4.1. Nivel D1

Es la seguridad básica, se caracteriza por la falta de protección del hardware, además de un sistema operativo vulnerable y la falta de autenticación de red y derechos por parte de los usuarios. En este nivel, se encuentra MS-DOS, Windows(3.x,95 y 98).

1.4.2. Nivel C1

Se le conoce como nivel de seguridad discrecional, se caracteriza por poseer el sistema operativo UNIX básico, por lo que tiene cierto nivel de protección a hardware y los usuarios deben de registrarse en el sistema con un nombre y contraseña para poder acceder.

1.4.3. Nivel C2

En este nivel se reconoce a Windows NT, se caracteriza por el refuerzo en las restricciones de usuarios al ejecutar comandos de acceso, permite especificar los niveles de acceso a los archivos, además requiere de auditorías del sistemas con la correspondiente creación de registros.

1.4.4. Nivel B1

Llamado Protección de Seguridad Etiquetada, se caracteriza por trabajar bajo control de acceso a “objetos”.

1.4.5. Nivel B2

A este nivel se le conoce Protección Estructurada, cada dispositivo se caracteriza por tener un nivel de seguridad bajo o alto, así como también en este nivel se establece pautas de comunicación de un objeto entre diferentes niveles de seguridad.

1.4.6. Nivel B3

Llamado también Dominio de Seguridad, se caracteriza por reforzar con la instalación de hardware de seguridad, adicionalmente, establece rutas seguras en las comunicaciones del usuario por lo que requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

1.4.7. Nivel A

Conocido como Nivel de Diseño Verificado, incluye procesos de diseño, control y verificación mediante métodos matemáticos. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos de equipamiento.

2. Criptografía

2.1. Definición

Según el Diccionario de la Real Academia, la palabra criptografía proviene de la unión de los términos griegos *oculto* y *escritura*, y su definición es: "*Arte de escribir con clave secreta o de un modo enigmático*". [2] Obviamente la criptografía hace años que dejó de ser un arte para convertirse en una técnica, que trata sobre la protección de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Teoría de Números o Matemática Discreta, que estudia las propiedades de los números enteros, y la Complejidad Algorítmica.

Existen dos trabajos fundamentales sobre los que se apoya prácticamente toda la teoría criptográfica actual. Uno de ellos, desarrollado por Claude Shannon en sus artículos "A Mathematical Theory of Communication" (1948) y "Communication Theory of Secrecy Systems" (1949) y el segundo, publicado por Whitfield Diffie y Martin Hellman en 1976, se titulaba "New directions in Cryptography".

2.2. Clasificación de los sistemas criptográficos

Los sistemas criptográficos se clasifican de acuerdo a tres factores que son independientes.

2.2.1. Tipo de operación para transformar el texto

Se refiere a cuando el texto claro es transformado a texto cifrado mediante los algoritmos de cifrado que se basan principalmente en la sustitución de cada elemento del texto claro por un elemento diferente y en la transposición de cada elemento del texto claro para su reordenamiento, todo ello ocurre sin perder la información.

2.2.2. Número de claves usadas

Se clasifica de acuerdo al emisor y el receptor de dos tipos: simétrico y asimétrico. Simétrico o de clave secreta es cuando el emisor y el receptor comparten la misma clave, es decir, la clave es igual tanto para cifrar y descifrar. Y es asimétrico o de clave pública cuando el emisor y el receptor utilizan claves diferentes, es decir, una clave para cifrar y otra para descifrar.

2.2.3. La forma de procesar del texto claro

Un cifrado en bloque se refiere a que recibe como entrada bloques de elementos y de acuerdo a ello, su salida también produce un bloque de elementos por cada entrada. Así mismo, un cifrador de flujo procesa los elementos de entrada de forma continua por lo cual su salida evidencia de un elemento cada vez.

2.3. Protocolos criptográficos

Los protocolos criptográficos son utilizados por los algoritmos criptográficos, dando respuesta a diferentes objetivos[4]. Si bien es cierto, existen una amplia variedad de protocolos, pero solo citaremos los más principales.

