UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD INGENIERÍA MECÁNICA ELÉCTRICA ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS

"MODELO DE SISTEMA CRIPTOGRÁFICO DE SEGURIDAD PARA LAS REDES DE COMUNICACIONES EN LA REGIÓN PUNO – 2012"

TESIS

PRESENTADO POR:

TIBURCIO MAMANI TTITO

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

PUNO – PERU

2014

Universidad Nacional del Altiplano

FACULTAD INGENIERÍA MECÁNICA ELÉCTRICA ELECTRÓNICA Y SISTEMAS

Escuela Profesional de Ingeniería Sistemas

"MODELO DE SISTEMA CRIPTOGRÁFICO DE SEGURIDAD PARA LAS REDES DE COMUNICACIONES EN LA REGIÓN PUNO – 2012"

TESIS

PRESENTADA POR:

TIBURCIO MAMANI TTITO

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE:

M.Sc. EDELERÉ FLORES VELÁSQUEZ

PRIMER MIEMBRO:

Ing. ALDO HERNÁN ZANABRIA GALVEZ

SEGUNDO MIEMBRO:

Ing. IRENIO LUIS CHAGUA ADUVIRI

DIRECTOR DE TESIS:

Mg. CARLOS BORIS SOSA MAYDANA

ASESOR DE TESIS:

Ing. ROGER DANDY MEDYNSON TINTAYA

PUNO – PERU

2014

ÁREA: Informática
TEMA: Sistemas de información tradicionales y expertos

DEDICATORIA

A Dios

Por ser mi creador, por darme la fuerza y el valor para hacer realidad este objetivo, por estar conmigo en cada momento de mi vida y por cada regalo de gracia que me ha dado; para emprenderme nueva etapa en mi vida. GRACIAS ¡DIOS MIO!

A mi madre: Mauricia, por haberme dado la vida y el amor incomparable.

A mi padre: Maximiliano, quien con su ejemplo de trabajo me enseño el camino de la felicidad; quienes me brindaron su apoyo incondicional y la confianza percibida en mí.

A mis hermanos: Olga Matilde, William y Edith Yhovana por brindarme su permanente aliento y apoyo moral para seguir adelante con inspiración optimista.

...Tiburcio Mamani T.

AGRADECIMIENTO

A la Universidad Nacional del Altiplano, Facultad de Ingeniería Mecánica Eléctrica, Electrónica y Sistemas, Escuela Profesional de Ingeniería de Sistemas y a toda su plana docente por sus sabios enseñanzas y personal administrativo, por haberme contribuido en mi formación profesional.

Al Ing. M. Sc. Edelfré Flores Velásquez, un reconocimiento muy especial por sus buenos consejos, por su desinteresado apoyo y aportes en la realización del presente trabajo de investigación.

Al Ing. Mg. Carlos Boris Sosa Maydana, por su apoyo y aportes de la forma más desinteresada en la dirección de la presente tesis.

Al Ing. Roger D. Medynson Tintaya, por su aporte y apoyo desinteresado en el desarrollo del presente trabajo de investigación.

Al Ing. Mg. Marco Antonio Quispe Barra, por sus buenos consejos y haberme brindado su permanente apoyo moral y aliento en la realización del presente trabajo de investigación.

A mis compañeros de estudio, y amigos por brindarme su apoyo, aliento, amistad, confianza. A mi abuelita Antonia por aconsejarme en mi vida, a mi tío Fabián Sebastián y a Vidoy Jorge quienes me brindaron su apoyo moral, amistad y confianza. Y a todas las personas que contribuyeron y contribuirán con el desarrollo de la Ciencia, Tecnología de la Información, Criptografía y Seguridad Informática.

Finalmente dirigir un reconocimiento al M.Sc. Edelfré Flores Velásques, Ing. Aldo Hernán Zanabria Gálvez, Ing. Irenio Luis Chagua Aduviri; por alentarme en el inicio y en la conclusión del presente trabajo de investigación.

ÍNDICE

ANEXOS

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo despliega con el diseño del “Modelo de sistema criptográfico de seguridad para las redes de comunicaciones en la región puno-2012”, debido a que cuando se requiere compartir datos e informaciones en las redes, estas son expuestos a riesgos como denegación de servicios, observación y modificación no autorizada, la cual trae consecuencias en las transacciones. Para ello se planteó como objetivo fundamental “Modelar el sistema criptográfico de seguridad para las redes de comunicaciones” para proteger y tomar medidas de seguridad restringiendo los datos, cumpliendo con las políticas de seguridad, mecanismos consistentes y prácticas que regulan. Por tal razón se considera justificable la elaboración del modelo. La metodología utilizada es la investigación científica, exploratoria, descriptiva y explicativa, para el diseño se utilizó la herramienta técnica UML con los procedimientos científicos de la ingeniería de software. La implementación del modelo de seguridad se realizó a través de la aplicación del sistema de seguridad criptográfico asimétrica estándar corporativo determinando mecanismos y niveles de protección de datos, para las transacciones en redes, utilizando protocolo SSL con autenticación certificada, con esta se cifran los datos para intercambiar entre el servidor y el cliente mediante el algoritmo de criptografía asimétrica. Se ha demostrado que la aplicación de sistema seguridad con SSL VeriSign con tecnología web mejora de manera continua en seguridad e integridad de datos, asegurando el tráfico de HTTP, que lo convierte en HTTPS que garantiza que las transacciones sean seguras entre terminales distintas en redes, de esta manera disminuye vulnerabilidades y riesgos.

Palabras claves: Modelo de seguridad, Certificado SSL, Criptografía asimétrica, Redes de comunicaciones, Riesgos, Datos, Tecnología web

ABSTRACT

This work presents the design of the "Model of cryptographic security system for communications networks in 2012 puno region," because when you need to share data and information networks, these are exposed to risks such as denial of services, observation and alteration unauthorized, which has consequences in transactions. To this was raised as a fundamental objective "Shaping the cryptographic security system for communications networks" to protect and take security measures restricting the data, in compliance with security policies, consistent mechanisms and practices governing. For this reason it is considered justifiable modeling. The methodology is scientific, exploratory, descriptive and explanatory research to design the UML technical tool with scientific methods of software engineering was used. The implementation of the security model was performed by applying the standard security system determining corporate asymmetric cryptographic mechanisms and levels of data protection for transactions in networks, using certified SSL protocol with authentication, this data is encrypted for exchanged between the server and the client using asymmetric cryptography algorithm. It has been shown that the application of security system with SSL VeriSign web technology improves continuously in security and data integrity, ensuring HTTP traffic, making it HTTPS ensures that transactions are secure between different terminals in networks, thus reduces vulnerabilities and risks.

Key words: security model, SSL Certificate, Asymmetric Cryptography, Network Communications, Risk, Data, Web Technology.

INTRODUCCION

Las organizaciones de seguridad ponen todos sus conocimientos y recursos en crear sistemas y aplicaciones cada vez más seguras y fiables para los usuarios. Estos cada día, están más concienciados con los conceptos e intentan ponerlos en práctica cuando realizan transacciones por internet. Pero todos estos esfuerzos, a veces se olvidan cuando utilizamos nuestro computador y/o el dispositivo móvil de última generación, pues llegan a ser contagiados con virus y ser controlados por otros usuarios (Hacker). De esta manera se exponen los datos hacia los riesgos, entonces no se deben realizar transacciones en sitios webs que no están cifradas, no se pueden revelar nuestros datos bancarios por correo electrónico, y así preservar informaciones confidenciales.

En la actualidad poseemos dispositivos de última generación con su infinidad de aplicaciones y su conexión directa con todas las redes sociales que las atraen a los usuarios. Con estas dispositivos y aplicaciones no somos conscientes y/o cuidadosos de los potenciales peligros que esconden que simplemente navegar por internet podemos exhibirnos a muchos peligros que en posterior estaríamos expuestos a riesgos de ataque.

Hoy en día todo gira a nuestro entorno de perfil virtual, que creamos en las diversas plataformas sociales que existen en internet y preferimos que todos nuestros conocidos (o incluso los que no lo sean) estén al tanto de todo lo que realizamos en cada momento. Esta publicación de información, que nosotros pensamos que la controlamos al cien por ciento, a veces estamos compartiendo mucha más información encubierta que la que de verdad vemos.

La finalidad de esta tesis, es la elaboración del modelo de sistema de seguridad con criptografía asimétrica y aplicarla en la mejora continua en la protección de

datos e información en las transacciones a través de la red, y así disminuir los riesgos.

En el capítulo I se plantean las principales problemáticas sobre la inseguridad en las redes de comunicaciones, los objetivos de la investigación, la justificación, limitaciones.

En el capítulo II se definen los antecedentes del trabajo de investigación, sustento teórico y la operacionalización de variables que se utilizan a lo largo de la investigación. La finalidad de este capítulo es que se entienda los conceptos que están relacionados con modelo de sistema, criptografía y seguridad informática en sus diversos aspectos.

En el capítulo III se exponen tipo y diseños de investigación, población y muestra, técnicas e instrumentos para recolectar información, técnicas para el procesamiento y análisis de datos, tratamiento de datos. Utilizando datos recopilados sobre seguridad, riesgos y vulnerabilidad, datos estadísticos de los principales riesgos sobre aplicaciones web.

El capítulo IV se muestran los análisis e interpretación de resultados de la investigación, como la aplicación del modelo de seguridad criptográfica en sitios web utilizando certificada SSL autenticada, firewall, seguridad HTTPS estructuras del modelo de seguridad implementado, caso de usos donde se describe las técnicas para minimizar los riesgos adaptables a cualquier tecnología.

Así mismo se adjuntan como anexos las encuestas realizadas para su respectiva validación y el proceso de aplicación del Sistema de seguridad criptográfico asimétrica para la proteger y cifrar los datos e Información.

CAPITULO I.

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

1.1.1. Descripción del Problema:

Las organizaciones han realizado siempre lo imposible por la seguridad, así mismo los desafíos técnicos en redes y telecomunicaciones requieren de herramientas técnicas para dar mayor protección a los datos e información. Debido a que estas transmitidas a través de Internet pasan por muchos computadores a lo largo de su camino, y existe la posibilidad que alguien pueda estar averiguando y extrayendo información confidencial.

La necesidad de establecer y mantener transmisiones seguras usando canales de comunicaciones, ha conseguido que esta tendencia se convierta en algo extremadamente complejo de elaborar que un conjunto de esquemas de cifrados sea no fiable. De hecho, en muchos casos, un esquema de cifrado es solamente un elemento más de criptografía formado por innumerables capas, llevando todos ellos a la función de garantizar la seguridad de la información asociada a ese nivel, uno de los puntos que siempre está en discusión sobre el almacenamiento de la información en computadoras digitales, fue la seguridad de los sistemas computacionales en entidades privadas, gubernamentales y militares, la necesidad de resguardar la información almacenada allí se hace evidente.

Sabemos que no se debe realizar transacciones en sitios web que no están cifradas, no debemos revelar nuestros datos (bancarios) por correos electrónicos o por otros medios sobre la red de comunicaciones en internet.

Con la llegada de Internet y la masificación absoluta de las comunicaciones, la privacidad de los datos se ha vuelto un tema muy complejo en los últimos tiempos, originando todo tipo de problemas que

involucran desde el más simple e inocente usuario de Internet hasta las más altas organizaciones. Hasta la aparición de la informática la valoración de los activos de una empresa se realizaba según los objetos físicos útiles. Desde los últimos años se ha añadido un nuevo capital tan importante como, el valor de la información. Esto ha sido uno de los recursos que suele ser muy codiciado por entes cibernautas que tratan de aprovecharse de recurso ajenos, como el espionaje industrial es tan antiguo como la revolución industrial, pero se mantenía con el sistema de papel y archivadores y formaba parte de los activos de oficina.

Hoy en día, la información se maneja en grandes cantidades y de procedencias muy diversas, el valor añadido de una empresa puede ser la información que maneja. Como capital de la empresa cada vez es más importante mantener la seguridad de los datos e información, pero también los riesgos cada vez son mayores. Estos riesgos se pueden clasificar por su procedencia en tres categorías: Errores involuntarios de personas y/o máquinas. Desastres naturales, ataques voluntarios, siendo los primeros los más comunes. Los problemas fundamentales que se tienen en cuenta en el tercer riesgo son: *ataques voluntarios*. Los problemas creados por éstos se pueden clasificar en tres familias:

- *Denegación de servicio*: Disponibilidad, Prohibir el acceso a la información.
- *Observación no autorizada*: Confidencialidad, acceso a información por personas no autorizadas que pueden utilizarla para dañar la empresa.
- *Modificación no autorizada*: Integridad, acceso a la información y modificación, ya sea borrado, cambio, añadiendo o sustituyendo datos.

1.1.2. **Planteamiento del Problema:**

¿Cómo influye en la mejora, el Modelo de Sistema Criptográfico de Seguridad para las redes de Comunicaciones en la Región Puno - 2012?

1.1.3. **Justificación:**

La realización del presente trabajo de investigación dada la importancia y necesidad de toda organización es la de proteger el valor de la información de los riesgos voluntarios y/o mantener el proceso de mejora en la seguridad de información. Dada la posibilidad de que exista un incremento de vulnerabilidad en él envió de información sobre medios inseguros a consecuencia de procesadores y personas que se encargan de corromper la seguridad de criptografía, ocasionando que no exista confidencialidad en la transferencia de la información. De esta manera que le otorgue una ventaja competitiva frente a las demás organizaciones.

En la actualidad con llegada de la nueva tecnología y herramientas, cada vez somos más públicos y vulnerables ante posibles ataques, pues nuestra información circula por la red. Podemos tomar muchas medidas de seguridad que nos ayuden a bloquear lo que no deseemos que se publique, por ello lo mejor en cuanto a la seguridad y privacidad de la información es conocer a fondo los sistemas y sus aplicaciones existentes y estandarizadas a nivel mundial.

En consecuencia considero justificable la elaboración del presente trabajo de investigación, que a través de la aplicación del Modelo estándar corporativo se contribuiría a mantener la seguridad del valor de la información que posee la organización y con ello a mejorar la eficiencia en la protección de la información. Pues mediante ello nuestro aporte será de

gran relevancia, así contribuyendo al desarrollo de sistema criptográfico y sentar bases para posteriores estudios acerca del tema.

1.1.4. **Limitaciones de la Investigación:**

De la Aplicación:

El desarrollo de un modelo de sistema criptográfico, pretende apoyar en la mejora continua de la seguridad y gestionar la protección de datos y la información en las redes de comunicaciones durante su envío por medios inseguros de la red, de esta manera proteger su fiabilidad minimizando de los riesgos voluntarios.

La limitación se basa específicamente en proteger datos e información eficientemente de los riesgos sobre las redes. Con la tendencia a degradarse en el tiempo, es decir, a medida que pasa el tiempo el modelo y algoritmo de seguridad se van haciendo más fáciles de quebrantar debido al avance de la tecnología, velocidad y potencia del hardware.

1.2. Objetivos de la Investigación

1.2.1. **Objetivo General**:

"Modelar el sistema criptográfico de seguridad para las redes de comunicaciones en la región puno - 2012."

1.2.2. **Objetivos Específicos**:

- Analizar y diseñar los procesos de seguridad para las redes de comunicaciones.
- Implementar una tecnología basada en seguridad con criptografía asimétrica para que éste sirva de apoyo para la protección de la información.
- Implantar y evaluar un sistema de seguridad con tecnología web.

CAPITULO II.

MARCO TEÓRICO

2.1. Antecedentes de la Investigación

2.1.1. **TESIS**: "**Modelo del conocimiento en seguridad de aplicaciones Web"**

AUTOR: Ing. María Victoria Bajarlía, Argentina-2010-Tesis Maestría

El objetivo de esta tesis fue proponer un modelo, en el contexto de la Ingeniería de Conocimiento (INCO), aplicado al análisis de seguridad de aplicaciones de gestión. El modelo propuesto se fundamenta en un sistema basado en conocimiento (SBC) que cuenta con un componente cognitivo que le permite incorporar conocimiento.

Las amenazas y los ataques informáticos representan un problema de crecimiento progresivo. Por este motivo se puede suponer que el SBC, a través del aprendizaje dinámico que lo mantendrá actualizado, podrá asistir a los especialistas en seguridad informática a la elaboración de especificaciones de requerimientos de software (ERS), en dicha área de competencia.

Su metodología utilizada está conformada de: **Identificación** de la tarea, **Desarrollo** del prototipo, **Ejecución** de la construcción del sistema integrado, **Actuación** para conseguir el mantenimiento perfecto sobre el conocimiento y **Lograr** una adecuada transferencia tecnológica. Dado que necesita una importante comunicación y retroalimentación entre el ingeniero del conocimiento y el experto en seguridad informática.

Para adquirir el conocimiento, el ingeniero en conocimiento utilizando sus habilidades, deberá llegar a ser parte del problema a resolver. Sus principales conclusiones fueron

- Propuso un modelo de un SBC, capaz de dar respuesta al análisis de los niveles de seguridad de aplicaciones de gestión.

- Sistematiza y documenta, con metodología de Sistemas Expertos, el conocimiento para el área de la seguridad de aplicaciones de gestión.
- Aplica, para el área de Ingeniería en Conocimiento asegurando el desarrollo y posterior crecimiento del Sistema Experto.
- Documenta y modela la deducción y extracción de conocimiento.
- Sostiene la aplicación de la solución a través de un SBC, sobre la base de un Test de Viabilidad.

2.1.2. **TESIS: "Modelo de Seguridad en las Aplicaciones Web desarrolladas por un tercero**"

AUTOR: Sandra Cabrera García, María del Carmen García Castro, Juan Pablo Salinas Romero; Mexico-2009.

Su objetivo principal fue, disminuir los riesgos que se presentan en una aplicación Web desarrollada por un tercero conocido como Outsourcing, mediante la elaboración de un modelo de seguridad que enfrente a las principales vulnerabilidades que se encuentran en un entorno Web tomando en cuenta la mayoría de las técnica de ataque conocidas a nivel mundial, y como resultado la elaboración de las mejores prácticas con la finalidad de tener las bases para generar una aplicación estable.

Se ha utilizado metodología de investigación explicativa que van más allá de la descripción de conceptos o fenómenos, es decir es dar a conocer la realidad, establecer y tratar de contestar las preguntas tales como: ¿Cuáles son los principales riesgos de las aplicaciones web? ¿Existe una legislación que regule los ataques que sufre una aplicación web? ¿Por qué implementar un modelo de seguridad a las aplicaciones

web desarrolladas por un tercero? Para dar respuesta se aplicó una serie de encuestas dirigidas a expertos sobre el área.

De esta manera llego a la conclusión de que a lo largo de la aplicación del modelo de seguridad se obtiene una mayor perspectiva de certidumbre y confianza hacia la empresa que solicita el servicio de Outsourcing debido a que este prevé los puntos débiles existentes en un sistema Web

2.1.3. **TESIS**: **"Análisis del sistema de seguridad en servidores Web para su correcta utilización**"

AUTOR: Katherine Cantos Rivera; Karla Carangui Vintimilla - 2007

Su finalidad fue implantar medidas de protección dirigidas a asegurar las aplicaciones finales ofrecidas por los clientes, procurando que las mismas carezcan de vulnerabilidades, que pueden ser aprovechadas de manera indebida por personas mal intencionadas.

Como metodología utiliza la investigación científica con la cual identifica las principales técnicas en relación al análisis del sistema de seguridad en servidores web, orientados a ciertas normas, reglas y herramientas para garantizar la confidencialidad, confiabilidad e integridad de los datos.

Concluye que la mejora es muy importante en cuanto a la seguridad de los Servidores Web. El cual dificulta abarcar todas las alternativas para reducir las vulnerabilidades.

2.2. Sustento teórico

2.2.1. Modelo de seguridad informática

Un modelo de seguridad es la presentación formal de una política de seguridad. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada (López Barrientos & Quezada Reyes, 2006).

Un "Modelo de Seguridad de la Información" es un diseño formal que promueve consistentes y efectivos mecanismos para la definición e implementación de controles (Gómez: 2007.178).

De acuerdo a (López Barrientos & Quezada Reyes, 2006), los modelos se clasifican en:

- *Abstracto*: se ocupa de las entidades abstractas como sujetos y objetos.
- *Concreto*: traduce las entidades abstractas en entidades de un sistema real como procesos y archivos.

Además, los modelos sirven a tres propósitos en la seguridad informática:

- Provee un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas.
- Provee representación de política general de seguridad formal clara.
- Expresar la política exigida por un sistema de cómputo específico.

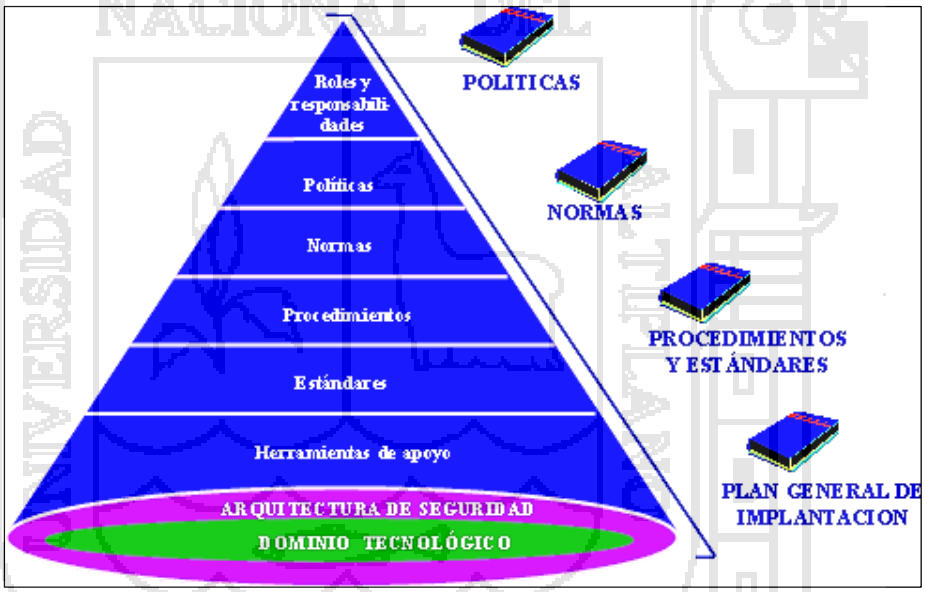
Como construir una arquitectura de seguridad informática

Un adecuado modelo de "Seguridad Informática" está basado en políticas sólidas de seguridad de la información, teniendo como marco de referencia las mejores prácticas internacionales tales como BS ISO/IEC 17799:2005 y BS 7799-1:2005, con el apoyo de la alta dirección y realizando una divulgación periódica y capacitación constante a los

miembros de las organizaciones referente a los riesgos que se expone la información y los controles necesarios para su mitigación.

Se debe contar con herramientas de protección de última tecnología, permanentemente actualizadas, funcionando 7X24X365 y con un alto grado de capacidad de respuesta, y un equipo de trabajo altamente calificado, que cuente con las certificaciones de seguridad informática necesarias, disponible 7X24X365, actualizado permanentemente y con un enfoque único y total en seguridad y administración del riesgo. (Nocella: 2013. http://negociosymanagement.com.ar/?p=2285)

FIGURA Nº 1: Componentes del Modelo de Seguridad de Información



Fuente: (Nocella: 2013. http://negociosymanagement.com.ar/?p=2285)

2.2.2. **Criptologia**

La Criptologia (del griego krypto y logos, estudio de lo oculto) es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones, *(Lucena. 2000: 28).*

- **La criptografía**: Es el conjunto de procedimientos que garantizan la seguridad de la información y utilizan técnicas criptográficas. El elemento fundamental es la “llave”.
- **El criptoanálisis**: Área de la matemática, son los métodos para romper los criptogramas (descifrar el mensaje sin ser el verdadero destinatario) por análisis y deducción sin tener conocimiento previo de la clave.

De forma general labor de la criptografía es convertir un texto plano en uno cifrado, mientras que del criptoanálisis es conseguir el texto original a partir del criptograma sin poseer las claves necesarias *(Lucena. 2000: 24)*

2.2.3. Criptografía.

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. Esto da lugar a cuatro aspectos de la seguridad informática *(Ramio. 2006: 82*).