1. *Protocolo de Autentificación del Usuario:* Permite garantizar que el receptor de un mensaje es realmente quién pretende ser.
2. *Protocolos de Autentificación del Mensaje:* Garantiza la integridad del mensaje enviado.
3. *Protocolos para Compartir Secretos:* Distribuir un secreto entre un conjunto de participantes, de forma que ciertos subconjuntos prefijados de los participantes puedan acceder uniendo sus particiones y así recuperar dicho secreto.
4. *Transacciones Electrónicas Seguras:* Permite realizar las transacciones electrónicas de manera segura.
5. *Pruebas de Conocimiento Cero:* Permite que un individuo convence a otro de que posee cierta información, sin revelar nada sobre el contenido de la misma.
6. *Transferencias Transcordadas:* Permite que el emisor envíe un mensaje o secreto al receptor entre dos posibles, por lo cual el emisor no conoce cuál de las dos ha recibido realmente el receptor.
7. *Elecciones Electrónicas:* Garantiza la privacidad de cada sufragante e imposibilita el fraude electoral.
8. *Compromiso de bit:* Tras escoger una elección no se revele hasta un momento posterior garantizando que no se cambie la elección por otra parte.

2.4. Principios a salvaguardar en la criptografía

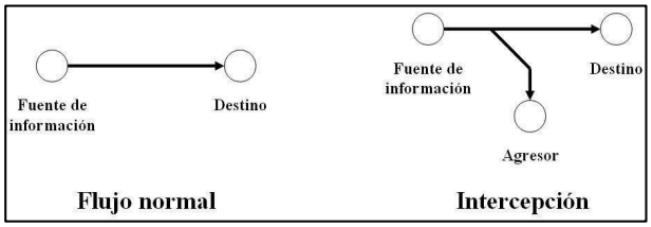
La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican, el objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. En efecto y bajo las premisas previamente mencionadas, de acuerdo a [7], un sistema criptográfico busca salvaguardar las siguientes características:

2.4.1. Confidencialidad

La confidencialidad asegura que la información sólo sea accesible para entidades autorizadas. Esta característica está expuesta a un ataque de seguridad clasificado como intromisión pasiva o intercepción, en donde alguien, sin interferir o alterar un mensaje que no está dirigido a él, logra captarlo y enterarse de su contenido. Esto se logra en mensajes de radio de manera muy simple, o en telefonía, por ejemplo, interviniendo una línea (Ver Figura 4):

Figura 4

Interceptación de mensajes



Nota. Introducción a la criptografía.

2.3.2. Autentificación

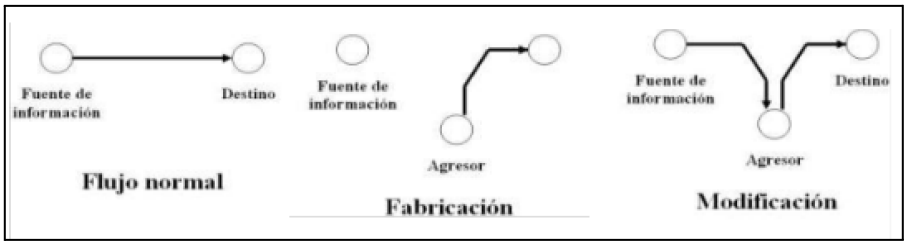
Asegura que el origen de la información sólo sea accesible para entidades autorizadas. Esta característica está expuesta a un ataque clasificado como intromisión activa de tipo inserción o fabricación en la cual una entidad no autorizada inserta información en el sistema, un ejemplo de autenticación son los famosos login.

2.4.3. Integridad

La tercera característica de la criptografía es la integridad, la cual asegura que sólo entidades autorizadas tienen acceso a la modificación de la información transmitida, esta característica está expuesta a un ataque clasificado como intromisión activa de tipo modificación en la cual una entidad no autorizada no sólo tiene acceso a la información sino que lleva a cabo una alteración de la misma. Los ataques a la integridad de un determinado mensaje o documento, básicamente consisten en la modificación del mensaje original, por ejemplo: si A envía el mensaje “Hola” a B, el agresor intercepta dicho mensaje y lo puede alterar, otro caso también conocido consiste no solo en la alteración del mensaje, sino en la creación de nuevos mensajes, desencadenando malos entendidos entre emisor y receptor. Ambos casos son ilustrados en la siguiente imagen (Ver Figura 5):

Figura 5

Interceptación de mensajes



Nota. Introducción a la criptografía.