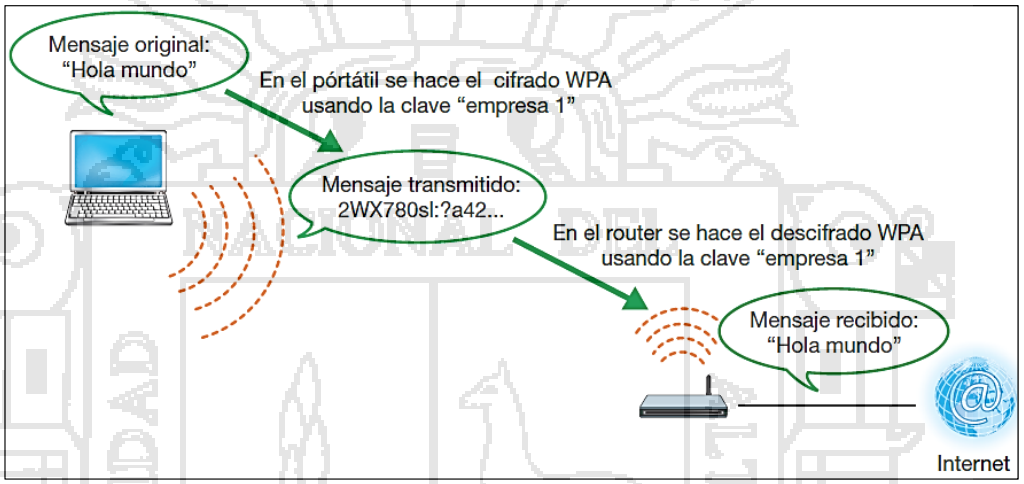
Los principales problemas de seguridad que resuelve la criptografía son: La confidencialidad. , la integridad, La disponibilidad y el no rechazo o no repudio.

2.2.4. Fundamentos teóricos de la criptografía

Etimológicamente viene del griego “*Kriptos*” que significa *ocultar* y “*Graphos*”, que significa *escritura*. Es la ciencia que estudia cómo mantener la seguridad de la información, a través de códigos y claves. Es decir es ocultando su significado a través de un proceso que se le llama Cifrado. Con la ventaja que si es interceptado el mensaje cifrado, lo hace no entendible (Lucena 2011: 20).

¿Cómo funciona la criptografía? "Se basa en que el emisor emite un texto plano, y con una clave, crea un texto cifrado", Este texto cifrado, se envía por medio del canal de comunicación insegura, llega al destinatario que lo convierte, apoyándose en la clave del emisor o en otra clave, según sea el tipo de criptografía que esté utilizando de llave Pública o privada, en el texto plano.(Roa Buendía. 2013:29).

FIGURA Nº 2: Esquema de proceso cifrado WPA en redes WIFI



Fuente: (Roa: 2003. 29)

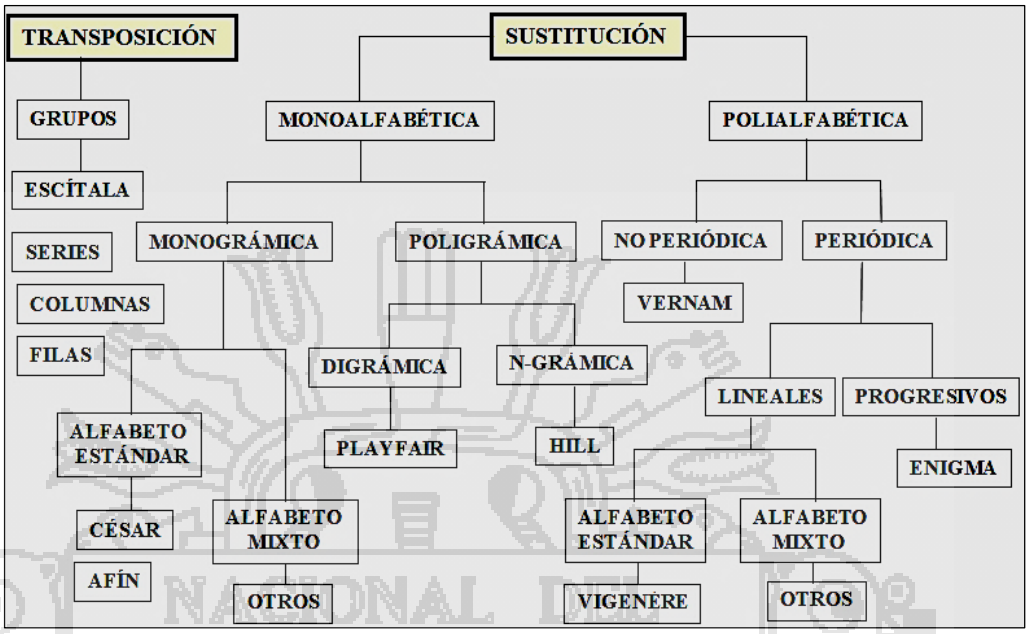
2.2.5. **Técnicas de Criptografía**

En el 2001 Fuster, hace uso de dos técnicas básicas orientadas a caracteres o letras propuestos por Shannon:

- *Técnicas de sustitución*: Las letras del mensaje en claro se modifican por otros elementos (letras) en la cifra. El cifrado tendrá entonces caracteres distintos a los que tenía el mensaje en claro.
- *Técnicas de transposición o permutación*: los caracteres del mensaje en claro se redistribuyen sin modificarlos y según unas reglas, dentro del cifrado. El cifrado tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

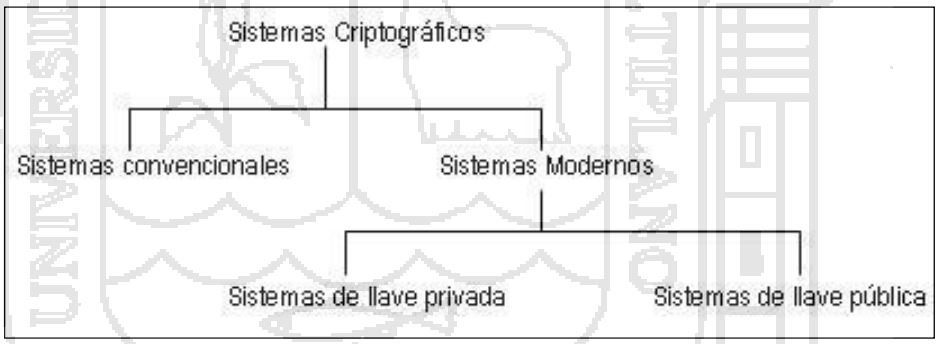
2.2.6. Clasificación de la criptografía

FIGURA Nº 3: Clasificación de los criptosistemas clásicos



Fuente: (Acosta: 2010. es.slideshare.net/jmacostarendon/criptografia-principios-matemticos)

FIGURA Nº 4: Mapa Conceptual de Sistemas Criptográficas



Fuente:(Romero: 2008. www.utilidad-aritmetica-modular-sistemas-criptograficos3.shtml)

2.2.6.1. Criptografía Simétrica.

Los algoritmos de criptografía simétrica utilizan la misma clave para los dos procesos cifrar y descifrar. En general, resultan bastante eficientes, tardan poco tiempo en cifrar o descifrar. Todos los algoritmos desde la antigüedad hasta los años setenta, eran simétricos, los más utilizados actualmente son DES, 3DES, AES, Blowfish e IDEA. (Caballero. 1997:48)

Ventajas y desventajas de la criptografía simétrica.

En el 2013 Roa, hace referencia las siguientes ventajas y desventajas de la criptografía simétrica

Ventajas

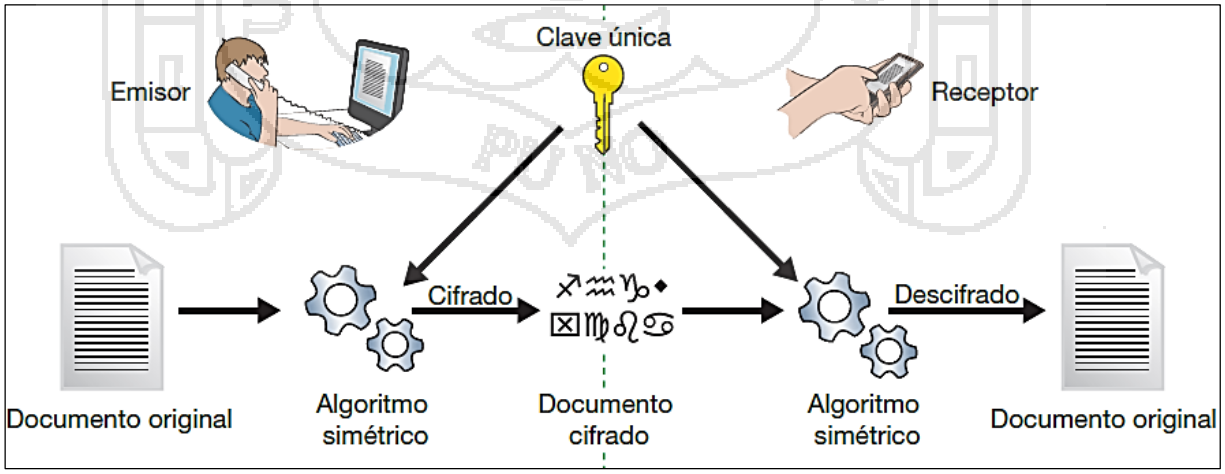
- Fácil de utilizar, resultan eficientes.
- Rápido en cifrado y descifrado con la única clave

Desventajas

- El problema principal es la circulación de las claves.
- Gestión de las claves almacenadas, si en una empresa hay 10 trabajadores y todos tienen conversaciones privadas con todos, cada uno necesita establecer 9 claves distintas y encontrar 9 canales seguros para actualizarlas cada vez (en total 81 claves y 81 canales).

  Si aparece un trabajador nuevo, ahora son 100 claves y 100 cabales. Si tiene 500 trabajadores 5000 claves y 5000 canales. ¿Cada vez que cambie mi clave tengo que avisar a 49999 compañeros? Es poco manejable.

FIGURA Nº 5: Esquema de Criptografía Simétrica



Fuente: (Roa:2013.30)

Aplicación práctica de la criptografía simétrica

En el 2013 Roa, explica la ***autenticación de un móvil GSM***: porque sabe que es nuestro número, aunque insertamos la tarjeta SIM en otro teléfono. El procedimiento es la siguiente:

- Nuestra tarjeta SIM contiene un identificador T y una clave K.
- Identificador T y la clave K aparecen asociados a nuestro contrato en servidores de autenticación de la operadora de la que somos clientes.
- Cuando encendemos el teléfono, se conecta a la red de la operadora y solicita entrar con el identificador T. Su servidor de autenticación recibe la petición y genera un número aleatorio A que nos lo envía.
- Una vez recibido, en nuestro teléfono aplicamos un determinado algoritmo simétrico sobre ese número A, utilizando la clave K. Resultado es el numero B. Enviamos el numero B al servidor de autenticación.
- Cuando lo recibe, el también aplica el mismo algoritmo con la misma clave. Si el resultado es igual a B, se confirma que somos los dueños del identificador T. Nos asigna nuestro número 9xx, y ya podemos hacer y recibir llamadas.
- Si cambiamos de teléfono, no importa porque el número va asociado a la SIM. Con esta solución estamos protegidos de una posible captura de tráfico inalámbrica mediante un sniffer de red.
- Podría capturar el numero A. Pero es un simple número aleatorio; sin el algoritmo y la clave, el atacante no podrá generar respuesta correcta B.
- Podría capturar también el numero B y ya tendría la respuesta correcta cuando el servidor envía el numero A. Pero la probabilidad de que el servidor repita el mismo número A para este abonado es muy baja. Es

decir, si el atacante elabora una tarjeta SIM preparada para responder B cuando le pregunten A, es muy poco probable que tenga éxito.

2.2.6.2. Criptografía Asimétrica

Su algoritmo de cifrado utiliza dos claves matemáticamente relacionadas de manera que lo que cifras con una solo lo puedes descifrar con la otra. Comparando con la criptografía simétrica, ahora el emisor no necesita conocer y proteger una clave propia; es el receptor quien tiene el par de claves. Elige una de ellas (***clave pública***) para comunicarla al emisor por si quiere enviar algo cifrado. Pero ya no hace falta buscar canales protegidos para enviarla, aunque la tercera persona la conozca todo lo que se cifra con esa clave solo se podrá descifrar con la otra clave de pareja (***clave privada***), que nunca es comunicada. Y matemáticamente es imposible deducir la clave privada conociendo solo la clave pública.

Las dos claves pertenecen al emisor, la clave pública se puede entregar a cualquier usuario, la otra clave privada el propietario debe guardarla de modo que nadie tenga acceso a ella (Roa. 2013:34).

La clave pública puede ser usada por cualquiera que desee comunicarse con su emisor. Entonces, se necesita sólo **n** pares de claves por cada **n** personas que deseen comunicarse entre sí. (Lucena. 2000:68)

Según Díaz, las dos principales ramas de la criptografía Asimétrica son:

- **Cifrado de clave pública:** un mensaje cifrado con la clave pública de un receptor no puede ser descifrado por nadie (incluyendo al cifrador), excepto un poseedor de la clave privada correspondiente. *Se utiliza para confidencialidad*.

- **Firmas digitales:** un mensaje firmado con la clave privada del emisor puede ser verificado por cualquier persona que tenga acceso a la clave pública del emisor. Se utiliza la identificación y autenticidad del emisor.

Una analogía con el cifrado de clave pública es la de un buzón con una ranura de correo. La ranura de correo está expuesta y accesible al público; su ubicación (la dirección de la calle) es, en esencia, la clave pública. Alguien que conozca la dirección de la calle puede ir a la puerta y colocar un mensaje escrito a través de la ranura; sin embargo, sólo la persona que posee la clave puede abrir el buzón de correo y leer el mensaje (Roa. 2013:37).

Una analogía para firmas digitales es el sellado de un sobre con un sello personal. El mensaje puede ser abierto por cualquier persona, pero la presencia del sello autentifica al emisor. (Roa. 2013:40)

Esquema de criptografía asimétrica

En el 2012 Jimeno, especifica dos esquemas de criptografía asimétrica.

- **Esquema centralizado**: Existe una arquitectura cliente-servidor donde los servidores juegan un papel central y proveen servicios a los clientes. Son más vulnerables a ataques de denegación de servicio, debido a que basta con el fallo del servidor central para que el sistema de confianza caiga por completo.
- **Esquema descentralizado**: existen varios nodos y cada uno tiene capacidades y derechos. Se considera menos seguros contra ataques encaminados a publicar claves públicas falsas debido a que al haber varios nodos posibles a atacar es más difícil asegurar su seguridad.

Modelos de criptografía asimétrica

- **Uso de una infraestructura de clave pública (PKI).** Existen varias entidades emisoras de certificados (CA) que aseguran la autenticidad de la clave pública y de ciertos atributos del usuario (Nash 2002: 218).
- **Establecimiento de una web de confianza.** No existen nodos aparte de los usuarios. Este tipo de implementación de la confianza es el que usa PGP (Nash 2002: 220).
- **Uso de criptografía basada en identidad**. existe un generador de claves privadas o PKG (**P**rivate **K**ey **G**enerator) que a partir de una cadena de identificación del usuario genera una clave privada y otra pública para ese usuario (Nash 2002: 198).
- **Uso de criptografía basada en certificados**. el usuario posee una clave privada y otra pública. La clave pública la envía a una CA que basándose en criptografía basada en identidad genera un certificado que asegura la validez de los datos (Roa. 2013: 48).
- **Uso de criptografía sin certificados**. similar al modelo que usa criptografía basada en identidad pero con la diferencia de que lo que se genera en el centro generador de claves o KGC (**K**ey **G**enerator **C**enter) es una clave parcial.(Lucena. 2011: 60,80)

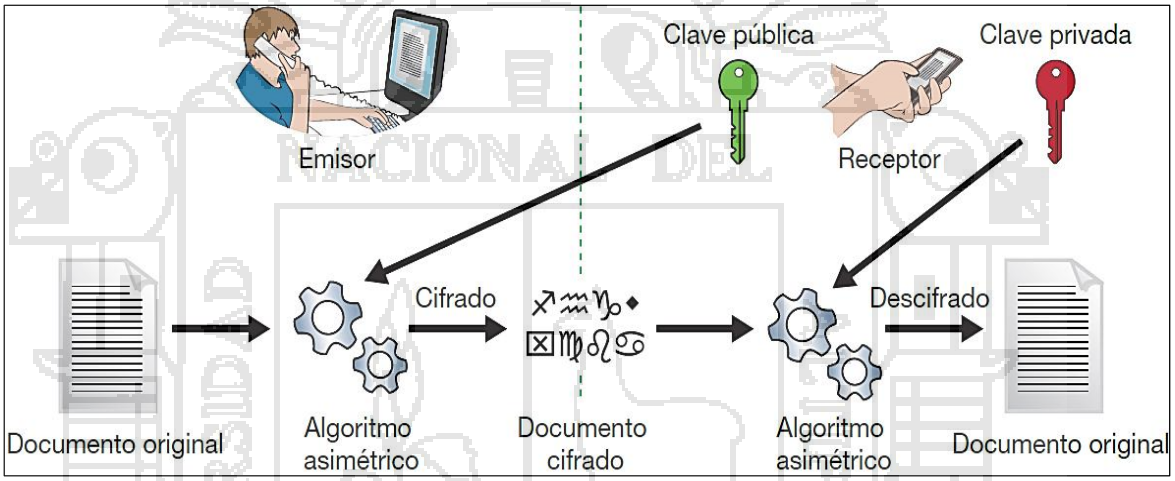
Niveles de confianza de criptografía asimétrica

Se distingue tres niveles que dan los distintos modelos a la autoridad que interviene en el proceso (PKG, KGC o CA según cada caso):

- **Nivel 1**: La autoridad puede calcular claves secretas de usuarios y por tanto pueden hacerse pasar como cualquier usuario sin ser detectado. Las firmas basadas en identidad pertenecen a este nivel de confianza.

- **Nivel 2**: La autoridad no puede calcular claves secretas de usuarios, pero puede todavía hacerse pasar como cualquier usuario sin ser detectado. Firmas sin certificados pertenecen a este nivel
- **Nivel 3**: La autoridad no puede calcular claves secretas de usuarios, y tampoco puede hacerse pasar como un usuario sin ser detectado. Es el nivel más alto de fiabilidad. Las firmas tradicionales PKI y la firmas basadas en certificados pertenecen a este nivel (caballero. 1997:126)

FIGURA Nº 6: Esquema de Criptografía Asimétrica



Fuente: (Roa: 2013.34)

Ventajas y desventajas de la criptografía asimétrica

En el 2013 Roa, define las siguientes ventajas y desventajas de la criptografía asimétrica

Ventajas:

- Distribución de la clave pública es más fácil y segura manteniendo la clave privada para el uso exclusivo del emisor.

Desventajas

- Mayor tiempo de proceso para la longitud de clave y mensaje.
- El mensaje cifrado ocupa más espacio que la original.

Los nuevos sistemas de clave asimétrica basado en curvas elípticas tienen características menos costosas. Herramientas como PGP, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y esta para la transmisión de la información.

Seguridad en criptografía simétrica y asimétrica

Según el segundo principio de Kirchhoff toda la seguridad debe descansar en la clave y no en el algoritmo. El tamaño de la clave es una medida de la seguridad del sistema (Díaz. 1996:78).

En un ataque de fuerza bruta sobre un cifrado simétrico con una clave del tamaño de 80 bits, el atacante debe probar hasta 2^{80}-1 claves para encontrar la clave correcta. Y *sobre un cifrado asimétrica* con una clave del tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales) (Ramio. 2006:122).

La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos. (Caballero. 1997: 98)

En el 2013, Roa explica que la criptografía asimétrica resuelve los dos problemas de la clave simétrica.

- No necesitamos canales seguros para comunicar la clave que utilizaremos en el cifrado. Podemos adjuntarla en nuestros correos, añadirlas al perfil de nuestras redes sociales, “postearlas” en un blog.

- No hay desbordamiento en el tratamiento de claves y canales. Si somos 10 empleados, solo necesitaremos 10 claves y un solo canal; la intranet de la empresa y un correo destinado a toda la empresa.

2.2.7. Definición matemática de sistema criptográfica

En el 2000, Lucena define el sistema de cifrado, matemáticamente como una quíntupla formada por (M, C, K, D, E) donde:

a) M = {m_1, m_2, m_3, …, m_n }:

Es el conjunto de todos los mensajes sin cifrar. Es el espacio de mensajes construidos con los textos en claro que se pueden formar con el alfabeto. Cada texto $m_i \in M$ (i=1…n) se representa por un formato numérico en el que se transforma el texto plano $\mathbf{m_i}$ por un medio previamente definido. *Por ejemplo*: asignándole a cada letra de nuestro alfabeto el número de su posición. A=1, B=2, C=3, D=4, E=5, F=6…

b) C= {c_1, c_2, c_3, …, c_n }:

Representa el conjunto de todos los mensajes cifrados. Es el conjunto finito de posibles textos cifrados.

c) *K* = {k_1, k_2, k_3,…,k_n }:

Representa el conjunto de llaves que se pueden emplear en la criptografía. Es el conjunto finito de posibles claves.

d) E= {e_1, e_2, e_3…e_k…e_n}:

Es el conjunto de aplicaciones de cifrado, que para cada $k \in \mathbf{K}$, aplica a cada elemento $\mathbf{m} \in \mathbf{M}$ para obtener un elemento $\mathbf{c} \in \mathbf{C}$. Esto es: Para cada clave k_i(i=1,2,…, n); e_k envían cada mensaje sin cifrar en el mensaje cifrado.

$$E = \{e_k / e_k : M \longrightarrow C\}$$

$$E = \{e_k / e_k : \text{es biyectiva}\} \text{ para cada } k \in K$$

La última definición de E nos dice que la propiedad básica de toda aplicación de cifrado es que sea biyectiva en razón de:

- No pueden haber dos letras distintas que se conviertan en la misma. La traslación de Cesar tiene claramente esa propiedad.
- Porque siendo f una aplicación biyectiva, al aplicar f(m) puede enviar c=f(m) al destinatario y este para poderlo leer debe aplicarle la función inversa de fa c obteniendo m, f^{-1} (c)=m, donde se puede recuperar el texto original

e) D = {d_1, d, d_3…..d_k ….d_n}:

Es el conjunto de aplicaciones de descifrado, análogo a E. Es decir: $D = \{d_k / d_k : C \longrightarrow M\}$. Las aplicaciones d_k envían cada mensaje cifrado en el mensaje sin cifrar correspondiente según la clave k∈**K**. Transforma un elemento c∈**C** en un elemento m∈**M**. Esto es, $d_k(e_k(m)) = m$

El objetivo del cifrado y del posterior descifrado de un mensaje es obtener el texto original: $\mathbf{d_k}(e_k(m)) = m$ condición matemática que debe cumplir todo criptografía. Se concluye algunas consecuencias que aun siendo obvias, conviene tratar:

- Para cada mensaje m∈M y para cada k∈K existe un único mensaje cifrado c∈C tal que $e_k(m) = c$
- El mismo resultado para d_k
- La aplicación e_k es biyectiva para cada k∈K

2.2.8. Esteganografia

Es la parte de la criptología que estudia y aplica técnicas que permite el ocultamiento de mensajes, de modo que no se perciba su existencia. De esta forma establecer un canal encubierto de comunicación,

de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal (Pastor. 1998:114).

Funcionamiento de Esteganografia

La idea que sigue es enviar el mensaje oculto *(E)* en un mensaje de apariencia inocua **(C)** que servirá de "camuflaje". Esto es, se aplica una función de esteganografía *f(E)*. El resultado de aplicar la función *(O),* se envía por un canal inseguro y puede ser visto sin problemas por el guardián. Finalmente, el otro prisionero recibe el objeto O y, aplicando la función inversa $f^{-1}(O)$, puede recupera el mensaje oculto (Rodríguez. 1986:97).