2.4.4. Vinculación

Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado, es decir se asegura que ni el receptor ni el transmisor puedan negar que se efectuó una transmisión. Cuando se trata de una persona, se

trata de asegurar su conformidad respecto a esta vinculación (content commitment) de forma que pueda entenderse que la vinculación gestionada incluye el entendimiento de sus implicaciones por la persona. Antiguamente se utilizaba el término "No repudio" que se está abandonando, ya que implica conceptos jurídicos que la tecnología por sí sola no puede resolver. En relación con dicho término se entendía que se proporcionaba protección frente a que alguna de las entidades implicadas en la comunicación, para que no pudiera negar haber participado en toda o parte de la comunicación, para conseguirlo se puede usar por ejemplo firma digital. En algunos contextos lo que se intenta es justo lo contrario: poder negar que se ha intervenido en la comunicación, por ejemplo cuando se usa un servicio de mensajería instantánea y no queremos que se pueda demostrar esa comunicación, para ello se usan técnicas como el cifrado negable.

Aplicaciones y/o Investigaciones de la Criptografía en la Seguridad de la Red en Sudamérica

Para sustentar este trabajo y detallar el tema, se realizó una búsqueda bibliográfica en medio de la literatura informática de varias fuentes sobre temas enfocados en seguridad de la red y criptografía en algunos países de Sudamérica incluyendo Perú. También se realizaron consultas en artículos y trabajos de conclusión de cursos y/o grados, así como exploraciones en sitios de internet especializados. A continuación se presentan algunas.

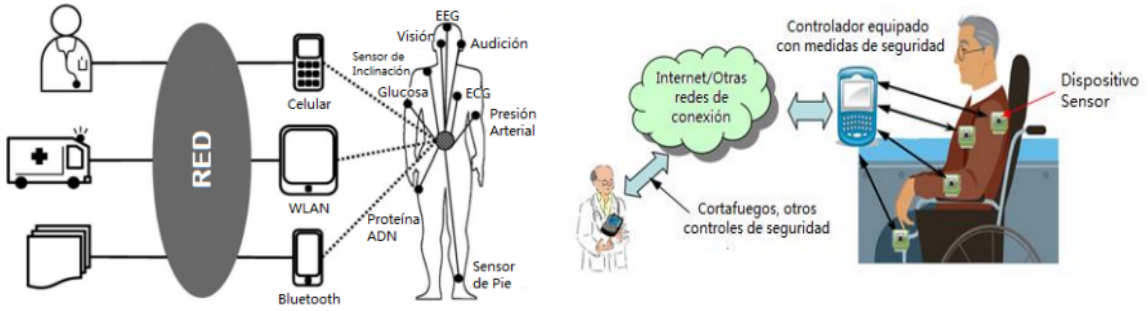
Una investigación titulada “**Criptografía De Curva Elíptica Aplicada A Seguridad Para Redes Wban Bajo La Norma IEEE 802.15.6”**, desarrollado por [5], en la Universidad de Santiago de Chile. Este trabajo presenta un Sistema de Seguridad basado en Criptografía de Curva Elíptica aplicado a Redes de Área Corporal Inalámbricas (WBAN: Wireless Body Area Network) fundamentado en la Norma IEEE 802.15.6.

El documento ofrece en primer lugar el concepto, aplicaciones y características de WBAN, así como los retos, tipos de ataques y los requerimientos de seguridad que éstas exigen.

WBAN, están formadas por nodos de sensores de bajo consumo, inteligentes, miniaturizados, invasivos/no invasivos de micro y nano tecnología ubicados estratégicamente dentro o alrededor del cuerpo humano, que recolectan los datos de los parámetros vitales del cuerpo de un paciente para posteriormente ser procesados y trasladados a bases de datos médicas. El uso de una WBAN permite monitoreo continuo de parámetros fisiológicos proporcionando mayor movilidad y flexibilidad a los pacientes sin causar ninguna molestia. Los datos se monitorizan a distancia, de forma continua y en tiempo real. Esta información médica es compartida para el personal médico, investigadores y compañías de seguros, tal como se muestra en la Figura 6.

Figura 6

Concepto de una WBAN para aplicaciones en el cuidado de la salud.



La versión aprobada del Estándar IEEE 802.15.6 fue ratificada en febrero del 2012 y sus objetivos son "*desarrollar un estándar de comunicación para dispositivos de bajo consumo y operación sobre, dentro o alrededor del cuerpo humano …*" [5].

Posteriormente se presenta un análisis comparativo de los sistemas criptográficos asimétricos RSA(Rivest, Shamir y Adleman) y ECC(Criptografía de Curva Elíptica).

Definiendo que RSA es un sistema criptográfico de clave pública, su seguridad radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, el funcionamiento en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Mientras que, el criptosistema RSA se basa en la suposición de que la factorización es una tarea computacionalmente difícil. Esto significa que dado suficiente tiempo y recursos computacionales, un adversario no debe ser capaz de "romper" RSA (obtener una clave privada) por factorización. Y al comparar las características de rendimiento de los algoritmos, se indican las ventajas que presenta ECC sobre RSA. Donde ECC ofrece seguridad equivalente a RSA utilizando tamaños de clave mucho más pequeñas, las actuaciones se ensayaron de acuerdo a como se indica en la Tabla 1, de la cual se puede decir que ECC tiene longitudes de claves mucho más cortas, los requisitos de ancho de banda y memoria son más pequeños, factor crucial en algunas aplicaciones con limitada memoria y potencia de procesamiento (WBAN).

Tabla 1. *Tamaños de Clave (en bits)*

Simétrico	ECC	RSA
80	163	1024
112	233	2240
128	283	3072
192	409	7680
256	571	15360

Fuente: [5]

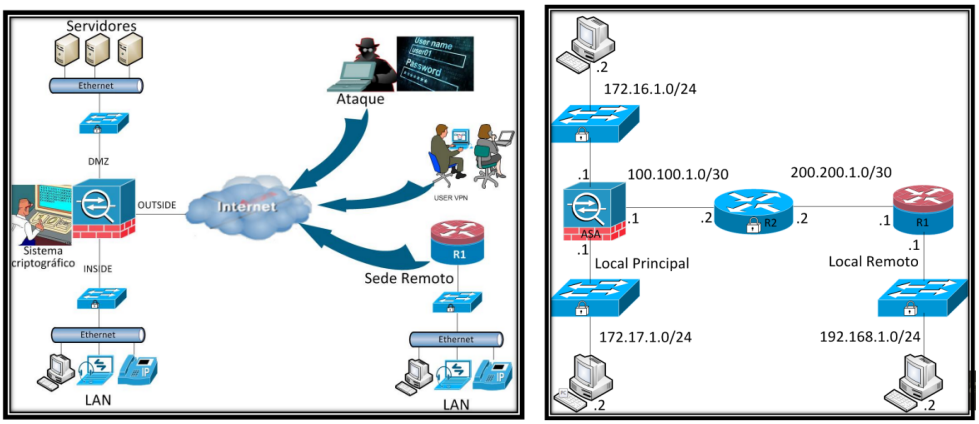
Finalmente, dentro de las conclusiones se desarrolla un análisis que perfila como una de las mejores técnicas a emplear, a la Criptografía de Curva Elíptica supliendo los retos de seguridad y como una solución de seguridad aplicada a WBAN.

Otra investigación para optar el grado de fin de la carrera de Ingeniería de Sistemas, es la "**Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática**", desarrollado por [8], en la Universidad Señor de Sipán de Chiclayo - Perú.

El tema de esta tesis es desarrollar una alternativa de sistema de seguridad para la red informática del Instituto Abaco, utilizando un prototipo, simulado en GNS3. El sistema utiliza algoritmos avanzados para la encriptación y desencriptación de los paquetes de información enviados en la entidad de estudio para la protección de datos privados del usuario. Además, el sistema puede extenderse para incorporar encriptación basada en más algoritmos de este tipo, tal como se muestra en la Figura 7.