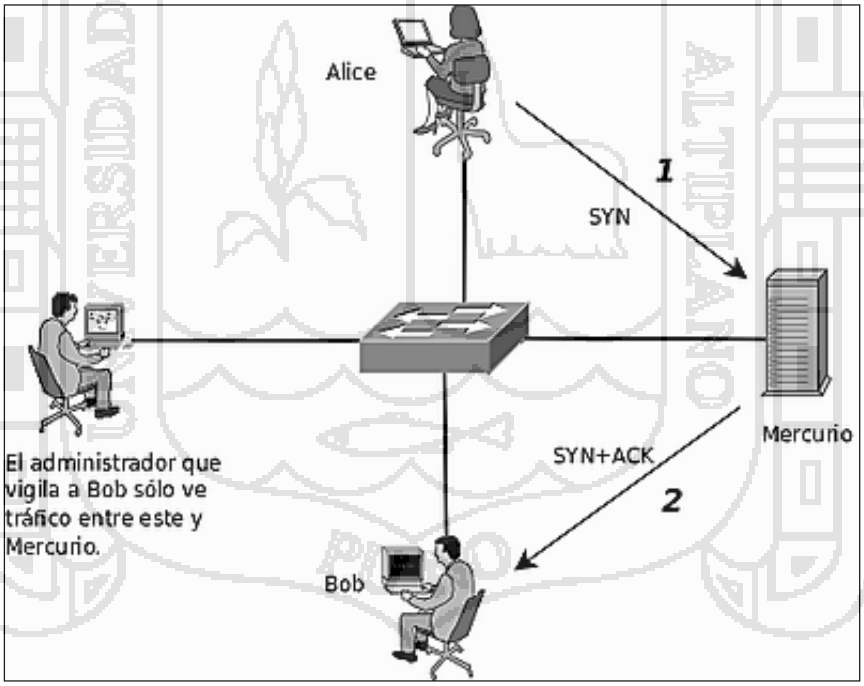
La que resulta menos conocida es la denominada *esteganografía de red***,** la cual utiliza determinadas características de los protocolos de red para encapsular datos y transmitirlos camuflados por Internet.

En el 2012 Jimeno identifica tres métodos principales de la esteganografía de red basada en:

a) Encapsulación de un protocolo en otro.
b) Encapsulación de información en el campo de datos de un protocolo.
c) Encapsulación de información en un campo numérico de un protocolo.
   - *El campo de identificación cabecera IP*. Con 16 bits de longitud.
   - *El campo de número inicial de secuencia de la cabecera TCP*. Sus 32 bits de longitud nos permite enviar 4 caracteres ASCII por paquete.
   - *El campo de número de secuencia reconocido de la cabecera TCP*. También de 32 bits.

El uso del último es más interesante y es el que utiliza herramientas como **Ncovert**. Supongamos que Alice quiere enviarle un mensaje a Bob, pero ella sabe que hay un administrador de red para Bob y monitoriza todo el tráfico de su ordenador. Resulta que Alice no conoce oficialmente a Bob y sabe que cualquier acercamiento a él levantaría sospechas y lo mismo pasaría a nivel de red si se detectase tráfico desde el PC de Alice hacia el Bob. Pero Alice ha leído estas líneas y sabe que puede ocultar su mensaje entre el tráfico "legal" de Bob. Para ello Alice elegiría un servidor al que acceda usualmente Bob, llamémoslo por ejemplo Mercurio, y lo utilizaría de intermediario para pasarle el mensaje. (López. 2009: 168)

FIGURA Nº 7: Uso del campo de número de secuencia reconocido de la cabecera TCP/IP



Fuente: (Siguenza:2011.blogspot.com/2011/01/esteganografia-para-ocultar-un-mensaje.html

La idea es la siguiente:

1) Alice crea sucesivos paquetes SYN (conexión) con Mercurio poniendo en el campo de Número Inicial de Secuencia TCP (IP) los caracteres de

su mensaje tal y como veíamos antes pero falsificaría el origen del paquete SYN poniendo que proviene de la dirección IP de Bob.

2) Mercurio crea paquetes de SYN+ACK con destino a Bob (ya que él cree que es Bob el que le envía los paquetes SYN), utilizando en el campo de número de secuencia reconocido el número fijado por Alice más 1.
3) Bob recopila dichos paquetes SYN+ACK, extrae sus campos de Número de Secuencia Reconocido, restarle 1 y pasar a ASCII.

La ventaja de este sistema es que el administrador sólo ve un flujo de paquetes entre Bob y Mercurio por lo que no sospecha nada. Además, no es necesario dirigir los paquetes a un puerto a la escucha de Mercurio, ya que en caso de utilizar un puerto cerrado, Mercurio reenviará los datos a Bob en un paquete RST+ACK en vez de en un SYN+ACK. La pega es que los paquetes RST+ACK llaman bastante más la atención en una captura de red que los de SYN+ACK al señalar errores en las conexiones, por lo que si Alice quiere minimizar la probabilidad de llamar la atención del administrador fijaría un puerto de destino abierto por ejemplo, si Mercurio fuese un servidor Web utilizaría el puerto 80 (Stallings.2000:348).

2.2.9. **Estegoanalisis**

Es la ciencia que estudia la detección de mensajes ocultos usando esteganografia. Dichos mensajes pueden estar ocultos en diferentes tipos de medio, como pueden ser las imágenes digitales, los ficheros de vídeo, los ficheros de audio o incluso un simple texto plano. El criptoanálisis es necesario descifrar el mensaje para considerar roto un criptografía, en el caso del estegoanálisis basta con ser capaz de detectar la existencia de un mensaje oculto para considerar el sistema roto. (Ramio. 2006: 142)

2.2.10. Algoritmo RSA (Rivest, Shamir y Adleman)

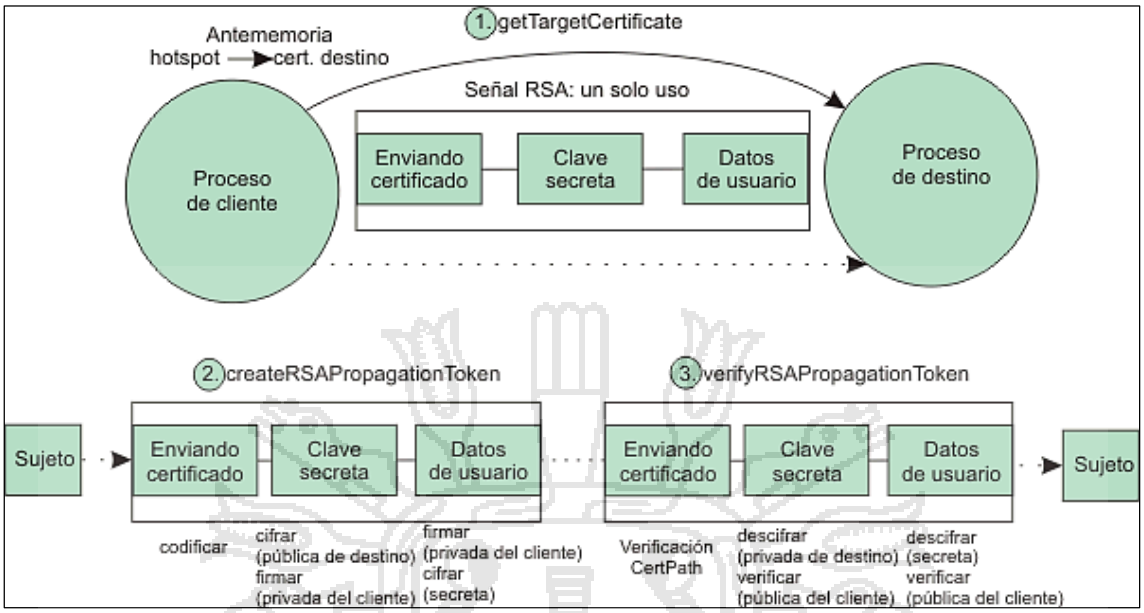
Es un sistema criptográfico de clave pública. La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10^{200}, y se prevé que su tamaño aumente con el aumento de la capacidad de cálculo de los ordenadores (Jimeno 2012:757).

Mecanismo de autenticación de señales RSA

Se utiliza para simplificar el entorno de seguridad para la topología de Gestión flexible. Con esta puede gestionar trabajos administrativos, local o remotamente, utilizando un gestor de trabajos que gestiona aplicaciones, realiza el mantenimiento de producto, modifica las configuraciones y controla el tiempo de ejecución de servidor de aplicaciones. El mecanismo de autenticación RSA sólo se utiliza para la autenticación administrativa de servidor a servidor, por ejemplo solicitudes de transferencia de archivos y de conector admin. Para el uso del mecanismo de autenticación RSA no se sustituye LTPA ni Kerberos por aplicaciones (Jimeno. 2012: 759).

La visión general del mecanismo de autenticación de señales RSA y describe el proceso que tiene lugar cuando se envía una solicitud desde un servidor como cliente a un servidor de destino. El servidor como cliente tiene un asunto administrativo en la hebra que se utiliza como entrada para crear la señal RSA. El resto de información necesaria es un certificado público RSA del servidor de destino.

FIGURA Nº 8: Visión general del mecanismo de autenticación de señales RSA



Fuente: www.com.ibm.websphere.zseries.doc/ae/csec_7rsa_token_auth.html?lang=es

El objetivo básico es convertir el asunto del cliente en un asunto en el destino mediante la propagación protegida de la información necesaria. Una vez que se haya generado el asunto en el destino, se habrá completado el proceso del mecanismo de autenticación RSA

2.2.11. Análisis de riesgos

En el 2012 Jimeno, especifica las técnicas que brinda la seguridad lógica consistente en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas. Los medios para conseguirlo son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores en el trabajo no pueden modificar los programas ni los archivos.
- Asegurar que se utilicen los datos, archivos y programas correctos por el procedimiento elegido.

- Asegurar que la información transmitida sea la misma que reciba el destinatario.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos.
- Actualizar las contraseñas de accesos a los sistemas de cómputo.

2.2.12. Políticas de seguridad

En el 2007 Gómez, identifica exclusivamente para asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad

2.2.13. Técnicas de enumeración de sistemas

En el 2012 Jimeno, define que las técnicas de enumeración se basan en la obtención de información a través de peticiones a los servicios y herramientas configurados en un sistema. Mediante las diferentes técnicas de enumeración podremos acceder a la siguiente información:

- Tipo de red
- Recursos compartidos
- Usuarios del sistema
- Información obtenida del protocolo SNMP
- Información obtenida del protocolo LDPA
- Datos de los dominios y su organización

Dentro de una red encontramos diferentes host que dan un determinado servicio a la red, ya sean servidores de correo, servidores de impresión, servidores de dominio, o simplemente equipos que comparten carpetas o impresoras. Podríamos decir que las técnicas de enumeración nos ayudaran a descubrir todos estos recursos y indicarnos qué usuarios pueden acceder a ellos. Debido a que cada sistema operativo tiene unos servicios y una forma de gestionarlos diferente, estas técnicas las tenemos que dividir según el sistema operativo (Fuster 2001:218).

Para obtener la información que deseamos de un sistema, será el hecho de intentar ocultar dicha petición de información, para que nuestros rastreos no sean detectados. Si el administrador de un sistema detecta la intención de recuperar información del mismo pondrán mucha más atención a sus medidas de seguridad e intentara por todos modos proteger su sistema (Jimeno 2012: 106).

Uno de nuestros primeros objetivos será detectar el sistema operativo que se encuentra instalado en la máquina que estemos rastreando. Identificar con la mayor exactitud posible, todas y cada una de las versiones de los programas y software instalados en la maquina objetivo, pues una vez obtenida dicha información, podremos seleccionar los exploits que aprovechan las posibles vulnerabilidades de dichas versiones.

Las vulnerabilidades se van solucionando con las diferentes versiones de los componentes de software, por lo que si encontramos un exploit para una versión en concreto puede que no nos sirva en versiones diferentes. (Jimeno. 2012: 107)

2.2.14. Métodos de enumeración en sistema Windows

Para obtener información de un sistema Windows, lo primero que se fija es en los servicios y recursos compartidos que pueden tener publicados al exterior. Otro dato importante son las cuentas de usuarios y sus perfiles. Todo este tipo de datos se apoyan en los protocolos de red.

De entre todos los protocolos, o conjunto de ellos, el que más nos interesa para este tipo de enumeración será el protocolo TCP. Se utiliza en la red de ordenadores para que estos puedan enviarse información entre ellos. El protocolo TCP garantiza él envió y la coherencia de los datos en el destino, soporta gran parte de los servicios más comunes en internet, como puedan ser: HTTP, SMTP, FTP, POP3, etc. (Jimeno. 2012:111)

Según Jimeno, los métodos apropiados de enumeración de sistemas son:

a). Sesiones Nulas

Una sesión nula es el establecimiento de una conexión entre dos máquinas a través del servicio NetBIOS. Son conexiones no autentificadas, quiere decir que estaríamos accediendo a un recurso del sistema sin la necesidad de un usuario y una contraseña. Son utilizadas por los sistemas operativos Windows para obtener el listado de los recursos compartidos.

b). NetBIOS (Network Basic Input Output System)

NetBIOS, es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. Método de búsqueda es:

- Recursos compartidos de las máquinas y de los dominios accesibles.
- Dominios accesibles
- Búsqueda de los controladores de dominio

Utilidad de NetBIOS

- Permite a las aplicaciones 'hablar' con la red. Su finalidad es aislar los programas de aplicación de cualquier tipo de dependencia del hardware.
- La red local con soporte NetBIOS, las computadoras son identificadas con un nombre. Cada computador de la red tiene un nombre.
- Cada PC de una red local NetBIOS se comunica con los otros con una conexión (sesión), usando datagramas NetBIOS o mediante broadcast.

Funciones y Servicios de NetBIOS

- Provee los servicios de sesión descritos en la capa 5 del modelo OSI.
- Permite comunicación orientada a conexión (TCP) o no orientada a conexión (UDP).

c). Registros de Windows

Es una base de datos jerárquica que almacena los ajustes de configuración y opciones en los sistemas operativos Microsoft Windows. Contiene la configuración de los componentes de bajo nivel del sistema operativo, así como de las aplicaciones que haya funcionado en la plataforma. Hacen uso del registro el kernel, los controladores de dispositivos, los servicios, el SAM, la interfaz de usuario y las aplicaciones de terceros.(Jimeno. 2012: 124)

Estructura de Registros

El registro contiene dos elementos básicos:

- **Claves del Registro:** son similares a carpetas, cada clave puede contener subclaves, que a su vez pueden contener más subclaves, y así sucesivamente. Ejemplo:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows se refiere a la subclave "Windows" de la subclave "Microsoft" de la subclave "Software" de la clave raíz HKEY_LOCAL_MACHINE.

- **Valores del registro**:

CUADRO Nº 1: Listado de valores estándar del registro Windows

LISTA DE TIPOS DE VALORES ESTÁNDAR DEL REGISTRO		
Nombre	**Nombre de tipo simbólico de datos**	**Significado y codificación de los datos almacenados en el valor de registro**
0	**REG_NONE**	Datos sin ningún tipo (en todo caso, el valor almacenado)
1	**REG_SZ**	Valor de cadena, normalmente almacenado y mostrado en UTF-16LE (cuando se utiliza la versión Unicode de las funciones API de Win32), que generalmente termina con un carácter nulo
2	**REG_EXPAND_SZ**	Valor de cadena "expandible" que puede contener variables de entorno, normalmente almacenado y mostrado en UTF-16LE, que generalmente termina con un carácter nulo
3	**REG_BINARY**	Datos binarios (cualquier dato arbitrario)
4	**REG_DWORD / REG_DWORD_LITTLE_ENDIAN**	Valor DWORD, número entero no negativo de 32 bits (números entre el 0 y el 4.294.967.295 [232 – 1]) (little-endian)
5	**REG_DWORD_BIG_ENDIAN**	Valor DWORD, número entero no negativo de 32 bits (números entre el 0 y el 4.294.967.295 [232 – 1]) (big-endian)
6	**REG_LINK**	Enlace simbólico (UNICODE) a otra clave de registro, especificando una clave raíz y la ruta a la clave objetivo
7	**REG_MULTI_SZ**	Valor de cadena múltiple, que generalmente es una lista ordenada de cadenas no vacías, normalmente almacenadas y mostradas en UTF-16LE, cada una de ellas terminada en un carácter nulo, y la lista normalmente también termina con un carácter nulo.
8	**REG_RESOURCE_LIST**	Lista de recursos (usada por la enumeración y configuración del hardware Plug-n-Play)
9	**REG_FULL_RESOURCE_DESCRIPTOR**	Descriptor de recursos (usado por la enumeración y configuración del hardware Plug-n-Play)
10	**REG_RESOURCE_REQUIREMENTS_LIST**	Lista de requisitos de recursos (usada por la enumeración y configuración del hardware Plug-n-Play)
11	**REG_QWORD / REG_QWORD_LITTLE_ENDIAN**	Valor QWORD, número entero de 64 bits (puede ser big-endian o little-endian, o sin especificar). (Introducido en Windows XP)

Fuente: http://es.wikipedia.org/wiki/Registro_de_Windows

Sub arboles

El registro comprende varias secciones lógicas o "subárboles". Se nombran según las definiciones de sus *API de Windows*, las cuales

empiezan siempre por "HKEY". Técnicamente, se trata de indicadores predefinidos para claves específicas que se mantienen en la memoria o se almacenan en archivos de subárbol almacenados en el sistema de archivos local y cargado por el kernel del sistema en el tiempo de arranque.

Existen 7 claves raíz predefinida, nombradas según su identificador constante definido en la API de Win32:

HKEY_LOCAL_MACHINE (HKLM): almacena configuraciones específicas del equipo local.

HKEY_CURRENT_CONFIG(HKCC):información recogida en tiempo ejecución.

HKEY_CLASSES_ROOT(HKCR): información sobre aplicaciones registradas.

HKEY_CURRENT_USER (HKCU): almacena configuraciones específicas del usuario

HKEY_USERS (HKU): contiene subclaves correspondientes a las claves HKCU.

HKEY_PERFORMANCE_DATA: proporciona información del tiempo de ejecución mediante datos de rendimiento proporcionados por el propio kernel NT.

HKEY_DYN_DATA: Contiene información sobre dispositivos de hardware.

d). Enumeración LDAP (*L*ightweight *D*irectory *A*ccess *P*rotocol)

Es el “Protocolo Ligero de Acceso a Directorios”, que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversas informaciones en un entorno de red. LDAP es un protocolo diseñado para trabajar junto al protocolo TCP/IP con la finalidad de extraer información desde un directorio jerárquico. LDAP está basado en el protocolo X.500 y fue creado para poner a disposición de los creadores de directorios un protocolo de fácil manejo, permitiendo a las aplicaciones y a los directorios comunicarse entre sí. (Jimeno: 2012. 125)

2.2.15. Enumeración en sistemas Linux/Unix

Las técnicas de enumeración en los sistema Linux/Unix son completamente distintas en función de los servicios que estos tengan activos. Si el sistema Linux, por ejemplo, tiene instalado un servidor Samba, su comportamiento es muy similar al de un sistema Microsoft Windows. Uno de los puntos más débiles de los sistemas Linux/Unix sea el servicio finger, que normalmente se encuentra ejecutando en el puerto 79. Este servicio proporciona de forma gratuita información básica sobre los usuarios de un sistema. La manera de explotar dicha debilidad es tan simple que basta ejecutar el comando TELNET dirigiéndolo sobre dicho puerto y escribir de forma aleatoria un nombre de usuario.

En el caso de que este usuario este dado de alta en el sistema nos aparecerá toda su información de la cuenta. No proporciona la contraseña, pero tenemos el nombre, apellidos, shell y un montón de información más.

A partir de ese instante se puede comenzar un ataque de ingeniería social, o simplemente probar a usar como contraseña combinaciones de letras, realizando un ataque de los conocidos como fuerza bruta. Algunos sistemas son capaces de detectar este tipo de ataques y pueden bloquear automáticamente la cuenta de ese usuario, además de advertir al administrador del sistema y al propio usuario.(Jimeno: 2012:125)

Según Jimeno, hay 3 técnicas de enumeración en sistemas Linux/Unix.

- El uso fraudulento del finger.
- El uso de los servicios SNMP (Simple Network Manager Protocol).
- El uso de los sistemas NFS (Network File System), que es algo similar a compartir carpetas dentro de entorno Microsoft Windows.

a). Enumeración SNMP (*Simple Network Management Protocol*)

El Protocolo Simple de Administración de Red, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento. (Jimeno: 2012. 126)

Componentes básicos de SNMP

Una red administrada a través de SNMP consiste de tres componentes:

- **Un dispositivo administrador** una ordenador conectada a la red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los sistemas de administradores de redes usando SNMP. Los dispositivos administradores de red (routers, servidores de acceso, switches, bridges, hubs, computadores, impresoras).
- **Un agente** un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.
- Un **sistema administrador de red** ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados

2.2.16. Herramientas de enumeración

Estas herramientas llevaran a cabo un gran número de escaneos y técnicas de enumeración para devolvernos toda la información que puedan recuperar de la maquina sobre quien las deseamos. (Jimeno. 2012:137)

En el 2012 Jimeno, describe algunas de las herramientas más utilizadas:

a) Comandos NET

- **NetAccounts***:* Gestiona la base de datos de cuentas de usuario y modifica los requisitos de contraseña e inicio de sesión para todas las cuentas.
- **NetComputer***:* Agrega o elimina equipos de la BD de un dominio.
- **NetConfig:** Muestra los servicios configurables que están en ejecución, cambia la configuración de un servidor o estación de trabajo.
- **NetContinue**: Reanuda un servicio que se suspendió con el comando hetpause.
- **NetFile***:* Muestra los nombres de todos los archivos compartidos abiertos en un servidor.
- **NetGroup:** Agrega, lista o modifica los grupos globales de un dominio.

b) **GetUsurInfo.** Utilidad para obtener información en el sistema Windows.

c) **NetScanTools.** Herramienta para realizar un gran número de escaneos en red, pues engloba rastreos de todo.

d) **LANguard.** Un magnifico servicio de enumeración y rastreo bajo entornos Windows. Nos devolverá todos los puertos, servicios y versiones que tiene un sistema.

e) **NetBrute.** Entre sus escaneos está el de enumeración NetBIOS. Nos da la posibilidad de escasear una maquina en concreto o directamente toda una red, para ver todas las maquinas conectadas a la misma.

2.2.17. Servicios de seguridad

En el contexto del modelo ISA (Interconexión de Sistemas Abiertos) un servicio de seguridad se va a suministrar como parte de un servicio de

nivel (N). Cada servicio de seguridad en el interfaz entre los niveles (N) y (N+1) está soportado por uno o más mecanismos incorporados a las entidades de nivel (N) y al protocolo de nivel (N). El estándar *ISO 7498; y e*l ISO 7498-2 define como el servicio proporcionado por un nivel de un sistema abierto que garantiza la seguridad. (Gómez. 2007:89)

En el 2007 Gómez, describe estos servicios en 5 categorías y 14 servicios específicos. Las categorías son:

A. Autenticación y autorización:

Asegura que las entidades que se comunican son quién reclaman ser. ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener. El estándar ISO 7498-2 define dos servicios autenticación específicos:

- Autenticación del origen de los datos
- Autenticación de entidades pares

B. Control de acceso:

Este servicio evita el uso no autorizado de los recursos.

C. Confidencialidad:

Según la norma ISO-17799, garantiza que la información sea accesible únicamente a aquellos autorizados a tener acceso. La criptografía asimétrica cumple este objetivo mediante el uso de algoritmos matemáticamente comprobados y el hecho de eliminar la necesidad de mantener la clave de codificación en secreto. Según Black las versiones de este servicio son:

- Orientada a conexión
- No orientada a conexión
- Selectiva
- Aplicada al análisis del trafico

D. *Integridad:*

La integridad de la información es “mantener los datos libres de modificaciones no autorizadas”. Un ejemplo puede ser una transferencia bancaria donde el campo “importe” pueda ser modificado para contener “1000” en lugar de “100”.

En 1990, Black define las modalidades de servicio de integridad así:

- Integridad orientada a conexión con mecanismos de recuperación
- Integridad orientada a conexión sin mecanismos de recuperación
- Integridad orientada a conexión sobre campos selectivos
- Integridad no orientada a conexión sobre campos selectivos

E. No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

- No repudio con prueba de origen
- No repudio con prueba de entrega

2.2.18. **Redes Privadas Virtuales VPN** (Virtual Private Network)

Una VPN es un mecanismo que permite establecer conexiones seguras, entre dos o más redes, a través de internet. VPN tiene por finalidad transportar datos de forma segura entre dos equipos de red.

Para llevar a cabo esta función se utiliza un canal seguro, llamado túnel de datos, por el cual viaja la información cifrada. (Jimeno: 2012:159)

Requerimientos básicos

- Identificación de usuario
- Administración de claves
- Codificación de datos
- Soporte a protocolos múltiples

2.2.18.1. **Tipos de VPN:**

En el 2012 Jimeno, define tres arquitecturas de conexión VPN:

2.2.18.1.1. **VPN de acceso remoto**

El más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas) (Gratton. 1998:159).

2.2.18.1.2. **VPN punto a punto**

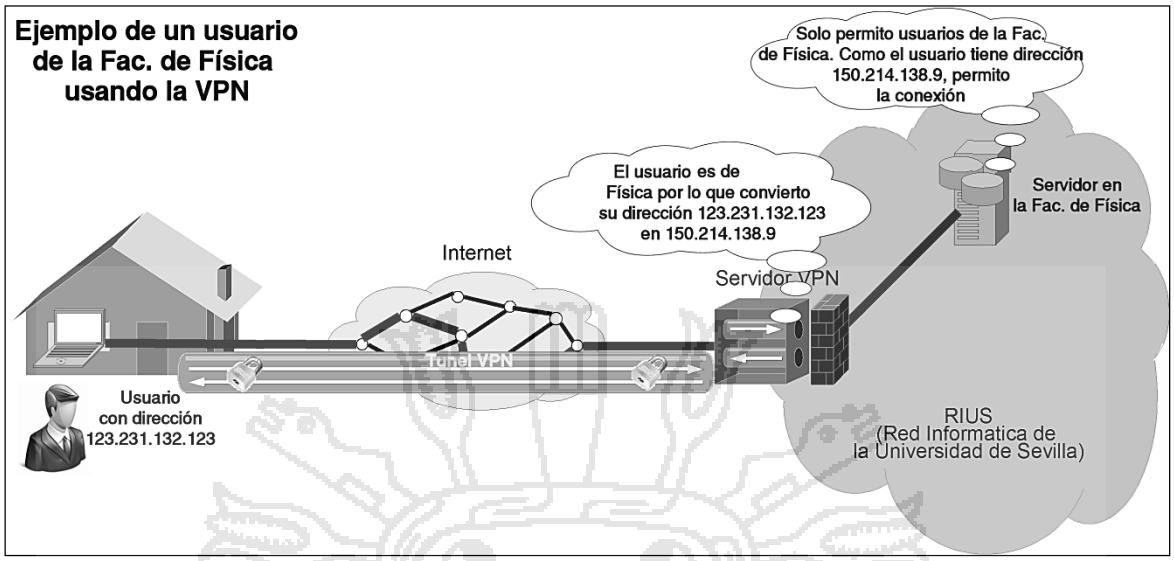
El esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN.

Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Permite eliminar costosos vínculos punto a puntos tradicionales, sobre todo en las comunicaciones internacionales. (Gratton. 1998:160)

Según Jimeno, esta configuración puede ser de dos tipos:

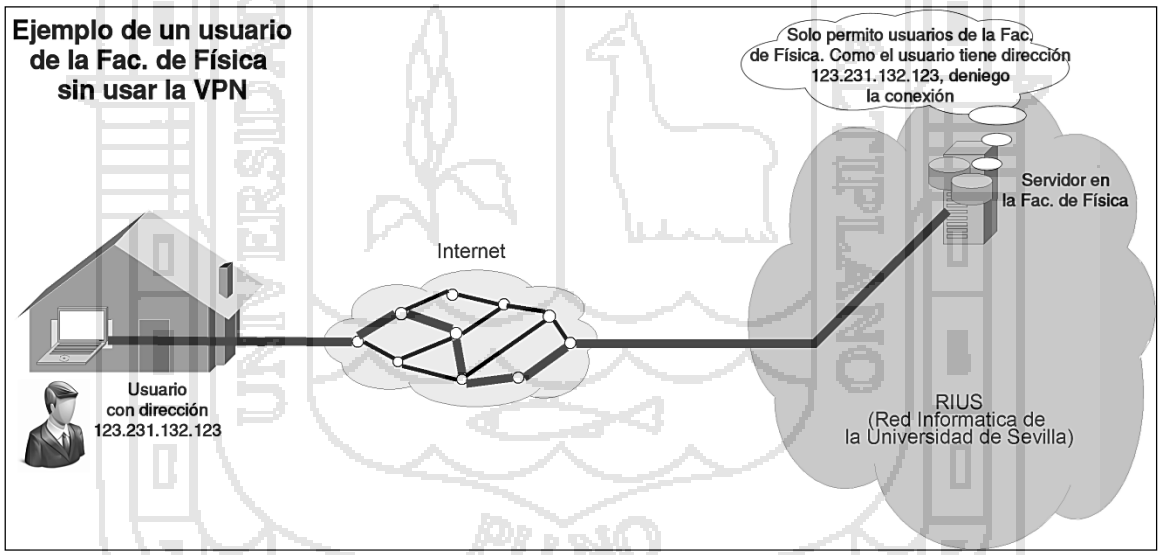
- **Tipo Intranet**, si la empresa tiene sucursales remotas que quiere unir en una única red privada, puede hacerlo creando una VPN para conectar ambas redes locales.
- **Tipo Extranet**, cuando la empresa tiene una relación cercana con otra compañía (una empresa asociada, un proveedor o cliente), entonces pueden desarrollar una VPN que conecte sus redes y permita a estas empresas trabajar en un ambiente compartido. Es más común el punto anterior, también llamada tecnología de túnel.

FIGURA Nº 9: Ejemplo de un usuario de la Facultad Física usando VPN



Fuente: (Universidad Sevilla, España: http://www.vpn.us.es/presentacion.html)

FIGURA Nº 10: Ejemplo de un usuario de la facultad física sin usar VPN



Fuente: (Universidad Sevilla, España: http://www.vpn.us.es/presentacion.html)

2.2.18.1.3. **VPN interna WLAN**

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo “acceso remoto” pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios

de la red interna. Esta realiza para mejorar las prestaciones de seguridad de las redes inalámbricas (*https://es.wikipedia.org/wiki/Red_privada_virtual*)

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

2.2.18.2. ¿Por qué VPN?

Las VPN soluciona el problema de costos, que al utilizar un medio compartido (Internet) reducen considerablemente el costo. Además, compartiendo el medio de interconexión con el resto de la red, hace más fácil la gestión de los enlaces implicados y no requiere añadir líneas adicionales para obtener nuevas conexiones. Usando VPN se puede crear enlaces nuevos de manera simple y económica.

Otros factores de éxito de este tipo de redes son la flexibilidad y la capacidad de adaptación que permiten. Para establecer la conexión a una VPN, solo se necesita una conexión a internet siendo totalmente independiente de la tecnología de acceso utilizada es decir, se adaptan a cualquier tecnología como: ADSL, UMTS/GPRS. Por red telefónica básica “RTB” modem convencional, sobre redes LAN, ya sean cableadas o inalámbricas. (Jimeno 2012:160).

2.2.18.2.1. Implementaciones VPN

El protocolo estándar de hecho es el IPSEC, pero también tenemos PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de

clientes soportados. Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas. (Varios autores. 2000).

- **Las soluciones de hardware** ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Tenemos Sonic WALL, Symantec, Nokia, D-link, etc.
- **Las aplicaciones VPN por software** son configurables e ideales. El rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general.

  Ejemplo las soluciones nativas de Windows, Linux y los Unix en general. En ambos casos se pueden utilizar soluciones de firewall, obteniendo un nivel de seguridad alto por la protección y del rendimiento.

2.2.18.2.2. Ventajas y tipos de conexión VPN

En el 2012 Jimeno resume las ventajas y tipos de conexión VPN asi:

Ventajas de VPN

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costes y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

Tipos de conexión VPN

a) Conexión VPN de acceso remoto

Es realizada por un cliente de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y este se autentica al servidor de acceso remoto, y el servidor se autentica ante el cliente.

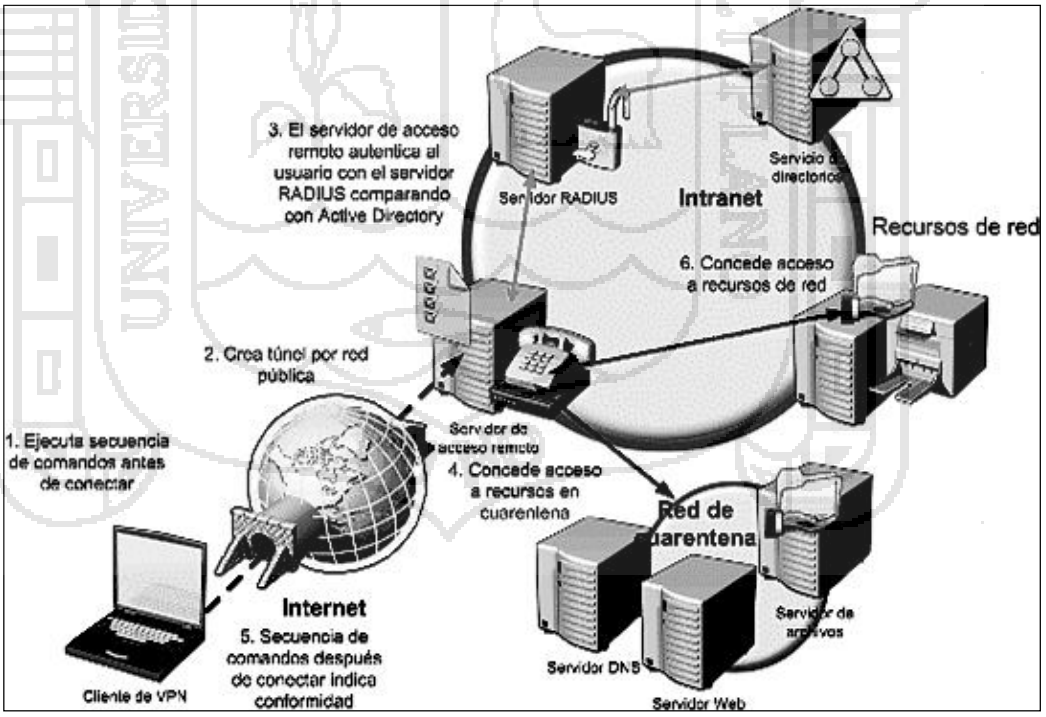
b) Conexión VPN router a router

Es realizada por un router, conectada a una red privada. Los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router receptor, y este a su vez se autentica ante el router emisor. Sirve para la intranet.

c) **Conexión VPN firewall ASA a firewall ASA**

Es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentica ante el que responde y éste a su vez se autentica ante el llamante.

FIGURA Nº 11: Esquema de Seguridad en Comunicación VPN



Fuente: http://www.ekontsulta.net/ekontsulta/wiki/index.php/VPN

2.2.18.3. **Tecnología de Túnel**

Esta tecnología está basada en estándares, permite transmitir datos entre dos redes similares. Llamado “encapsulación”, es decir, la tecnología que coloca paquetes dentro de otro protocolo TCP. (Jimeno. 2012:162)

Esta técnica de tunneling consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure Shell), a través de la cual se realizan las transferencias seguras. De esta manera la utilidad de un sniffer es bloqueada en la red (Lucena 2000:78).

Según Jimeno, existen dos tipos de túneles:

2.2.18.3.1. **Túneles de capa 2, basados en el transporte.**

Se utilizan en las conexiones a servidores que se realizan a través del modem. Existen tres protocolos para proteger la información en redes:

- ***PPTP (Protocolo de túnel punto apunto):*** El primero en establecer una comunicación segura, entre un equipo y un servidor de acceso, en forma de túnel virtual. La autenticación realizada es de tipo PAP (Protocolo de Autenticación de Contraseñas) y CHAP (Protocolo de Autenticación por Desafío Mutuo). Esta no se utiliza como VPN, debido a vulnerabilidades de autenticación que presenta.
- ***L2F (Reenvío de capa 2):*** desarrollado por CISCO, utiliza PPP (Protocolo Punto a Punto) para autenticarse, añade autenticación mediante RADIUS.
- ***L2TP (Protocolo de túneles de capa 2):*** consta de dos tipos de mensajes: Los mensajes de datos contiene el paquete original encapsulado, y de control aseguran que los datos lleguen a su destino correctamente.

2.2.18.3.2. **Túneles de capa 3, basados en el enrutamiento**.

Los túneles GRE (Encapsulamiento de Ruta Genérica) son estáticos y se pueden utilizar para encapsular y transportar cualquier tipo de protocolo. La forma más habitual de trabajar es creando interfaces virtuales en los elementos a comunicar. Con este procedimiento se utiliza un rango de direcciones IP y se encamina el tráfico a través de la interfaz creada.

2.2.19. **Seguridad IP en comunicaciones VPN mediante IPsec**

Para crear un canal seguro en las comunicaciones entre dos extremos, es prioridad utilizar IPsec. IPsec es un protocolo que implementa un conjunto de mecanismos de seguridad para asegurar la información transmitida entre los extremos de un túnel. De esta forma se evita, mediante mecanismos de cifrado y autenticación, la lectura y modificación de la información transmitida de forma no autorizada. (Jimeno: 2012. 163).

Funcionamiento de IPsec

Según Caballero, la implementación se puede realizar de dos formas:

- ***Modo Transporte:*** método utilizado en comunicaciones entre dos elementos conectados directamente a internet y entre los que no existen elementos que realicen traducciones de direcciones IP (NAT) ni de puertos (PAT).
- ***Modo Túnel:*** cada paquete, al pasar por el Gateway de seguridad, es encapsulado dentro de un paquete IPsec, añadiendo cabeceras que posteriormente serán eliminadas al llegar al destino, obteniendo el nuevo paquete original.

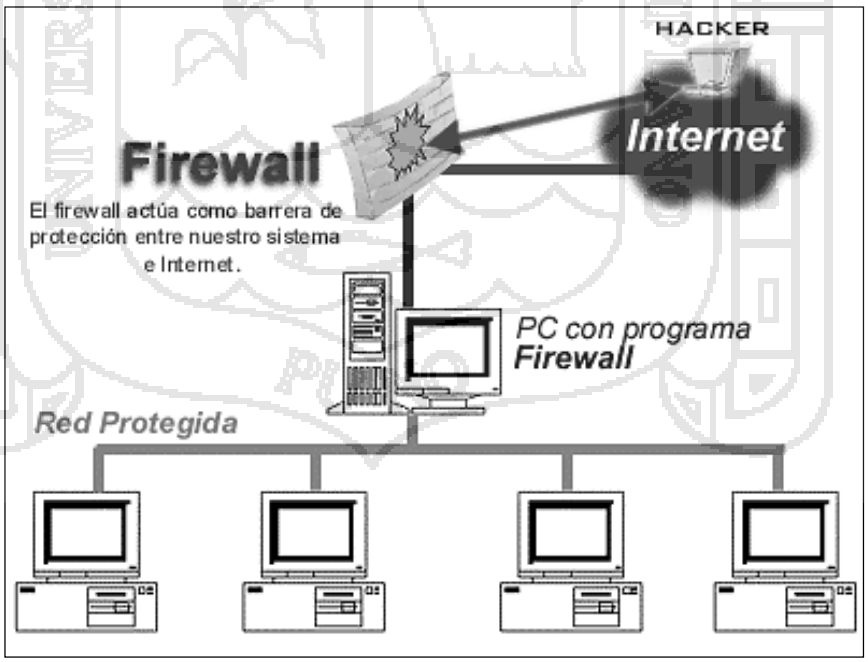
2.2.20. Firewall o cortafuegos

Es un software que permite o no el acceso de información por los diversos puertos TCP y UDP del ordenador atendiendo a una serie de directivas previamente configuradas para conseguir que nadie ajeno a nuestro entorno pueda acceder a los equipos de nuestra red.

Un cortafuegos podría asemejar mucho a la puerta de una casa, es decir nosotros solo abrimos la puerta de nuestra casa a las personas que querramos o que no tengan amenaza. Pero los que llaman a la puerta son los paquetes de datos, que vienen desde una determinada dirección IP, si esa dirección es sospechosa el cortafuegos no dejara que los paquetes enviados lleguen a su destino (Gomez 2007:339).

Una de las Ventajas es bloquear el acceso a personas y/o aplicaciones no autorizadas a redes privadas.(Jimeno: 2012:174)

FIGURA Nº 12: Esquema Firewall que protege a una red de una oficina



Fuente: (Hernández 2000.7. http://www.segu-info.com.ar/firewall/firewall.htm)

2.2.20.1. Tipos de cortafuegos

En el 2012 Jimeno identifica los siguientes tipos de cortafuegos.

- **Firewalls personales** (software) Los más conocidos: Zone Alarm Firewall, PC Tools Firewall, Look n Stop, Agnitum Outpost Firewall.
- **Enrutadores de Hardware**. no son firewalls realizan funciones, de disfrazar la dirección y puertos de su computadora a los intrusos.
- **Firewalls de Hardware**. Son costosos y complejos de manejar, son más apropiados para negocios con múltiples computadoras conectadas.

2.2.20.2. Políticas de los cortafuegos

En el 2012 Jimeno especifica dos políticas básicas en la configuración que cambian la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. Es la política más segura.
- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado

2.2.20.3. Limitaciones del Cortafuegos

Según Stallings, sistema firewall autoriza el paso del tráfico, y no puede:

- Ofrecer protección alguna una vez que el agresor traspasa a este.
- Proteger contra ataques que se realizan fuera del punto de operación.
- Proteger amenazas a que está sometido por usuarios inconscientes.
- Prohibir a los espías corporativos que copian datos sensitivos.
- Proteger contra ataques de la Ingeniería Social, ejemplo un hacker que pretende ser un supervisor o un nuevo empleado despistado.
- Proteger ataques a la red interna por virus a través de archivos y sw.
- Proteger fallos de seguridad de servicio, protocolos con tráfico permitido

2.3. Glosario de términos básicos

Modelo de seguridad

Es la presentación formal de una política de seguridad.

Modelo

Representación de la realidad por medio de abstracción de las propiedades. Identificación del conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada.

Política de seguridad

Conjunto de reglas para el establecimiento de servicios de seguridad

Modelo de seguridad de la información

Es un diseño formal que promueve consistentes y efectivos mecanismos para la definición e implementación de controles

Certificado SSL

Se utilizan para asegurar al visitante de un sitio web la autenticidad del mismo, asegurando que el sitio web es quien dice ser.

SSL (Secure Sockets Layer)

Sesión segura que protege la privacidad e integridad del mensaje. Protege los datos transferidos por http mediante el cifrado activado por un certificado SSL en un servidor. Los certificados SSL contienen una clave pública y otra privada.

HTTPS

Cifra y descifra las solicitudes realizadas por un visitante como la información que devuelve el servidor. Utiliza el puerto 443.

Seguridad de la Información

Su finalidad es la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Criptografía

Describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles utilizando algoritmo matemático, sin recurrir a una acción específica.

Algoritmo

Es el procedimiento paso a paso que convierte el mensaje original en un mensaje cifrado.

Llave o clave

Es un dato para el algoritmo con el cual se genera un mensaje cifrado tan complejo que es imposible deducir el mensaje original. La clave pública se utiliza para cifrar la información y la privada para descifrarla.

Seguridad Informática

Conjunto de normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Sitio web

Es un sitio (localización) en la World Wide Web que contiene documentos (páginas web) organizados jerárquicamente. Un sitio contiene una combinación de gráficos, texto, audio, vídeo, y otros materiales dinámicos o estáticos.

Página web

Cada documento (página web) contiene texto y o gráficos que aparecen como información digital en la pantalla de un ordenador.

Aplicación web

Es un conjunto de páginas que interactúan unas con otras y con diversos recursos en un servidor web, incluidas bases de datos. Esta interacción permite implementar características en su sitio como catálogos de productos virtuales y

administradores de noticias y contenidos. Adicionalmente podrá realizar consultas a bases de datos, registrar e ingresar información, solicitudes, pedidos y múltiples tipos de información en línea en tiempo real.

Red de Comunicaciones

Es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos, transmite datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc). La información se transmitir de forma analógica, digital o mixta. Las redes más habituales son ordenadores, teléfono, transmisión de audio (sistemas de megafonía o radio ambiental) y transmisión de vídeo (tv o vídeo vigilancia).

Suplantación

Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada desde su equipo, un atacante simula la identidad de otra máquina de la red, para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP.

Análisis y Diseño

Análisis es la descomposición de un todo, en partes para poder estudiar su estructura. Diseño es el proceso de plasmar el pensamiento de la solución, las alternativas mediante dibujos, esquemas trazados en cualquiera de los soportes, durante o posteriores a un proceso de observación.

Proceso

Es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias.

Dato

Unidad lógica de información que se suministra a la computadora.

Información

Una colección de datos no es información, los datos representan información de acuerdo a la medida de asociación existente entre ellos.

Servidor Web ó Servidor HTTP

Es un programa informático que procesa una aplicación del lado del servidor realizando conexiones bidireccionales y/o unidireccionales y síncronas y asíncronas con el cliente generando o cediendo una respuesta en cualquier lenguaje o aplicación del lado del cliente.

Criptografía Asimétrica

Es el método criptográfico o algoritmo que trabaja con dos llaves para el envío de mensajes, las dos llaves pertenecen a la persona remitente; una pública que se puede difundir por cualquier medio, la otra es privada que solo debe conocer el propietario.

Tecnología Web

Un conjunto de soluciones y servicios que nos permite asesorar, crear y consolidar proyectos de manera inteligente, destacando la elaboración de portales dinámicos, Web Sites, tiendas virtuales, hosting especializado, intranet-extranet.

Riesgo

Fines malintencionados para causar perjuicios a los usuarios a través del ordenador. Factores que componen son la amenaza y vulnerabilidades.

Vulnerabilidad

Es un defecto de una aplicación que puede ser aprovechado por un atacante. Si lo descubre, el atacante programa un software (malware) que utiliza la vulnerabilidad para tomar el control de esa máquina (exploit) y realizar una operación no autorizada.

Firewall o Cortafuegos

Sistema de seguridad que se compone de equipos (hardware) y de programas (software) en puntos claves de una red para permitir solo tráfico autorizado.

Amenaza

Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño sobre los elementos (activos, recursos) de un sistema.

Autenticación

Procedimiento de comprobación de la identidad de un usuario.

Ataque de Fuerza Bruta

Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras

2.4. Operacionalización de variables

CUADRO Nº 2: Sistema de variables

Variable General	Dimensiones	Indicadores	Categorías	Instrumentos
INDEPENDIENTE **Sistema Criptográfico**	Funcionalidad	Métrica de punto de Funciones.	• Esencial • Significativo • Medio • Moderado • Noinfluencia	Formatos de colección de información y observación
		Aceptación	• Excelente • Bueno • Regular • Malo • Muy Malo	Cuestionarios de encuesta y observación
DEPENDIENTE **Seguridad para las redes de comunicaciones**	Criterios de apoyo	Sobre la estructura y métodos destinados a proteger la información	• Total • Bastante • Regular • Mínimo • Ninguno	
		Servicios de seguridad contemplados y no contemplados en las redes computacionales		
		Integración con el entorno del proceso de comunicación.		
		Interacción con otras herramientas		

Fuente: Elaboración del autor

CAPITULO III.

DISEÑO METODOLÓGICO DE INVESTIGACIÓN

3.1. Tipo y diseño de investigación

La metodología utilizada es la investigación científica de tipo explicativa, descriptiva y evaluativa. Es investigación científica con la cual se identifica las principales técnicas en relación al análisis del modelo de seguridad para implementar la aplicación del sistema de seguridad criptográfico asimétrica.

Es "explicativo", porque están dirigidos a responder a las causas de los eventos, es decir por qué ocurre un fenómeno y en qué condiciones se da este (Sampiere 1991:67).

Es "descriptivo" por qué selecciona una serie de preguntas y se mide cada una de ellas, es decir se busca especificar las propiedades importantes del fenómeno que se ha sometido al análisis (Sampiere 1991:60).