Figura 7

Diagrama Contextual y Topológico del Sistema Criptográfico.



El desarrollo de este trabajo consiste en un estudio de las componentes a usar, tanto de hardware como de software, incluyendo los conceptos básicos necesarios para su diseño y operación, así como los estándares y metodologías que siguen.
Se realizó el diagnóstico del estado actual en ese momento de la seguridad perimetral de la red informática, para determinar cómo se lleva a cabo la gestión de la red y así poder tomar decisiones en el desarrollo del proyecto, debido a que las nuevas tecnologías como Internet han transformado los modelos de negocio, y por ello ha decidido transformar su infraestructura de seguridad.

Como resultado de la implementación, el sistema criptográfico proporciona la autenticidad del origen del mensaje, garantizando al receptor que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo. También se concluyó la identificación de los factores influyentes en la seguridad perimetral de una red informática. El cual permitió reestructurar el diseño dando como resultado un diseño centralizado, escalable y seguro.

La siguiente investigación es para optar el grado de Ing. de Sistemas mediante la tesis titulada, "**Aplicación móvil android para proteger información por medio de criptografía simétrica**", en la Universidad Autónoma de Bucaramanga - Colombia, desarrollado por [8].

La cual surge tras la amenaza de seguridad de los dispositivos móviles y su aumento, ya que Kaspersky Lab detectó casi 3.5 millones de componentes de malware en más de un millón de dispositivos móviles de usuarios donde el malware móvil usa un código de distribución nativo en sistemas operativos móviles populares, como iOS y Android que distribuyen datos valiosos a través de las redes empresariales sin levantar sospechas.

Entonces, como solución, se desarrolló un aplicación móvil Android que cifra diferentes tipos de información que utiliza los algoritmos simétricos AES256 y 3DES de los cuales se analizaron sus características, estructura y rendimiento en aplicaciones móviles como se observar en la Figura 8 , así mismo, se empleó el paradigma de Programación Orientada a Objetos(POO), utilizando el lenguaje de programación Java y por medio del IDE de desarrollo de aplicaciones móviles Android Studio 3.5.3.

Figura 8

Tabla comparativa entre AES y 3DES.

CARACTERÍSTICAS	AES	3DES
Longitud de clave	256 bits	K1, K2 Y K3 168 bits (56 bits por llave)
Tipo de cifrado	Simétrica bloques de Cifrado	Simétrica bloques de Cifrado
Tamaño de bloque	98, 192 Y 256 bits	64 bits
Año desarrollo	2000	1978
Resistencia criptoanálisis	- Diferencial en contra de fuerte, truncado. - Diferencial e interpolación lineal y plazas de ataques	- Vulnerable al diferencial de fuerza Bruta - Propenso a análisis de texto plano diferencial
Seguridad	Es considerado seguro	Seguridad media
Ronda	14 (256 Bits)	48
Rendimiento (encriptacion-desencriptacion)	4.174 / 6.452	3.45/ 5. 665

Fuente: [8]

Con respecto a AES256 que es un algoritmo de clave simétrica, donde la clave puede tener un tamaño de 128,192 y 256 bits, se utilizó en el proyecto, 256 bits que se cifran mediante bloques, cada bloque con un tamaño de 128 bits, el número de rondas que realiza depende del tamaño de la clave, lo cual en este caso realiza 14 rondas. Además cada ronda comprende de 4 etapas, que son Byte substitution layer , donde se realiza la conversión no lineal de los elementos de estado de la matriz; ShiftRows, que permuta los elementos ; MixColum layer, donde se realizan operaciones con la matriz constante y estado; y finalmente; Key addition layer, que se encarga de hacer un XOR entre el estado actual y la subclave. El algoritmo 3DES es una evolución de DES, también cifra la información por bloques pero de 64 bits 3 claves de 56 bits en cada ronda y en un orden específico, además de que puede trabajar con claves más extensas.

La aplicación cuenta con 5 vistas principales, y entre ellas está el cifrado/descifrado donde se seleccionan los algoritmos y las herramientas para seleccionar un texto a cifrar, como su tipo de cifrado y función hash en MD5 o SHA.