La presente investigación también corresponde al diseño "explicativo" se ha explicado el efecto que causa la variable independiente sobre la variable dependiente. ¿Cuáles son los principales riesgos en las redes de comunicaciones?, ¿Existen herramientas tecnológicas que minimizan las vulnerabilidades sobre páginas web?, ¿Por qué implementar un modelo de sistema criptográfico de seguridad para las redes de comunicaciones?.

Se utiliza la metodología de programación orientada a objetos para diseñar el modelo de sistema criptográfico de seguridad para las redes de comunicaciones.

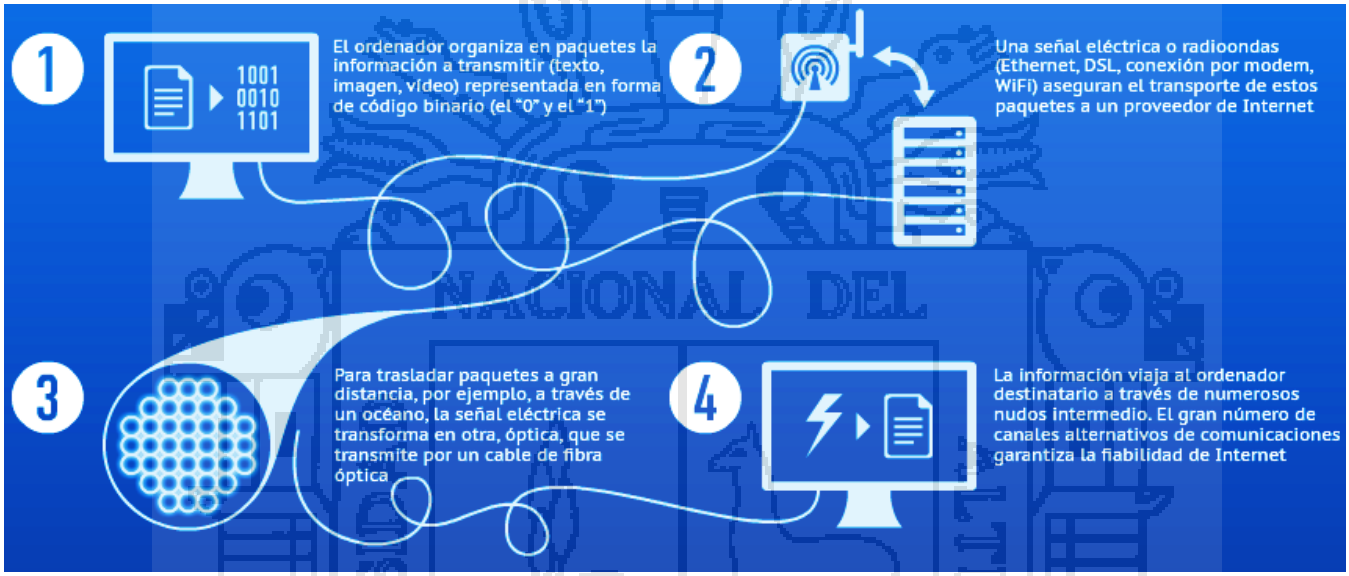
3.2. Población y muestra de investigación

La población está conformado por los usuarios de Internet.

3.2.1. ¿Cómo funciona transmisión de la Información?

Internet es un conjunto global de redes informaticas que usa el protocolo IP y el encaminamiento de paquetes de informacion.

FIGURA Nº 13: Esquema transmisión de la información

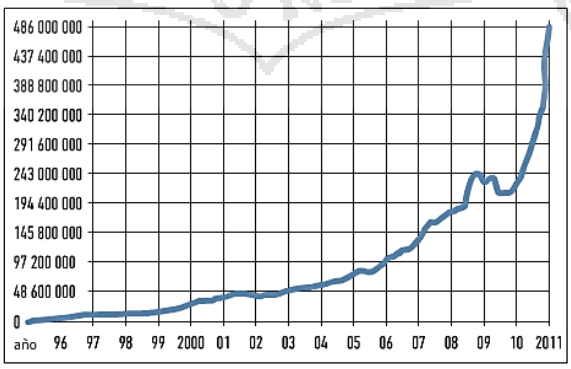


Fuente: http://sp.ria.ru/infografia/20111114/151569739.html

3.2.2. Número de sitios web en Internet

En el año 2011 se contabilizaron aproximadamente 485 173 671 Sitios web. Según la empresa Netcraft correspondientes a setiembre 2011.

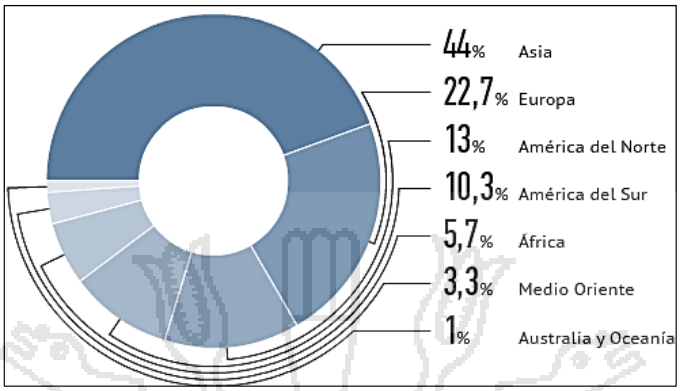
FIGURA Nº 14: Número de sitios web en internet



Fuente: http://www.netcraft.com/

3.2.3. Distribucion geográfica de los Internautas

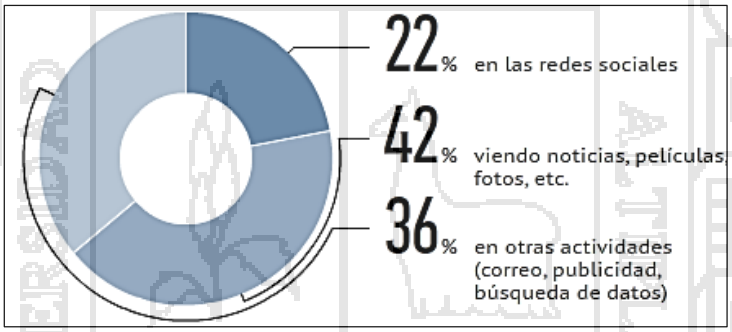
FIGURA Nº 15: Distribución geográfica de los internautas



Fuente: http://www.internetworldstats.com/stats.htm

3.2.4. Tiempo de uso de los internautas

FIGURA Nº 16: tiempo de uso de internet por los usuarios



Fuente: (Nielsen 2013. http://www.internetworldstats.com/usage.htm)

3.3. Ubicación y descripción de la población

El estudio del presente trabajo de investigación se realizó en el ámbito de la región puno perteneciente a república del Perú.

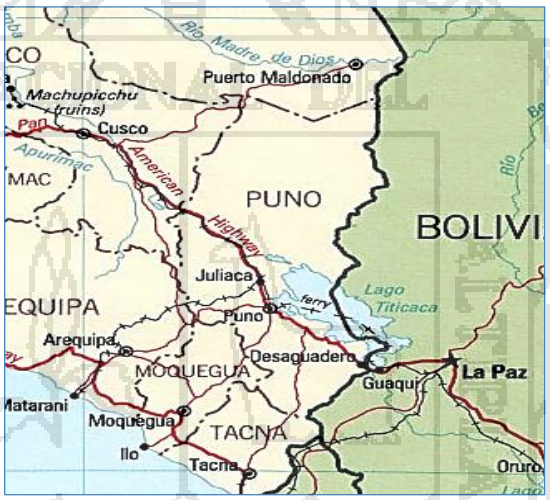
3.3.1. Características geográficas de la región puno

La región puno se encuentra ubicada geográficamente en la parte sureste del Perú, entre los 13°60´00" y 17°17´30" de latitud sur y los 71°06´57" y 68°48´46" de longitud oeste del meridiano de Greenwich. Tiene una superficie de 71,999 Km2 y políticamente está dividido en 13 provincias y 109 distritos.

La población total de acuerdo a las actividad censal del 2007 realizada por el INEI, la región Puno alcanzó 1, 268,441 habitantes y para el año 2010 la proyección es de 1, 352,523 habitantes ocupa el 21 lugar a nivel nacional y con una tasa de crecimiento del 1.13%. La población regional se encuentra constituida por dos culturas la colla y aymara.

Limita por el Norte con la región Madre de Dios, por el Este con la República de Bolivia y por el Oeste con las regiones de Moquegua, Arequipa y Cusco, y por el sur con la región Tacna.

FIGURA Nº 17: Mapa geopolítica de la región Puno



Fuente: http://www.zonu.com/peru_mapas/Mapa_Politico_Peru.htm

3.3.2. Área de estudio: Redes WAN

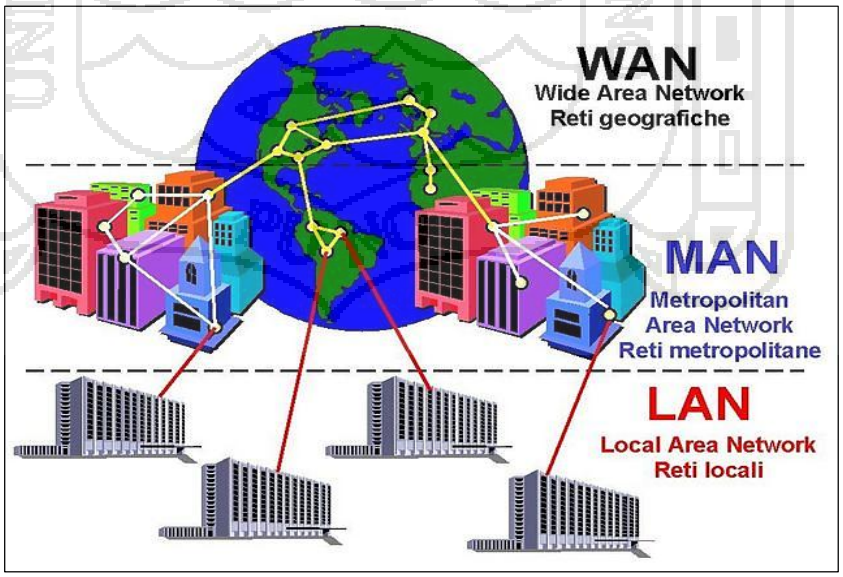
Una red de área amplia, o WAN, por las siglas de (*wide area network* en inglés), es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet (ISP) para proveer conexión a sus clientes.

Hoy en día, internet brinda conexiones de alta velocidad, de manera que un alto porcentaje de las redes WAN se basan en ese medio, reduciendo la necesidad de redes privadas WAN, mientras que las redes privadas virtuales que utilizan cifrado y otras técnicas para generar una red dedicada sobre comunicaciones en internet, aumentan continuamente. Las redes WAN usan sistemas de comunicación vía radioenlaces o satélite.

3.3.3. Características de Redes WAN

- Máquinas dedicadas a la ejecución de programas de usuario (hosts).
- Una subred, donde conectan varios hosts.
- División entre líneas de transmisión y elementos de conmutación (enrutadores).
- Es un sistema de interconexión de equipos informáticos geográficamente dispersos, que pueden estar incluso en continentes distintos. El sistema de conexión para estas redes normalmente involucra a redes públicas de transmisión de datos.

FIGURA Nº 18: Red de área amplia o WAN



Fuente: http://seguridadderedxd.bligoo.com.mx/mapa#first

3.4. Técnicas e instrumentos para recolectar información

Para la recopilación de datos del presente trabajo se tiene los recursos.

CUADRO Nº 3: Técnicas de recolección de datos

Método	Técnica	Instrumento
Investigación científica Explicativa, Descriptiva Evaluativa	Observación Revisión Literaria Aplicación	Encuesta Cuaderno de apuntes Eficiencia

Fuente: Elaboración del autor

3.5. Técnicas para el procesamiento y análisis de datos

3.5.1. Técnicas de observación directa

Técnica que permite obtener datos a través del tratamiento de la información expuestas en textos, internet que da entender sobre el tema

Se observa que China es el líder absoluto en 2008 por el total de ataques desde los recursos ubicados, así alojando programas dañinos.

CUADRO Nº 4: Ataques a través de la web

Lugar	País	Cantidad de ataques	Porcentaje del total de ataques
1	China	18.568.923	78,990%
2	EEUU	1.615.247	6,871%
3	Países Bajos	762.506	3,244%
4	Alemania	446.476	1,899%
5	Rusia	420.233	1,788%
6	Letonia	369.858	1,573%
7	Reino Unido	272.905	1,161%
8	Ucrania	232.642	0,990%
9	Canadá	141.012	0,600%
10	Israel	116.130	0,494%
11	Lituania	110.380	0,470%
12	Corea del Sur	46.167	0,196%
13	Hong Kong	44.487	0,189%
14	Estonia	41.623	0,177%
15	Suecia	40.079	0,170%
16	Francia	31.257	0,133%
17	Italia	29.253	0,124%
18	Brasil	25.637	0,109%
19	Filipinas	19.920	0,085%
20	Japón	16.212	0,069%

Fuente: (Gostev:2009. http://www.viruslist.com/sp/analysis?pubid=207271019)

Pérdida de privacidad y mecanismo para proteger la información en internet

Según Gartner aseguro que en 2011 solo un 7% de la información de los usuarios finales fue almacenada en la nube, sin embargo, se espera que para el año 2016 dicho porcentaje aumente a un 36%. Por otro lado la publicación "Global Cloud Index" de Cisco, estima que en 2017 los usuarios de América Latina habrán almacenado una cantidad de 298 exabytes de información en la nube (1 billón de gigabytes). A continuación se muestra la tabla Nº 5 en donde se proyecta el crecimiento de la nube en varias regiones del mundo y la cantidad de datos almacenados (expresados en Exabytes).

CUADRO Nº 5: Crecimiento de almacenamiento de información en la nube

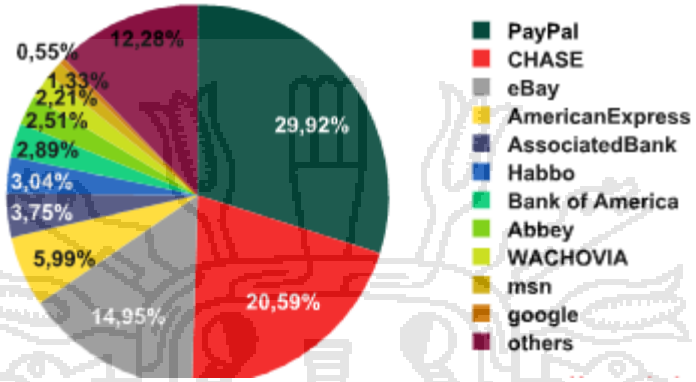
REGION	AÑO						Crecimiento Porcentual (2012-2017)
	2012	2013	2014	2015	2016	2017	
América latina	77	117	159	203	249	298	31%
Asia pacifico	319	505	736	1042	1415	1876	43%
Europa central y oriental	69	101	140	191	253	325	36%
Oriente medio y áfrica	17	31	51	77	112	157	57%
Norteamérica	469	691	933	1211	1526	1886	32%
Europa occidental	225	311	400	501	623	770	28%

Fuente: (Equipo de investigación ESET Latinoamérica "tendencias 2014": www.eset-la.com)

Los phishing demostraron interés con más frecuencia por el sistema PayPal, y no tanto por la información confidencial de los clientes de los bancos (Bank of América). Un hecho destacable es que Chase Manhattan Bank sólo sufrió ataques sólo en noviembre y diciembre de 2008, pero fueron de tal magnitud que el banco ocupó el segundo lugar en la lista de las organizaciones más atacadas.

Para no convertirse en víctima de los estafadores, basta que los usuarios recuerden que ningún sitio web serio solicita información confidencial a sus clientes después de seguir un enlace.

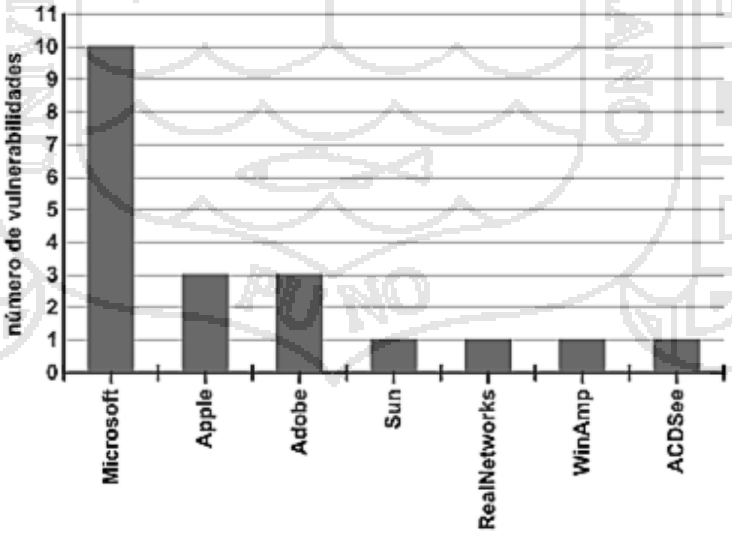
FIGURA Nº 19: Organizaciones más atacadas



Fuente: (Gudkova, Kulikova, Kalimanova, Bronnikova; 2009. http://www.viruslist.com/sp/analysis?pubid=207271020)

Aquí observamos en los productos de qué compañía se detectaron más vulnerabilidades 10 de cada 20 de las vulnerabilidades más difundidas son de Microsoft en 2008.

FIGURA Nº 20: Distribución de las vulnerabilidades por fabricantes

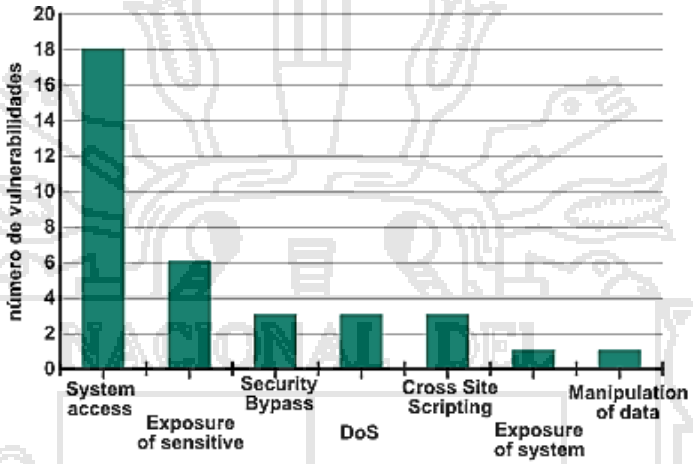


Fuente: (Gostev:2009. http://www.viruslist.com/sp/analysis?pubid=207271019)

.

Se observa en la figura sobre distribución de vulnerabilidades según consecuencias, que un numero de 18 vulnerabilidades abren brechas para obtener acceso al sistema, mientras que 06 pueden conducir a fugas de información importante.

FIGURA Nº 21: Distribución de vulnerabilidades según el tipo de consecuencia



Fuente: (Gostev:2009. http://www.viruslist.com/sp/analysis?pubid=207271019)

Vulnerabilidades en sitios latinoamericanos

En 2013, una de las principales tendencias que se analizó fue la propagación de códigos maliciosos utilizando un intermediario, servidor web que ha sido vulnerado por atacantes para tal propósito. De un total de 4500 sitios.

CUADRO Nº 6: Porcentaje de dominios gubernamentales por países

PAIS	Brasil	Argentina	México	Perú	Colombia	Ecuador	Nicaragua	Bolivia	R.D.	Otro
%	33	11	12	20	8	6	3	2	2	3

Fuente: (Equipo de investigación ESET Latinoamérica "tendencias 2014": www.eset-la.com)

De los códigos maliciosos que fueron alojados en dichos sitios, un 90% correspondían a troyanos y el 10% restante entre gusanos y backdoors. Respecto a páginas comprometidas de entidades educativas, México lidera con un 33%. Le siguen Perú y Argentina con un 17%.

CUADRO Nº 7: Porcentajes de dominios educativos por país

PAIS	Brasil	Argentina	México	Perú	Colombia	Ecuador	Nicaragua	El salvador	Otro
%	6	17	33	17	10	6	2	3	6

Fuente: (Equipo de investigación ESET Latinoamérica "tendencias 2014": www.eset-la.com)

3.5.2. Revisión literaria

Es la recopilación de la información requerida sobre textos, informes, etc. para la investigación con el fin de establecer las bases teóricas.

3.5.3. Recolección de datos

Estas provienen principalmente de dos fuentes.

Primarias, datos adquiridos a través de la encuesta dirigidos a usuarios de internet y expertos del área.

Secundarias, aquellos datos que serán elaboradas, adquiridas de las estadísticas contenidos en compendios, informes, boletines y así de internet.

3.6. Plan de tratamiento de los datos

Para el procesamiento de datos se utilizó las siguientes acciones.

- Recopilación y tabulación de datos
- Análisis y consistencia de la información

CAPITULO IV.

ANÁLISIS, E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

4.1. Análisis de la investigación

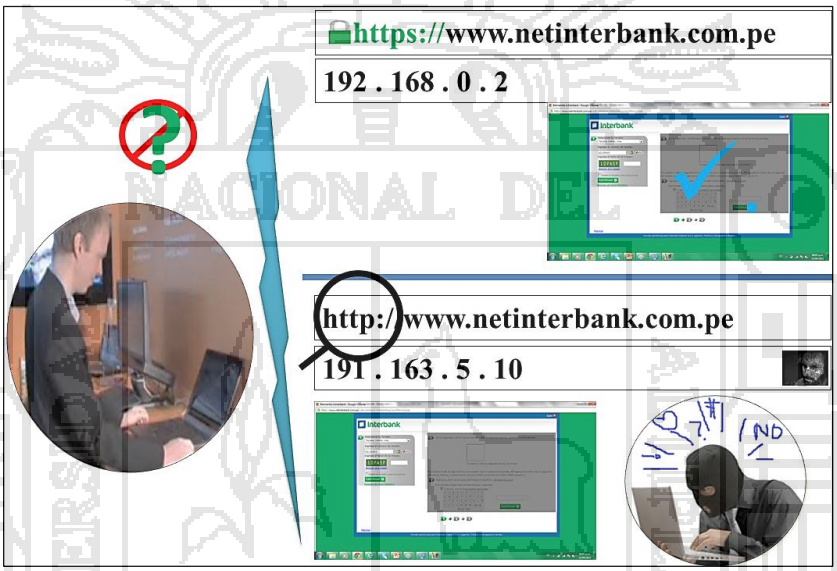
4.1.1. ¿Qué es el Phishing?

Es una modalidad de estafa con la finalidad de intentar obtener del usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Todos los datos posibles para luego utilizarlo de forma fraudulenta. Consiste en suplantar la imagen de una empresa, haciendo “creer” a la víctima que realmente los datos solicitados provienen del sitio "oficial” cuando en realidad no lo es. Realiza de varias formas como:

- ***SMS (mensaje corto)***; La recepción de un mensaje donde le solicitan sus datos personales.
- ***Llamada telefónica***; Pueden recibir una llamada telefónica en la que el emisor suplanta a una entidad privada o pública para que usted le facilite datos privados. Un ejemplo claro es el producido estos días con la Agencia Tributaria, ésta advirtió de que algunas personas están llamando en su nombre a los contribuyentes para pedirles datos, como su cuenta corriente, que luego utilizan para hacerles cargos monetarios.
- ***Página web o ventana emergente***; simula suplantando visualmente la imagen de una entidad oficial. La finalidad es que el usuario facilite sus datos privados. La más empleada es la "imitación" de páginas web de bancos, casi idéntico pero no oficial. Los sitios web falsos con señuelos llamativos, en los cuales se ofrecen ofertas irreales y donde el usuario novel facilita todos sus datos, un ejemplo Web-Trampa de recargas de móviles creada para robar datos bancarios.

- ***Correo electrónico***, la recepción de esta donde SIMULAN a la entidad que quieren suplantar para obtener datos del usuario novel. Estas son solicitados supuestamente por motivos de seguridad, mantenimiento de la entidad, mejorar su servicio, encuestas, confirmación de su identidad o cualquier excusa, para que usted facilite sus datos. aprovechan vulnerabilidades de navegadores y gestores de correos.

FIGURA Nº 22: Phishing suplanta la identidad del usuario para obtener información confidencial



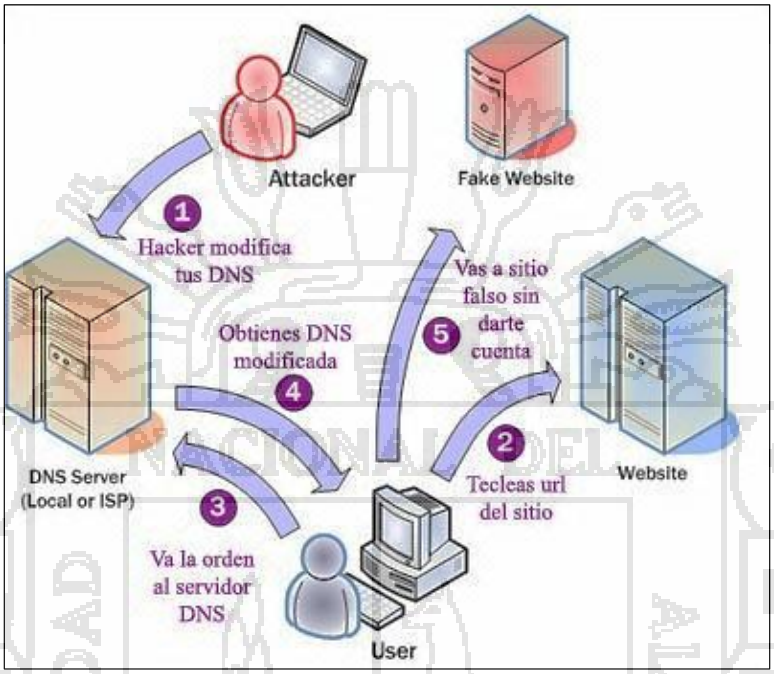
Fuente: Elaboración del autor

4.1.2. **Pharming**

Su finalidad es llevar al usuario a una página falsa para robarle la información personal, pero a diferencia del phishing utiliza técnicas muy diferentes, y estas engañan ya no al usuario sino al equipo o PC, para que resuelva las direcciones URL correctas y bien formadas hacia números IP diferentes de los originales y consecuentemente lleve al usuario a destinos no deseados. Con el pharming el usuario es más desprotegido debido a que la dirección o URL que está en el navegador es el correcto, aunque esté en realidad esta dirección le lleve a un servidor diferente. Su nombre

se debe principalmente a que al vulnerar un servidor DNS o un router todos los usuarios de ese servicio son víctimas probables, y si cualquiera de ellas introduce el URL correcto este será resuelto hacia el servidor del atacante.

FIGURA Nº 23: Tecnicas de ataque de pharming



Fuente: (Maulini: 2010. http://www.e-securing.com/novedad.aspx?id=45)

Según Maulini, esta técnica de ataque tiene tres variantes conocidas:

4.1.2.1. ***Pharming local:*** se realiza en el equipo del usuario, introduciendo un troyano o virus, que se encarga de alterar los registros de nombres que se encuentran en el archivo "hosts" (sin extensión).

4.1.2.2. ***Conducir por Pharming***: realiza atacando a los firewalls o routers, y cambiando la dirección del servidor DNS a la de un servidor DNS con el hacker, que seguro resolverá las direcciones tal como éste lo desee.

4.1.2.3. ***Envenenamiento de DNS:*** técnica que se basa en vulnerabilidades de los servidores DNS en lo que respecta al control de su caché de direcciones.

¿Cómo saber si ha sido víctima de un ataque de pharming?

- La técnica más usada es la de la infección del archivo host (pharming local). Busque el archivo host en su sistema y elimine cualquier línea con direcciones IP excepto aquella que define a "localhost" como 127.0.0.1
- Si tiene acceso a su router verifique que el número IP del servidor DNS configurado en el router sea el que le ha designado su proveedor de Internet o el administrador del sistema.

4.1.3. **Hacker**

Son usuarios con conocimientos muy avanzados en el funcionamiento interno de los ordenadores y redes informáticas. Aficionados con la seguridad en las redes, tratan de averiguar de qué forma se podría acceder a una red cerrada para luego arreglar ese error del sistema, desarrollan soluciones contra virus informáticos y programas que luego distribuye libremente. Son de la comunidad mundial que no oculta su actividad y que se ayuda mutuamente cuando hay necesidad, a través de foros de Internet o eventos sociales programados

4.1.4. **Crackers**

Son usuarios con conocimientos de redes e informática que persiguen objetivos ilegales, como el robo de contraseñas, destrozar la seguridad de una red doméstica o esparcir un virus informático a un gran número de computadoras. Realizan el trabajo buscando recompensas económicas (sustracción de dinero de tarjetas de crédito, estafas online). Un ejemplo sería infectar con un virus los ordenadores de una universidad determinada. En nuestras manos está la oportunidad de hacer cambiar este gran detalle.

4.2. Procedimientos de la investigación

4.2.1. Necesidad Creciente de Protección Denegación Distribuida de Servicios.

Una encuesta realizada por la compañía Verisign a responsables de tomar decisiones informáticas ha revelado algunos resultados alarmantes:

- El 63% de los encuestados experimenta un ataque DDoS el año 2013.
- De las empresas atacadas, 11% se vio afectado por seis ataques o más
- El 67% comentó que el tiempo de inactividad afectó a los clientes
- El 51% afirmó que habían perdido ingresos por el tiempo de inactividad

4.2.2. Ataques *DoS(Denial of service "denegacion de servicio")*

Son los ataques en ordenadores individuales o sitio web con la intención de negar servicios a los usuarios. Las agresiones pueden dirigirse a los sistemas de usuario final, servidores, enrutadores y vínculos de red. La técnica se basa en solicitar un recurso a un servidor web una gran cantidad de veces de forma que el servidor no pueda atender a otras solicitudes. Esta técnica no es efectiva es controlada por firewall.

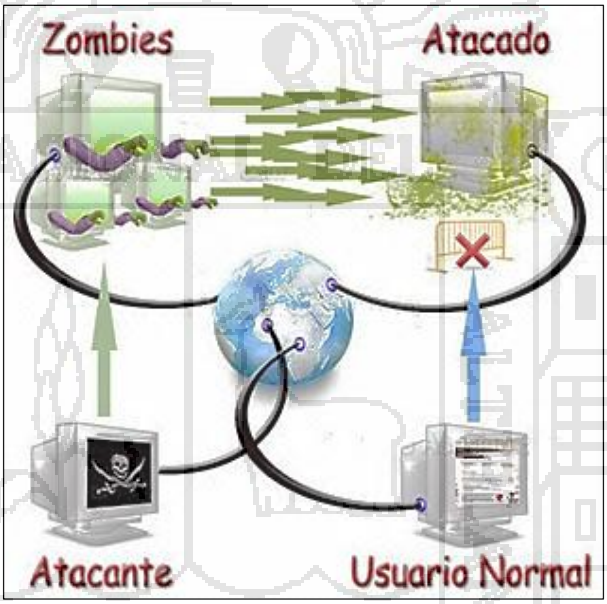
4.2.3. Ataque DDoS (*Distributed Denial of Service; Negación de Servicio Distribuida*).

***BotNet*.** Una 'botnet' es una cantidad de computadores conectados en Internet, sus propietarios pueden no ser concientes de ello. Estos computadores están en condiciones de realizar transmisiones (incluyen código malicioso, spam, virus, etc.) hacia otros computadores conectados también a la red. Estos computadoras son conocidos como 'zombies', un computador robot que actúa bajo el control de un computador maestro o controlador. Muchas de estas computadoras 'robots' son computadores instaladas en hogares.Las BotNets usualmente "pertenecen" a un Hacker.

Mientras más grande es BotNet, más "poderoso" es el hacker y más rápido y eficiente es el ataque.

El **DDoS** es un ataque de negación de servicio pero distribuido, ejecutado a través de una red de computadores zombies, difícil de detener, no se puede detectar el origen del ataque para bloquear la solicitud, estas no se aislan de los clientes reales. El cracker utiliza a **zombies** que atacan en grupos a diferente recursos.

FIGURA Nº 24: Ataque de denegacion de Distribuida de Servicios



Fuente: (College: 2010. https://itgscaso1.wikispaces.com/Ataque+de+denegacion+de+servicio)

Los ataques DDoS tienen como finalidad obtener un beneficio económico realizando colapsos en la red y ataques a los recursos de Internet de forma simultánea de varios puntos. Los equipos que se generan son los “Bots” o “Zombies”. Y estas realizan ataques de varias formas pero todas utilizan el protocolo TCP/IP para conseguir su propósito. Y básicamente consisten en :

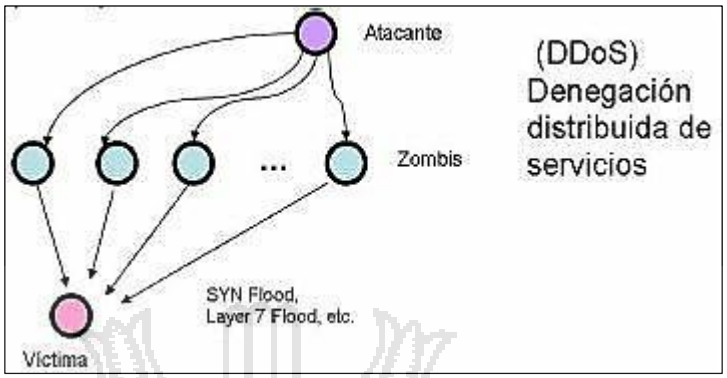
- Consumir recursos computacionales, ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, rutas de encaminamiento.
- Alteración de información de estado, como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima.
- **Bots o Zombies** son piezas de software ejecuta de manera autónoma una tarea en nombre de una persona o entidad. Realiza las siguientes actividades: *Búsqueda de información de forma automática, Contestar interrogantes, Informar cuando un evento se ejecuta, Provisión de noticias en la forma y tiempo deseado, Tutoría/asistencia inteligente, Buscar los mejores precios para un ítem, comportamiento malicioso*.

  Red organizada de clientes 'bots' maliciosos. Son la causa raíz de una serie de ataques informáticos, a saber: *DoS Distribuido, Spamming, Ataques click fraud, Robo de identidad, Otros que emergen y crecen con las redes sociales.*

4.2.4. Estructuras de Botnets

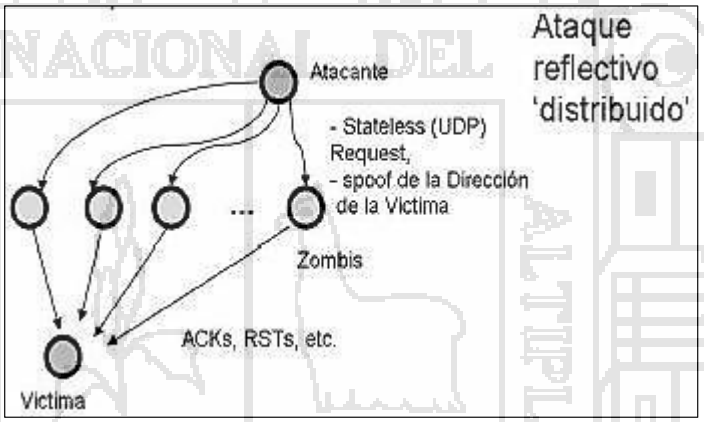
Está conformada con la generación de nuevas amenazas, con el crecimiento y perfeccionamiento de los ataques, sobre mecanismos de protección. Para evadir las detecciones básicas (protección a nivel 4), los Worms (código malicioso) se expanden a través de las aplicaciones (nivel 7). Para proteger, es necesario hacer análisis de todos los e-mail, tráfico P2P, IRC, y en general construir patrones de tráfico y comportamiento.

FIGURA Nº 25: Estructura de botnet usada para generar DDoS



Fuente: (Community Latam:2009. http://cxo-community.com/blogs/2142-ataques-de-seguridad-botnet.html)

FIGURA Nº 26: Estructura de botnet usada para ataques reflectivos



Fuente: (Community Latam:2009. http://cxo-community.com/blogs/2142-ataques-de-seguridad-botnet.html)

4.2.5. Funciones y tareas de los bots

Los bots ingresan secretamente en el ordenador del usuario, y se propagan por internet en busca de ordenadores vulnerables y desprotegidos a los que puedan infectar rápidamente e informan a su creador. Permanece oculto hasta que se les indique que realicen una tarea.

Una vez tomado el control de un equipo realiza las tareas como se muestra en la tabla Nº 8:

CUADRO Nº 8: Tareas automatizadas que realiza un bots en el ordenador del usuario

Enviar	Función (robar)	DoS (denegación de servicio)	Fraude mediante Clics
Envían - Spam - Virus - software espía	Robar información privada y personal y se la comunican al usuario malicioso: - números de tarjeta de crédito - credenciales bancarias - otra información personal y confidencial	Lanzan ataques de denegación de servicio (DoS) contra un objetivo específico. Los criminales cibernéticos extorsionan a los propietarios de los sitios web por dinero, a cambio de devolverles el control de los sitios afectados. Sin embargo, los sistemas de los usuarios diarios son el objetivo más frecuente de estos ataques, que sólo buscan molestar.	Los estafadores utilizan bots para aumentar la facturación de la publicidad web al hacer clic en la publicidad de Internet de manera automática.

Fuente: elaboración del autor

4.2.6. Selección y análisis de variables

Selección de variables.

La selección de variables para el trabajo de investigación corresponde:

Variable Independiente: Sistema Criptográfico

Variable Dependiente: Seguridad para las redes de Comunicaciones

Análisis de variables

La funcionalidad del sistema criptográfico se basa en algoritmos, protocolos para dar seguridad a los datos sobre las redes de comunicaciones. Esta gestión se logra con el diseño del modelo implementado e implantando.

Criterios de Apoyo de Seguridad para las redes de Comunicaciones

- Apoyo sobre la estructura y métodos destinados a proteger la información
- Apoyo en los servicios de seguridad contemplados y no contemplados en las redes computacionales
- Integración con el entorno del proceso de comunicación.
- Interacción con otras herramientas tecnológicas.

4.3. Diseño de soluciones

4.3.1. Análisis y diseño de sistemas de seguridad

Para desarrollar el proceso del diseño del modelo de sistema criptográfico se realiza un análisis exhaustivo de la situación actual de los sistemas y sus aplicaciones, desde el punto de vista de la seguridad y el hacking, identificando posibles problemas de riesgo y amenazas de ataques voluntarios, sus implicaciones en disponibilidad, confidencialidad e integridad. El mismo que fue elaborado bajo el modelo de proceso unificado de desarrollo de software.

Para tener un concepto amplio sobre el contexto de como es el proceso de modelo de sistema criptográfico de seguridad, se hace necesario el modelo de negocios del sistema en términos de casos de uso y actores respectivamente.

4.3.2. Caso de uso del negocio del proceso de técnicas de Phishing

En todo proceso de tecnicas de Phishing, hay muchas maneras de ataque la gran mayoría se basa en enviar e-mails aparentando ser de fuentes fiables y asi lograr datos confidenciales del usuario para realizar algun tipo de fraude.

En este proceso normalmente interactuan tres actores: usuario, administrador de redes y Phishing (Atacante). Las acciones que realiza el usuario en el proceso de tecnicas de phishing son:

Ingresa a nevegar en la web clon

Las acciones que realiza el phishing en proceso de tecnicas de ataque son:

Envia mensajes por telefono solicitando datos personales.

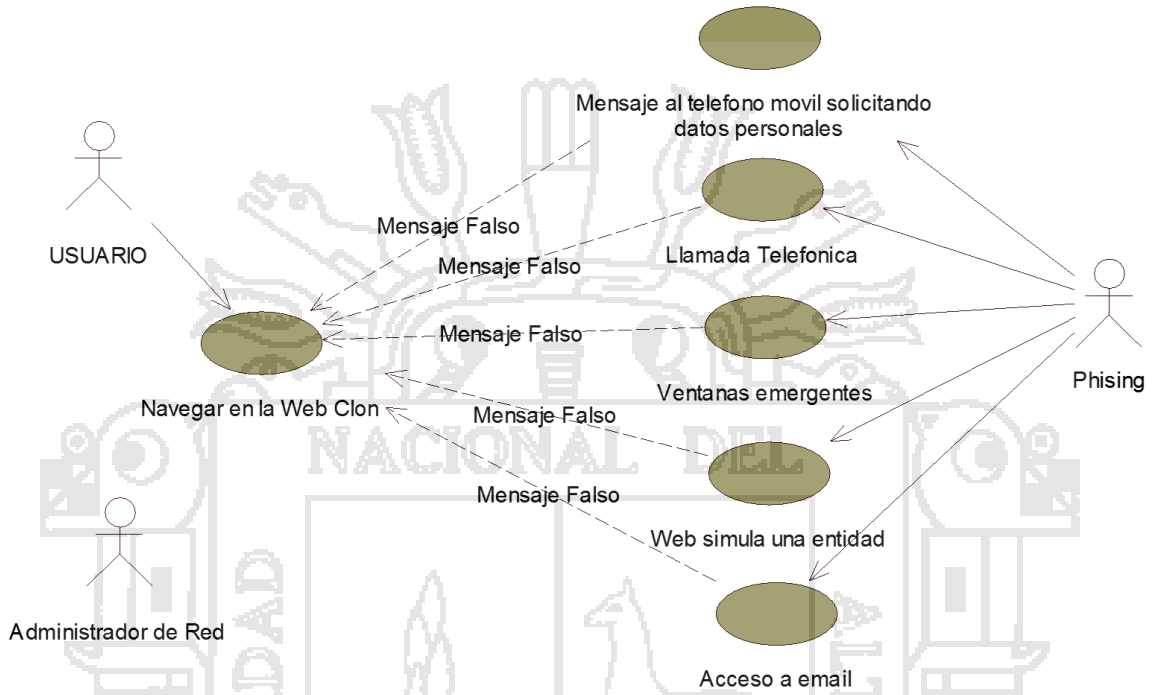
Realiza llamadas telefonicas a traves de la web clon

Envia ventanas emergentes hacia la web clon

Envia una web simulada de la entidad hacia la web clon

Accede a correo electrónico en la web clon

FIGURA Nº 27: Diagrama de casos de uso de técnicas phishing



Fuente: elaboracion del autor.

4.3.3. **Caso de uso del negocio proceso de "plan para un ataque web"**

En todo proceso de plan de ataque hacia una web, se realiza en primeramente la visita a la web del objetivo, luego creamos una pagina web HTML, muy parecido a la web comercial, para obtener y/o conseguir la información confidencial del usuario.

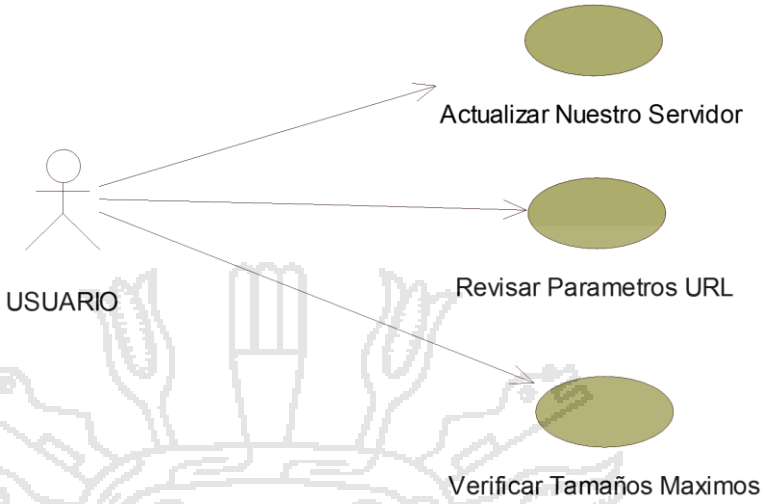
En este proceso, interactua solamente un actor: usuario, y realiza las siguientes tareas:

Realiza la actualizacion del servidor.

Realiza la revision de los parametros de la URL

Realiza la verificacion de los tamaños maximos

FIGURA Nº 28: Diagrama de caso de uso de un plan para un ataque web



Fuente: elaboracion del autor

4.3.4. **Caso de uso del negocio proceso de prevención de un ataque phising**

En todo proceso de prevencion de un ataque, primeramente debemos actualizar nuestro servidor con las últimas actualizaciones y parches, luego revisar las aplicaciones para que no puedan ser sensibles a ingresos de parámetros peligrosos.

En este proceso, interactua solamente un actor: usuario, y realiza las siguientes tareas:

No responde la solicitud de información personal a ningún e-mail.

Realiza la verificacion de la pagina web si es cifrada o no.

Realiza el ingreso de la URL en la direccion del navegador.

Realiza consultas frecuentemente sobre el saldo bancario y credito

Realiza informaciones a las autoridades de la empresa personalmente

FIGURA Nº 29: Diagrama de caso de uso de prevención de un ataque

Fuente: elaboracion del autor

4.3.5. **Caso de uso del negocio del proceso de acceso a un sistema a través de ataque phishing** .

En todo proceso de acceso a un sistema a través de ataque phishing, interactua solamente un actor: atacante phishing, y realiza las siguientes tareas:

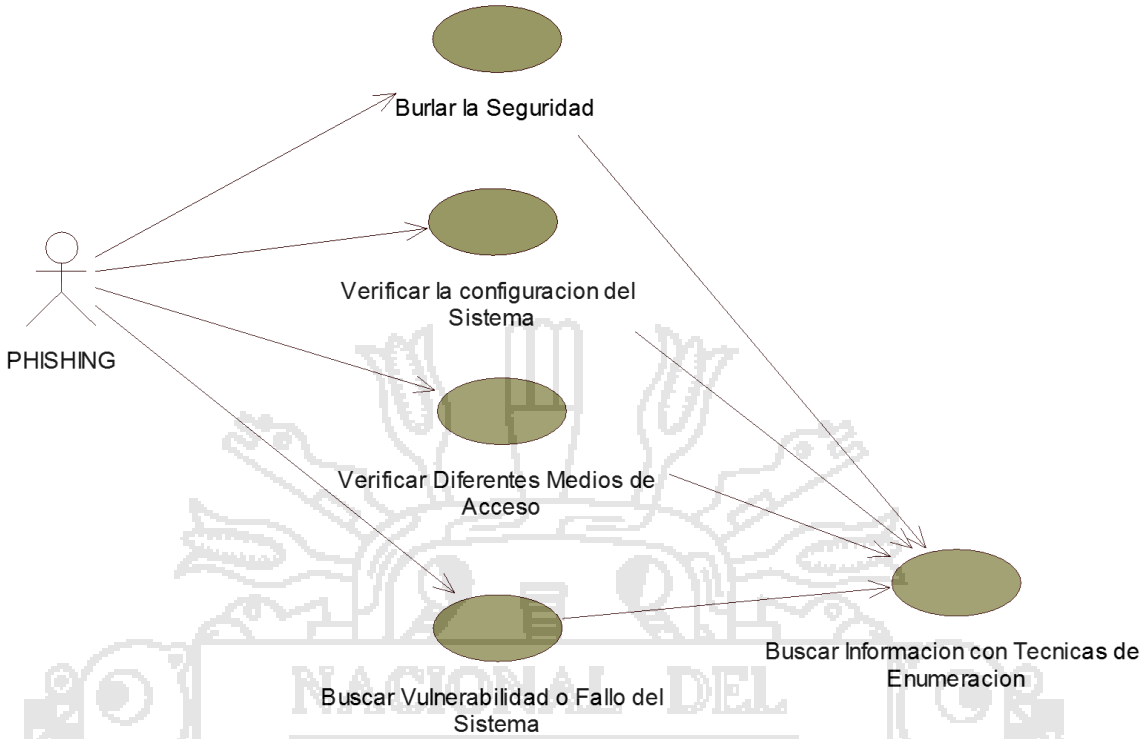
Ingresa logrando burlar la seguridad del sistema

Dentro del sistema verifica la de que manera esta configurado esta.