Como resultado obtenido se tuvo la creación de la aplicación de código abierto y protegiendo la información de los intrusos, mediante los algoritmos de encriptación y así, que la información se encuentre fuera de peligro, para ello ayudó también la definición de los requisitos para que precisen la ruta del trabajo para la utilización de Android con un desarrollo más dinámico permitiendo la integración de sus funcionalidades.

Conclusiones

La seguridad en Internet siempre ha sido una de las principales preocupaciones para todos aquellos que están conscientes de los peligros que puede ocasionar un intrusión de alguien no deseado en nuestra propia computadora o en los archivos más secretos.

Los clásicos sistemas de seguridad como la encriptación, antivirus y firewalls son los más útiles para tener una buena privacidad en la transferencia de los datos, sin embargo no son perfectos, los piratas siempre encuentran puertas traseras y formas de entrar.

Y en las investigaciones y/o aplicaciones presentadas de la criptografía en la seguridad de la red encontrados en nuestra indagación en algunos países de Sudamérica se evidencia y recalca la importancia de desarrollar los métodos, algoritmos y sistemas criptográficos según el problema y recursos de la problemática, porque a través del cifrados, obtuvieron una forma de garantizar la integridad, confidencialidad, estabilidad de la información en los diversos tipos de redes, evitándose así pérdidas.

Aún existe mucha investigación para mantener la información segura, algunos trabajos se orientan en que se puedan hacer cada vez más modificaciones a los algoritmos de encriptación para que resistan los ataques más usuales, evitando así, que haya incursiones y protegiéndonos de robos de archivos.

Referencias

[1] A. Torralba-Agell, A. T. Nicolau, A. Urbieta, A. C. Torres, A. Styrmoe, A. Miranda-Pascual, A. Viejo, A. J. Barceló, A. Fuster-Sabater, A. I. Gómez, *et al.* XVII Reunión española sobre criptología y seguridad de la información. RECSI 2022, volume 265. Ed. Universidad de Cantabria,2022.

[2] ASALE, R., & RAE. (2021). *Diccionario de la lengua española RAE - ASALE*. "Diccionario de La Lengua Española" - Edición Del Tricentenario. https://dle.rae.es/criptograf%C3%ADa

[3] Corletti A. (s/f). Seguridad en Redes. [Online] Available: https://www.mhe.es/cf/ciclos_informatica/844819974X/archivos/unidad9_recurso3.pdf

[4] Gutiérrez, Jaime, and Juan Gabriel Tena Ayuso, eds. *Protocolos criptográficos y seguridad de redes*. Ed. Universidad de Cantabria, 2003.

[5] H. K. CARCAMO and J. V. A. NEIRA. Criptografía de curva elíptica aplicada a seguridad para redes wban bajo la norma ieee 802.15. 6 A. M. de Castro Mota and P. R. C. Le˜ao. Análise de segurança sobre aplicativo de mensagem instantánea. *O Comunicante,* 8(3):14–22, 2018.

[6] J. A. Navarro Espinosa. Análisis de las entidades certificadoras de sudamérica. Res non verba (Guayaquil), 8(1): 59–71, 2018.

[7] J. M. Contreras. Introducción a la criptografía. DYNA, 79 (2):6–10, 2004

[8] Martínez Laguado, Miguel Fernando. "Aplicación móvil Android para proteger información por medio de criptografía simétrica."2020.

[9] R. C. Guevara Tinoco and W. L. Lopez Lopez. Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática. 2016.

[10] Sarkar, S. R. Chatterjee, and M. Chakraborty. Role of cryptography in network security. In The. Essence.of Network Security: An End-to-End Panorama , pages 103–143. Springer, 2021.

[11] The Internet Protocol Versión 6. Lee, D.C.; Lough, D.L.; Midkiff S.F.; Davis,N.J.,IV;Benchoff, P.E. lEER Network, Volume:12 Issue:I, Jan.-Feb. 1998 Page(s): 28 -33

[12] The never-ending saga of Internet security: why? how? and what to do next? Rabinovitch, E. IEEE Communications Magazine, Volume: 39 Issue: 5 , May 2001 Page(s):56-58