Logra obtener diferentes maneras de acceso al sistema

Verifica formas de fallo y/o vulnerabilidades del sistemas

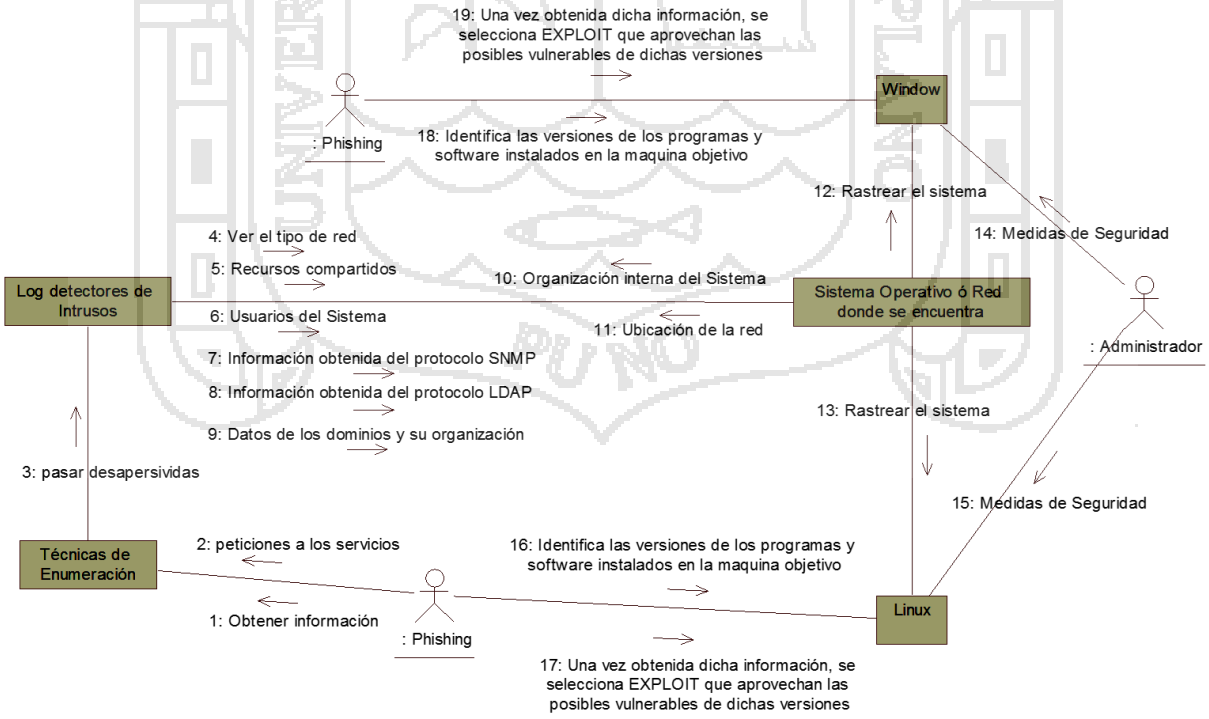
FIGURA Nº 30: Diagrama de caso de uso de acceso a un sistema a través de phishing



Fuente: elaboracion del autor

4.3.6. **Diagrama de colaboración de técnicas de enumeración de sistemas**

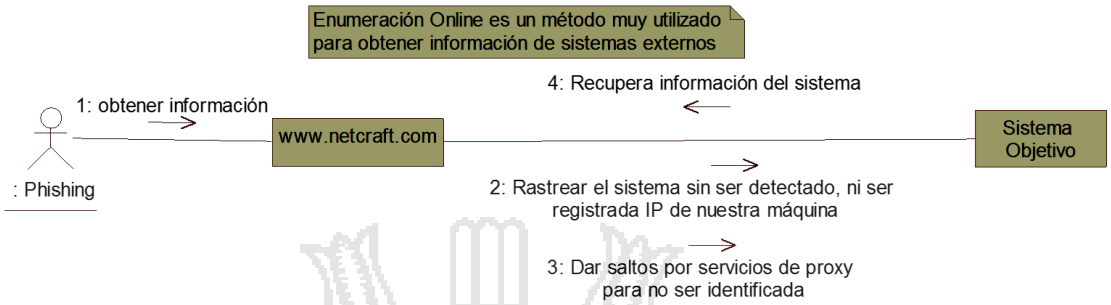
FIGURA Nº 31: Técnicas de Enumeración de Sistemas



Fuente: elaboracion del autor

4.3.7. Diagrama de colaboración de técnicas de enumeración en línea

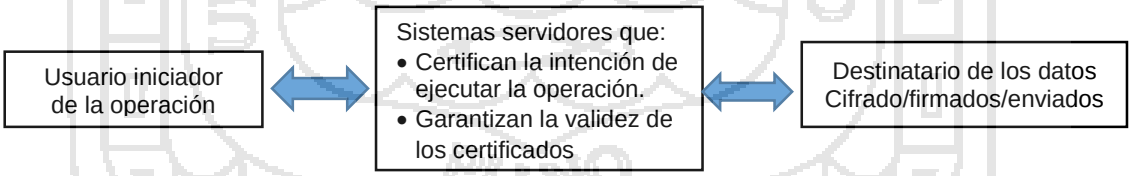
FIGURA Nº 32: Técnicas de Enumeración en Línea



Fuente: elaboracion del autor

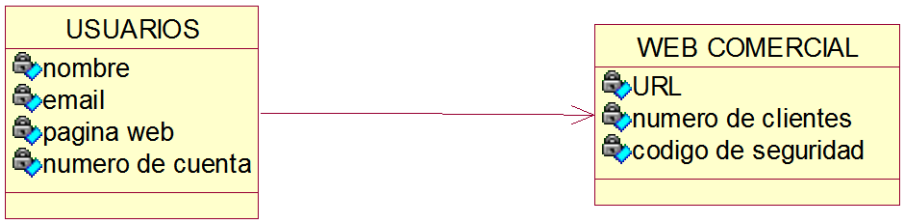
4.3.8. Autoridad de certificación (CA)

En criptografía una autoridad de certificación, es una entidad de confianza, responsable de emitir y revocar los certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía asimétrica. Autoridades de Certificación es el de *infraestructura de clave pública "PKI".* PKI es una combinación de software y hardware, políticas y procedimientos de seguridad que permiten ejecutar operaciones criptográficas, el cifrado, la firma digital o el no repudio de transacciones electrónicas, con las garantías necesarias. Las partes que intervienen cuando se usa PKI son:



4.3.9. Diagrama de base de datos de comercio electronico

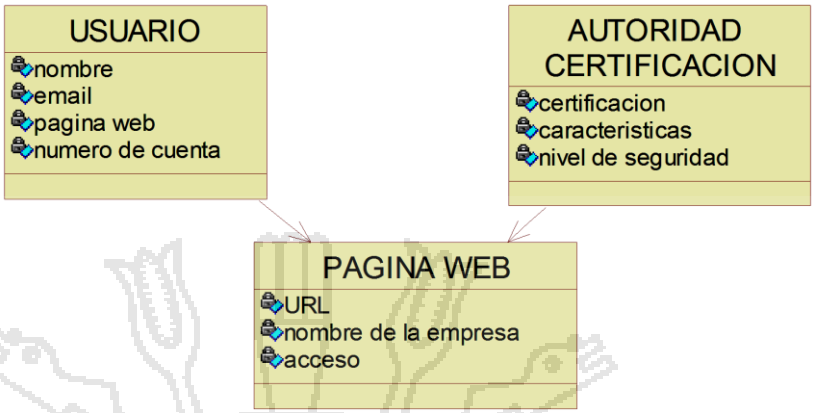
FIGURA Nº 33: Modelado de base de datos para comercio electrónico



Fuente: elaboración del autor

4.3.10. Diagrama de base de datos para cifrado de CA

FIGURA Nº 34: Modelado de base de datos para la Autoridad de Certificación



Fuente: elaboración del autor

4.3.11. Caso de uso del negocio del proceso autoridad de certificación.

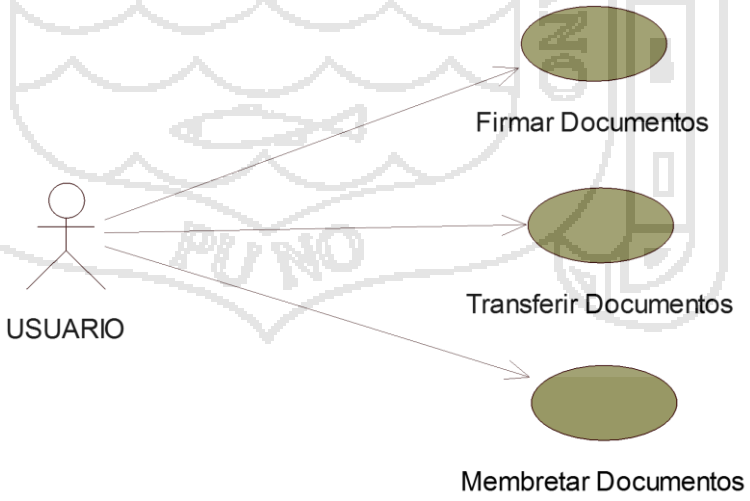
En todo proceso de autoridad de certificacion, interactua solamente un actor: usuario, y realiza las siguientes tareas:

Realiza la firma de documentos

Realiza la transferencia de documentos

Realiza la membretacion de documentos

FIGURA Nº 35: Diagrama de caso de uso de autoridad de certificacion



Fuente: elaboracion del autor

4.4. Implementación de soluciones del problema

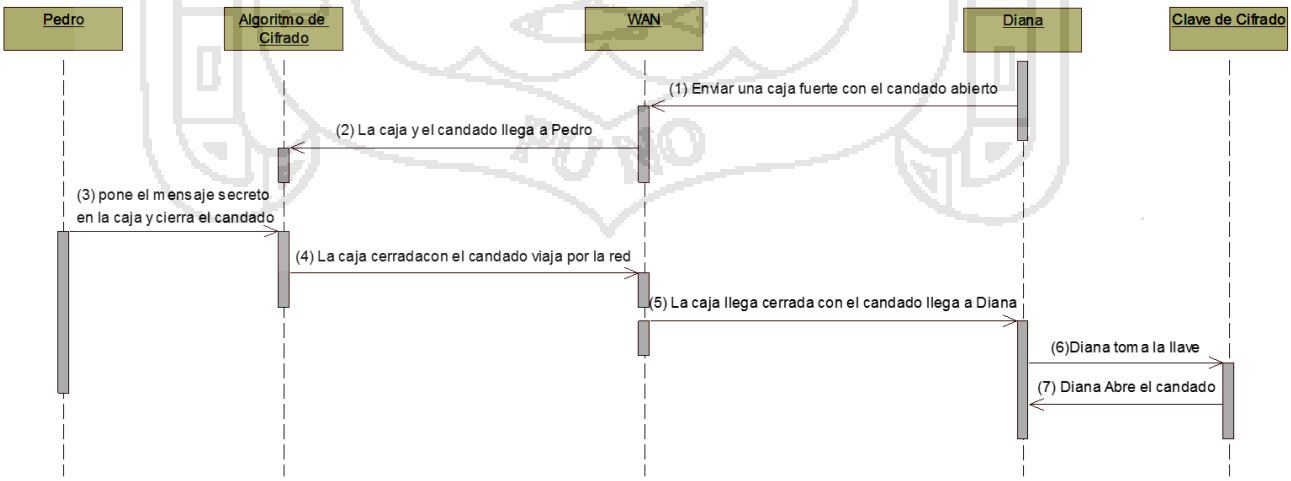
4.4.1. Diagrama de secuencia de procesos de cifrado con critpografia asimetrica

FIGURA Nº 36: Diagrama secuencia de procesos de cifrado asimétrica

Fuente: elaboracion del autor

4.4.2. Diagrama de secuencia de criptografia asimetrica

FIGURA Nº 37: Diagrama de secuencia de criptografía de Llave publica



Fuente: elaboracion del autor

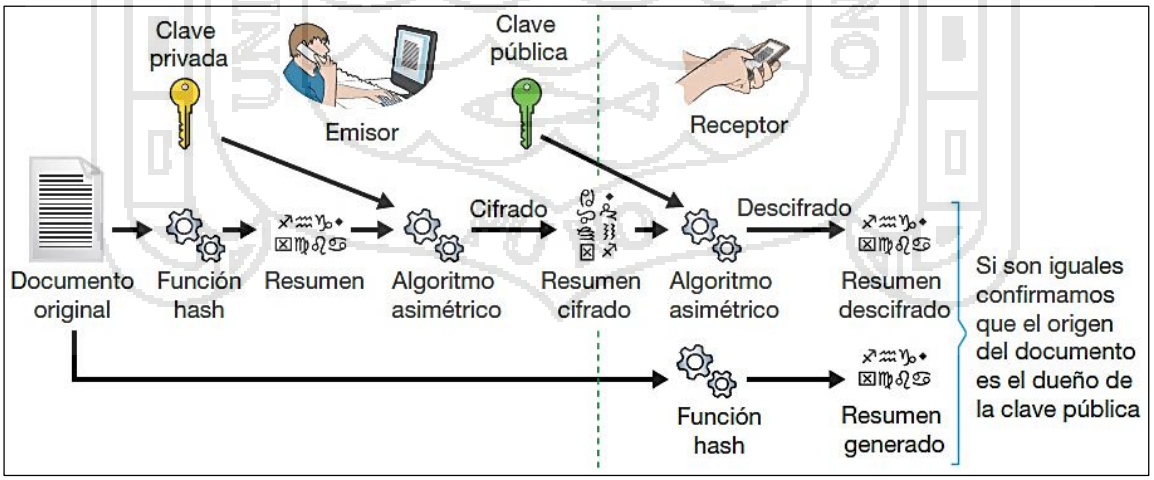
4.4.3. Certificado de clave pública o "Certificado"

Es una declaración firmada digitalmente que enlaza el valor de una clave pública con la identidad de un usuario, un dispositivo o un servicio que posee la clave privada correspondiente. La ventaja principal de estos, es que los "host" ya no tienen que mantener ningún conjunto de contraseñas para usuarios individuales que necesitan como requisito previo para autenticarse y así tener acceso. Por el contrario, el "host" simplemente establece la confianza en un emisor de certificados. Los certificados contienen la información siguiente:

- Valor de la clave pública del usuario
- Información del identificador del usuario (nombre, dirección e-mail).,
- Período de validez (tiempo de validación certificado).
- Información del identificador del emisor.

La firma digital del emisor, que da fe de la validez del enlace entre la clave pública del sujeto y la información del identificador de sujeto.

FIGURA Nº 38: Mecanismo de Firma



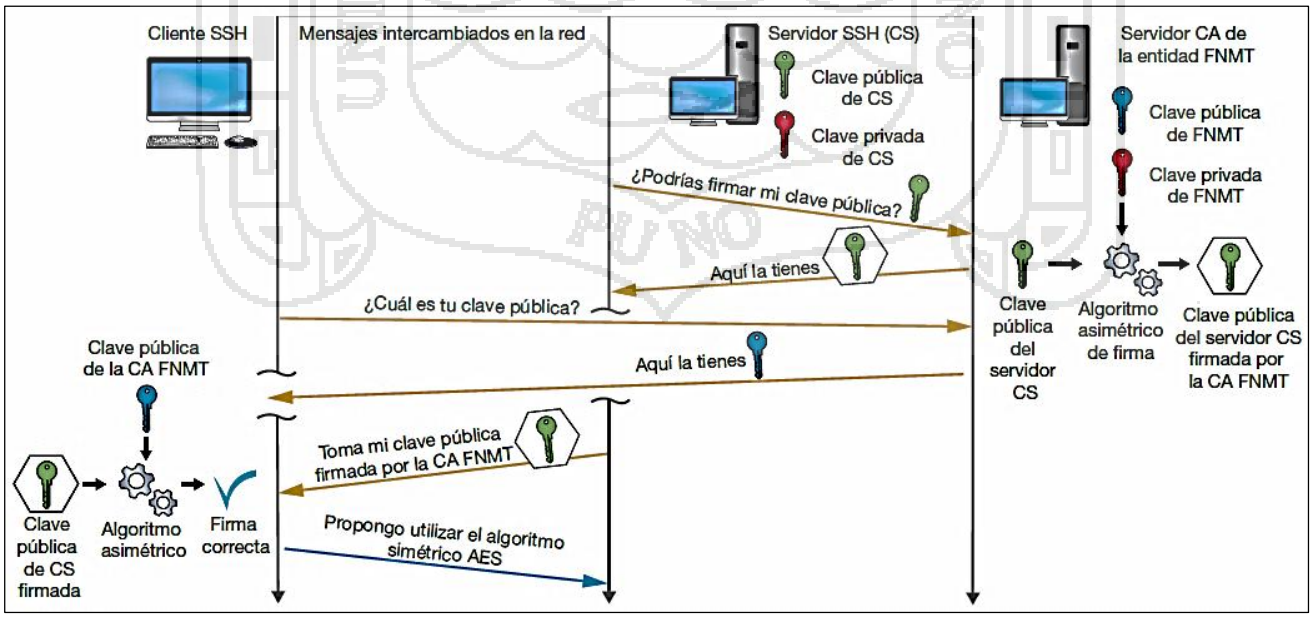
Fuente: (Roa: 2013. 40)

La mayoría de las comunicaciones seguras ocurren entre ordenadores muy alejadas entre sí que seguramente pertenecen a otras organizaciones. Por ejemplo, las oficinas virtuales de los bancos o el correo web (Gmail, Hotmail, etc). No podemos entras en sus ordenadores para ver las huellas, ni negociar con cada uno otro canal seguro donde poder consultar.

La solución a este problema es la implantación de un **PKI** (*Infraestructura de Clave Pública*). Ahora en la comunicación segura entre cliente y servidor aparecen nuevos interlocutores.

- **La Autoridad de Certificación** (CA). Cuya misión es emitir certificados.
- **La Autoridad de Registro** (RA). Responsable de asegurar que el solicitante del certificado es quien dice ser.
- **La Autoridad de Validación** (VA). Responsable de comprobar la validez de certificados digitales emitidos.
- **Los Repositorios.** Son almacenes de certificados.

FIGURA Nº 39: Funcionamiento de una PKI



Fuente: (Roa: 2013. 49)

Para que funcione la autenticación de una clave pública mediante PKI se necesitan dos pasos previos:

- El servidor ha conseguido que una CA le firme su clave pública. Por ejemplo VeriSign, FNMT, etc.
- El cliente dispone de la clave pública de esa CA dentro de su llavero de claves asimétricas.

4.4.4. Certificado SSL de VeriSign

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

Cuando se transfiere información de un servidor a otro, en una "puerta de enlace" de pagos, existen cierto tipo de ataques como el ataque "hombre en el medio" (man in the middle) que emplean las URLs de envío para infectar o robar nuestra información. La información en la web viaja desprotegida y visible a todo el mundo todo el tiempo. Entonces necesita cifrar para que solo el servidor y el usuario final lo puedan ver. Un certificado de seguridad hace imposible este tipo de ataques. Consta de dos partes:

- Certificado en el servidor de envío
- Certificado en el otro servidor de recepción

El certificado o ".cert" o ".crt" es un archivo cifrado que contiene la llave privada. Es necesario instalar el certificado en nuestro servidor. Uno de los certificados más conocidos es VeriSign. Poseen sus respectivos manuales.

El sitio no usa SSL. La mayoría de los sitios no necesitan usar SSL porque no solicitan información confidencial. Evita introducir información confidencial, como nombres de usuario y contraseñas, en la página.

Se ha establecido correctamente una conexión segura con el sitio. Busca este icono y asegúrate de que la URL tenga el dominio correcto si tienes que acceder al sitio o introducir información confidencial en la página.

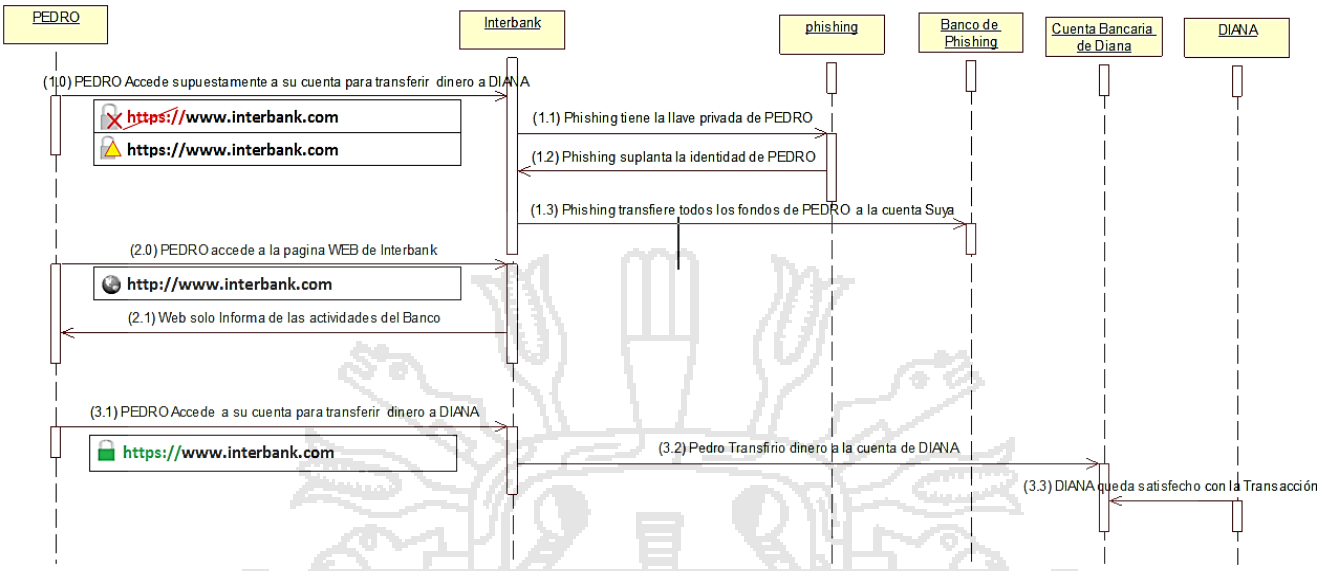
Si un sitio utiliza un certificado SSL con validación ampliada (EV-SSL), al lado del icono también aparecerá el nombre de la organización escrito en color verde. Asegúrate de que el navegador esté configurado en Comprobar la revocación del certificado del servidor para identificar los sitios con certificados EV-SSL.

El sitio usa SSL, pero Google Chrome ha detectado contenido que no es seguro en la página. Si vas a introducir información confidencial en esta página, ten cuidado. El *contenido peligroso puede ser una puerta de acceso para que alguien cambie el aspecto de la página*.

El sitio usa SSL, pero Google Chrome cree que el riesgo de que la página incluya contenido que no es seguro es alto o que puede haber una incidencia en el certificado del sitio. No introduzcas información confidencial en esta página. Un certificado que no es válido o la existencia de irregularidades graves en la **https**. *Podrían indicar que alguien está intentando manipular tu conexión al sitio.*

4.4.5. Diagrama de secuencia de transacción financiera y certificación SSL

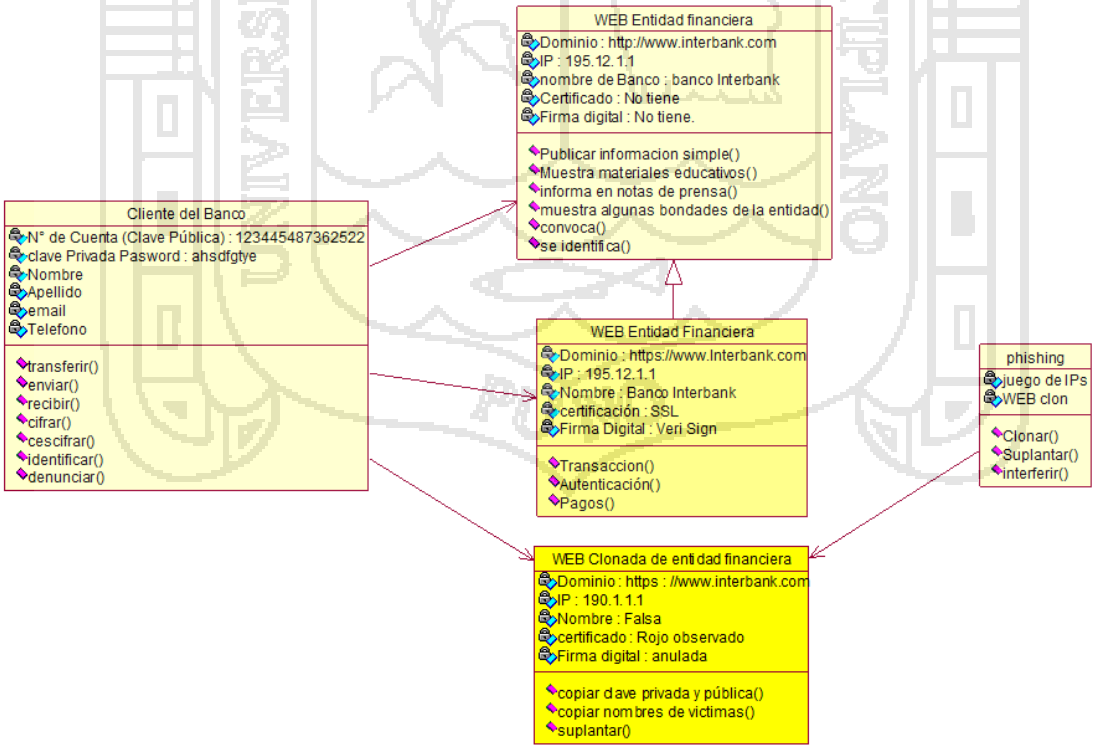
FIGURA Nº 40: Diagrama de secuencia de transacción financiera y SSL



Fuente: elaboracion del autor

4.4.6. Diagrama de modelo de clases para transacción financiera con CA

FIGURA Nº 41: Diagrama de modelo para transacción financiera y certificación SSL



Fuente: elaboracion del autor

4.5. Verisign frente a Denegación Distribuida de Servicios

Provee una solución integral para proteger las redes frente a las amenazas de DDoS, utilizando una tecnología de filtrado propia para detener un ataque DDoS en la nube antes de que ésta llegue a la red de algún cliente. Los servicios de inteligencia de red más disponibilidad de VERISIGN, contribuye a que las operaciones basadas en web se mantengan *seguras, disponibles y optimizadas*.

Posee un variado conjunto de soluciones de hardware y técnicas de mitigación, variedad de servicios de seguridad y telecomunicaciones desde certificados digitales, procesos de pagos y gestión de cortafuegos en llamadas de roaming por celular, etc. Entre los certificados digitales, se encarga de emitir los RSA para su uso en transmisiones seguras por SSL, especialmente para la protección de sitios con acceso por HTTPS; para hacer de Internet un lugar más seguro y fiable.

4.6. Servicio de mitigación de DDoS.

La más importante es mantener en funcionamiento los sistemas en línea, Al filtrar el tráfico malicioso en la nube, VeriSign detiene los ataques antes de que tengan la oportunidad de afectar de forma significativa a su red. Elimina la necesidad de hacer una provisión excesiva de ancho de banda para controlar el tamaño cada vez mayor de los ataques.

4.7. ¿Cómo funciona nuestra protección contra DDoS?

Cuando se detecta un evento malicioso, VeriSign redirige el tráfico dañino a un sitio de mitigación de VeriSign. La redirección y mitigación se produce en la nube antes de que pueda dañar su red.

Dado que VeriSign controla y analiza la información de los patrones de tráfico, las máquinas de seguridad empiezan a “limpiar” el tráfico desviado mediante el uso de las tecnologías de mitigación.

4.8. Los servicios de monitorización de VeriSign

- *Monitorización centralizada*. Proporciona una visión general de los patrones de red y tráfico, lo que mejora la posibilidad de iniciar estrategias de mitigación de forma rápida y segura.
- *Tráfico de red inicial*. Recopila paquetes de muestra pertinente de los conmutadores, routers y otros servicios para establecer una visión del tráfico normal. Incorporamos está a un motor de correlación para la detección, alertas e informes de amenazas.
- Tendencias históricas e inteligencia de amenazas mundiales
- Sistemas de alerta, registro y envío de informes orientados a DDoS.

Se reducen riesgo de ataques, combinando servicios de monitorización y mitigación. Detiene los ataques DDoS con el servicio de mitigación de DDoS basado en la nube de SSL Verisign.

4.9. ¿Cómo Protegernos de Phishing?

Tener un programa antivirus instalado y actualizado con filtro anti-spam. Además tener presente los consejos:

- Identificar correos electrónicos sospechosos de ser “phishing”
- Verificar la fuente de información.
- No acceder de la web hacia links.
- Comprobar sitio web, tiene dirección segura (**https://** y un pequeño candado cerrado debe aparecer en la barra de estado del navegador).
- Introducir los datos confidenciales en webs seguras.

- Revisar las cuentas para detectar transferencias irregulares.
- Phishing está presente en pagos por internet (PayPal, eBay, etc)
- El Phishing ya habla multitud de idiomas, entonces no confiar.
- Ante la mínima duda, abstente de facilitar información confidencial.
- Informarse sobre la evolución de sus técnicas de ataque.
- Las entidades bancarias no solicitan información confidencial a través de canales inseguros (e-mail).

4.10. Protección contra Bots

Los expertos en seguridad de Symantec aconsejan:

- Instale un software de seguridad de primera clase (Norton Internet Security)
- Configure el software para que se actualice de manera automática.
- Aumente las configuraciones de seguridad de su navegador.
- Limite los derechos de usuario cuando está en línea.
- No ejecutar los links adjuntos, a menos que pueda verificar su origen.

Configure los parámetros de seguridad de su equipo para que se actualicen automáticamente, a fin de asegurarse de tener siempre los parches más recientes del sistema.

4.11. ¿Cómo se realiza el cifrado de información con la Criptografía?

Consiste en tomar el documento original y aplicarle un *Algoritmo* cuyo resultado es un nuevo documento cifrado, y esta es ininteligible al leerlo directamente. Entonces podemos hacer llegar hacia el destinatario, quien sabrá aplicar el algoritmo para recuperar el documento original.

Para evitar a conocer la clave, tomaremos las siguientes medidas:

- Utilizar claves de gran longitud (512, 1024, 2048, 4096 bytes).

- Cambiar regularmente la clave.
- Utilizar todos los tipos de carácter posibles.
- Detectar repetidos intentos fallidos en un corto intervalo de tiempo.

En la criptografía; pueden existir **vulnerabilidades** en el propio algoritmo o en la implementación de esta, en alguna versión de un sistema operativo o un driver concreto.

4.12. Criptografía Asimétrica.

Su algoritmo de cifrado utiliza dos claves matemáticamente relacionadas de manera que lo que cifras con una sola (llave pública) lo puedes descifrar con la otra (llave privada).

En criptografía asimétrica para la firma digital esta se realiza al revés. Si cifra algo con su llave privada, entonces cualquiera que conozca su llave pública podrá descifrarlo.

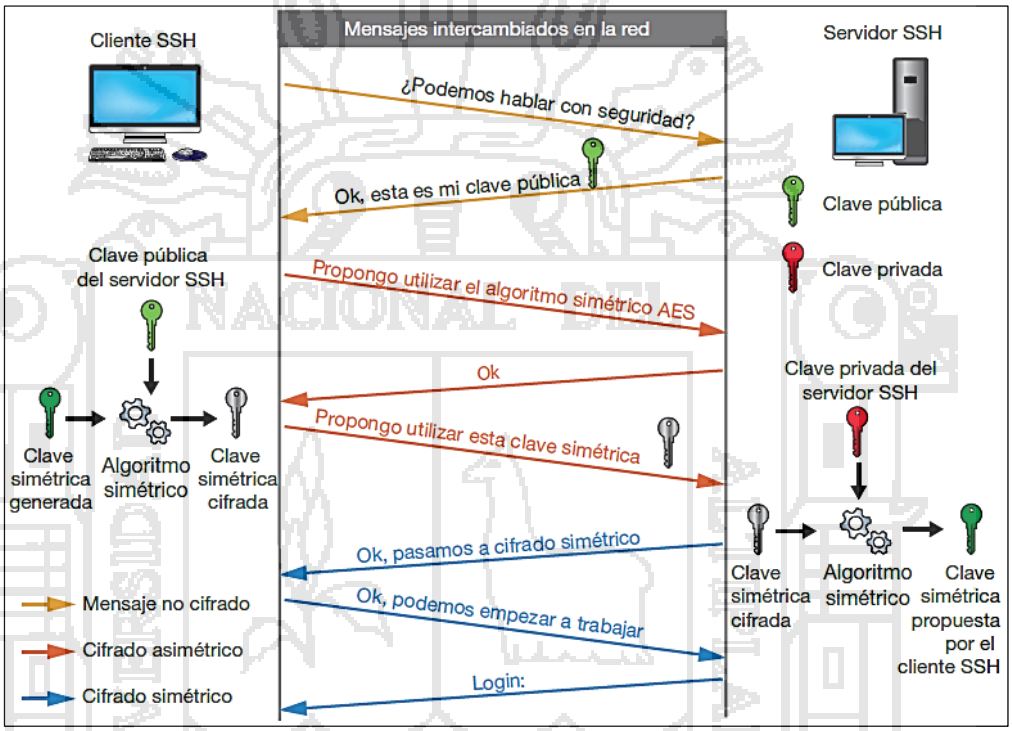
Cifrar un mensaje con una llave privada equivale a firmarlo, cuando cifras algo con tu llave privada estás demostrando tu autoría, eso se llama autenticación. Y no proporciona confidencialidad al mensaje, es decir no le añade secreto. La criptografía asimétrica resuelve los dos problemas de la clave simétrica.

- No necesitamos canales seguros para comunicar la clave. Se puede adjuntar en e-mails, añadirlas al perfil de nuestras redes sociales, postearla en un blog.
- No hay desbordamiento en el tratamiento de claves y canales. Si somos 9 empleados, solo necesitamos 9 claves y un solo canal; la intranet de la empresa, un correo destinado a toda la empresa. Y si aparece un empleado nuevo, serán 10 claves y el mismo canal.

4.13. **Esquema hibrido de cifrado en SSH** (Secure Shell)

Protocolo de comunicación que permite cifrar las conversación extremo a extremo. Se utiliza para sesiones interactivas de comandos (es un buen sustituto del telnet), transferencia de archivos (sustituto de FTP), túneles seguros entre aplicaciones

FIGURA Nº 42: Esquema hibrido de cifrado en SSH



Fuente: (Roa: 2013. 39)

4.14. Amenazas, seguridad y soluciones

CUADRO Nº 9: Amenazas, seguridad y soluciones

Amenaza	Seguridad y Solución	Función	Tecnología
Datos interceptados, leídos o modificados ilícitamente.	Cifrado	Los datos se codifican para evitar su alteración.	Cifrado simétrico y asimétrico.
Los usuarios asumen otra identidad para cometer un fraude.	Autenticación	Verifica la identidad del receptor y emisor	Firmas Digitales.
Un usuario no autorizado en una red obtiene acceso a otra red.	Firewall	Filtra y evita que cierto trafico ingrese a la red o servidor	Firewall; Redes Virtuales Privadas.

Fuente: elaboración del autor

4.15. Estándares de seguridad para internet

CUADRO Nº 10: Estándares de seguridad para internet

Estándar	Función	Aplicación
Secure HTTP	Asegura las transacciones en la web.	Exploradores, servidores web, aplicaciones para internet.
Secure Sockets Layer (SSL)	Asegura los paquetes de datos en la capa de la red.	Exploradores, servidores web, aplicaciones para internet.
Secure MIME (S/MIME)	Asegura los anexos de correo electrónico en plataformas múltiples.	Paquetes de correo electrónico con cifrado RSA y Firma Digital.
Secure Wide-Area Nets (S/WAN)	Cifrado punto a punto entre cortafuegos y enrutadores.	Redes Privadas Virtuales.
Secure Electronic Transaction (SET)	Asegura las transacciones con tarjetas de crédito.	Tarjetas Inteligentes, Servidores de Transacción, Comercio Electrónico.

Fuente: elaboración del autor

4.16. Utilizando protocolo SSL

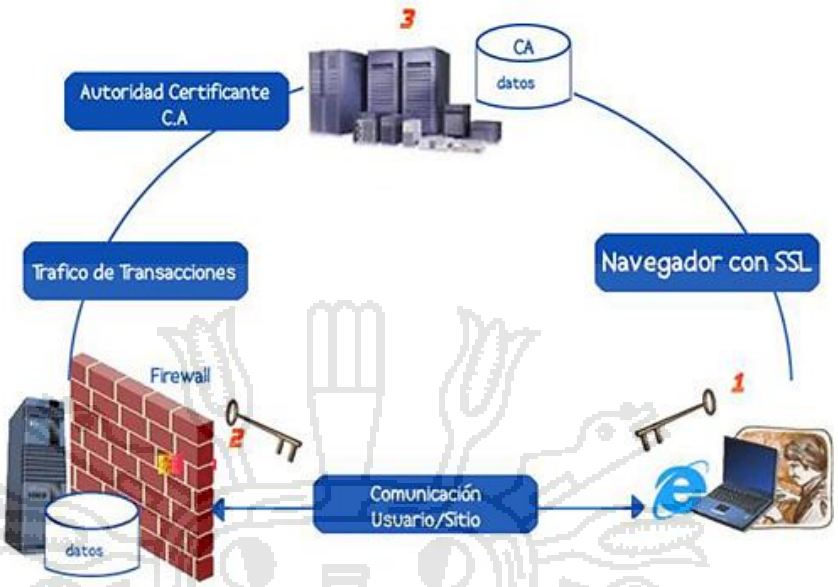
Herramienta base para proteger un sitio web, su implementación a través del protocolo SSL, adquiere un canal seguro para la transferencia de datos y/o las transacciones bancarias**.**

El SSL (Secure Sockets Layer) protege los datos transferidos por http mediante el cifrado activado por un certificado SSL en un servidor. Los certificados SSL contienen una clave pública que se utiliza para cifrar la información y la privada para descifrarla.

Cuando un navegador se dirige a un dominio seguro, se produce una “presentación SSL” que autentica al cliente y el servidor y establece un método de cifrado y una clave de sesión única.

Entonces pueden comenzar una sesión segura que protege la privacidad e integridad del mensaje. Segura que protege la privacidad e integridad del mensaje.

FIGURA Nº 43: Estructura de seguridad para comercio electrónico



Fuente: (Aponte. 2003. http://www.maestrosdelweb.com/segecom/)

Desde el punto 1, usuario se conecta hacia el punto 2 (www. tesucsa.*com*) utilizando un navegador compatible con el protocolo SSL. *El punto 2* es un sitio web tradicional (compra/venta) que establece conexiones seguras utilizando SSL para las transacciones, posee un firewall para el filtrado de paquetes. *El punto 3* es la autoridad que emite los Certificados de Autenticidad (CA) que por seguridad sea una tercera empresa el emisor.

4.17. ¿Por qué usar un certificado digital?

La aplicación de los certificados SSL es asegurar la transmisión de la información financiera en un comercio electrónico. Sin embargo, con la incidencia creciente del robo de identidades, la protección de la información personal se hace cada vez más importante. Esta categoría de datos incluiría los números de identidad y seguridad social, además de las direcciones de correo electrónico.

De modo que si realiza transacciones financieras a través de su sitio Web, si maneja datos sensibles de sus clientes entonces necesita uso de

certificados SSL, especialmente si la seguridad y privacidad de sus clientes o miembros ocupa uno de los primeros lugares en su lista de prioridades.

Existen dos razones principales para usar un certificado digital:

- Para probar la identidad de su empresa (o de su servidor) en línea, al realizar, genera fiabilidad y confianza a quien usa su sitio Web.
- Para ofrecer protección de los datos enviados a su sitio Web (o entre servidores) mediante el uso de codificación. Si llegara a interceptarse cualquier información, será imposible descifrarla sin la clave distintiva que debe utilizarse para la decodificación.

4.18. Seguridad HTTPS, (HTTP sobre SSL o HTTP segura)

HTTPS es el uso de Secure Socket Layer (SSL) o Transport Layer Security (TLS) como una subcapa de una solicitud HTTP.

HTTPS cifra y descifra las solicitudes realizadas por un visitante como la información que devuelve el servidor. HTTPS utiliza el puerto 443, a menos que se especifique lo contrario, en lugar del puerto HTTP 80 en sus interacciones.

Supongamos que usted visita un sitio Web para ver su catálogo en línea. Cuando esté listo para realizar su orden, se enviará una página Web con un formulario de pedido que comienza con ***https: //***. Al hacer clic en “enviar” desde su navegador HTTPS, toda la información será cifrada y enviada al vendedor.

De la misma manera, la respuesta desde el servidor/vendedor viajará de forma cifrada y llegará con una dirección URL https y será descifrada por su navegador. De esta manera toda la información desde y hasta el visitante y servidor viajan por el Internet de forma segura.

Algunos sitios web y redes sociales como facebook y twitter permiten utilizar el protocolo de seguridad HTTPS y no el protocolo HTTP estándar.

4.19. Firewalls (Corta Fuegos)

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin el firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Beneficia en ayudar a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

CONCLUSIONES

PRIMERO: Utilizando modelo de seguridad, buenas prácticas y arquitecturas que pueden asegurar al cliente la integridad y fiabilidad de sus datos e información se consigue la anhelada confianza y satisfacción que es muy importante para cualquier empresa.

SEGUNDO: La aplicación del modelo de seguridad y el uso del protocolo SSL junto con la técnica de cifrado asimétrica, ayuda a mantener la confidencialidad e integridad de los datos e información durante el envío sobre las redes de comunicaciones, protegiendo de esta manera las transacciones de información privada de una entidad a través de Internet.

TERCERO: El uso de protocolo SSL VeriSign ofrece de manera sencilla crear conexiones seguras por internet, es el más indicado para controlar operaciones en determinadas aplicaciones web cuando los ataques son múltiples y sofisticados, es muy apropiado para la seguridad de una página web de la entidad. Así mismo la metodología de proceso unificado de desarrollo de software, es adecuada para todo tipo de aplicación, sobre todo en lo referente al análisis y diseño.

RECOMENDACIONES

PRIMERO: Utilizar herramientas tecnológicas, aplicaciones recientes y aplicables para concientizar la seguridad para que esta sea integral en la protección de datos e informaciones en las redes de comunicaciones.

SEGUNDO: Realizar un análisis exhaustivo y permanente investigación sobre las medidas de seguridad y privacidad de la información en una entidad requerida, averiguando, abstrayendo y conociendo a fondo los sistemas y sus aplicaciones, así como también las vulnerabilidades y riesgos que lo poseen.

TERCERO: Finalmente se recomienda implementar un modelo de sistema de seguridad utilizando credenciales de autenticación SSL que son protocolos criptográficos que proporcionan comunicaciones seguras por una red, específicamente para las transacciones financieras de pago de autoavalúo entre el usuario y la entidad municipal de la región

BIBLIOGRAFIA

- Black, Uyless D. (1990). “Redes de computadoras: Protocolos, normas e interfaces” México D.F., Macrobit Editores S.A de C.V. 421 p.
- Caballero Gil, Pino. (1997). “Seguridad informática: técnicas criptográficas” México, D.F., Ediciones Alfaomega. 135 p.
- Caballero, A.E.(2000).“Metodología de la Investigación Científica”. Ed. Omega.
- Charaja, F. (2003). “Investigación Científica”. Puno – Perú: Ediciones Nuevo Mundo.
- Daltabuit, Enrique(2007)“La seguridad de la información” México, Limusa 774p
- Díaz, A.(1996). “Criptografía y Comercio Electronico”. Madrid, España: Editorial Paraninfo S.A..
- Fuster Sabater, Amparo. (2001). “Técnicas criptográficas de protección de datos” México, D.F., Alfaomega: Ra-Ma, 372 p.
- Gómez Vieites, Álvaro. (2007). “Enciclopedia de la seguridad informática” México, Alfaomega, 664 p.
- Gratton, Pierre. (1998). “Protección Informática en datos y programas en gestión y operación, en equipos y redes, en internet” México Trillas, 272 p.
- Jimeno, M., Caballero, M., Miguez, C., Matas, A., y Heredia, E. (2012). “La Biblia del Hacker”. España: Ediciones Anaya Multimedia.
- Kenneth E. Kendall (1997). ¨Análisis y diseño de sistemas¨. México: Prentice Hall Hispanoamericana.
- López Barrientos María Jaquelina y Quezada Reyes Cintia.(2006) “Fundamentos de seguridad informática” México, UNAM, Fac. Ingeniería, 223p
- Lucena, M. (2011).”Criptografía y Seguridad en Computadores”. Madrid, España.

- Nash, Andrew, et al. (2002). “PKI - Infraestructura de claves públicas: la mejor tecnología para implementar y administrar la seguridad electrónica de su negocio” Colombia, Osborne McGraw-Hill, 512 p.
- Palomino, P. (1997). “Diseño y Técnicas de Investigación”. FCEDUC UNA-PUNO: Editorial Titikaka.
- Pastor Franco, José, et al.(1998) “Criptografía digital: fundamentos y aplicaciones” Zaragoza, España, Prensas Universitarias de Zaragoza, 597 p.
- Pressman, R. (1998). “Ingeniería de Software un enfoque práctico” España: Cuarta Edición, Edit. McGraw – Hill.
- Hernandez Sampiere, Roberto; Fernández Collado, Carlos y Baptista lucio, Pilar (2007) “Metodologia de la Investigacion” 4ta Edic. Mc Graw-Hill, Mexico.
- Roa, J.F. (2013). “Seguridad Informática”. España: McGraw-Hill
- Rodríguez Prieto, Amador (1986). “Protección de la información: Diseño de criptosistemas informáticos” Madrid, Paraninfo, 255 p.
- Senge, P. (1998) "La Quinta disciplina en la práctica". Mexico: Ediciones Granítica.
- Stallings, William. (2000). “Comunicaciones y redes de computadores” Madrid, Prentice Hall , 747 p.
- VARIOS AUTORES. (2000).“La gestión del Redes Informáticas”. Chile:Trend Management, Volumen 2 Nº 3, pág. 83-107.
- Cabrera García, Sandra; García Castro, María del Carmen. () “Modelo de seguridad en las aplicaciones web desarrolladas por un tercero”.
- Silva Sarabia, Christopher Román. (2006). “Criptografía y curvas elípticas” Tesis Licenciatura (Matemático), Universidad Nacional Autónoma de México, Facultad de Ciencias, 183 p.

- Lucena López, Manuel J. “Criptografía y Seguridad en Computadores” [en línea], http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto recuperado: enero de 2012, 307 p.
- Ramió Aguirre, Jorge “Seguridad Informática y Criptografía” [en línea], http://www.criptored.upm.es/guiateoria/gt_m001a.htm recuperado: enero de 2012, 1106 p.
- Seguridad Redes Privadas virtuales (1997).[en línea]: http://fernandezg.wordpress.com/category/seguridad-en-la-comunicacion/
- NEGOCIO & MANAGEMENT http://negociosymanagement.com.ar/?p=2285 acceso 15 de julio 2013
- A SI FUNCIONA INTERNET http://sp.ria.ru/infografia/20111114/151569739.html
- CENTRO DE INVESTIGACIÓN APLICADA DE CIFRADO EN LA UNIVERSIDAD DE WATERLOO. http://www.cacr.math.uwaterloo.ca/
- DIVISIÓN DE INVESTIGACIÓN SOBRE CRIPTOGRAFIA http://www.cryptography.com/
- III JORNADAS DE SEGURIDAD INFORMÁTICA CONECTACON 2014 http://www.conectaconjaen.org/
- JORNADAS DE CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA http://wp.iese.edu.ar/?p=2760
- SEGURIDAD INFORMATICA http://www.emol.com/tag/1023/seguridad-informatica.html
- SEGURIDAD SOBRE PANEL DE INTERNET http://www.counterpane.com
- UNA DEFENSA EFICAZ CONTRA EL MAN-IN-THE-MIDDLE SOFTWARE Y MALICIOSOS http://www.zurich.ibm.com/Technology/Security/

ANEXOS

ANEXOS 01

Modelo de Encuesta: Seguridad en las Redes de Comunicaciones

DATOS GENERALES
Nombres y Apellidos:……
Ocupación :……
¿Desde qué Año es usuario de Internet?: ……

OBJETIVO: El objetivo central de la encuesta tiene la finalidad de obtener información necesaria para medir la situación actual de seguridad en las redes de comunicaciones en la región puno.

Lea cuidadosamente y marque con una X en un casillero, la respuesta considerada.

DESDE EL PUNTO DE VISTA DEL USUARIO

1. ¿Cómo Usuario, que uso le da a INTERNET?

Tipo de Uso	Uso		Tiempo (Horas)
	SI	NO	
Búsqueda de Información			
Difusión de Información			
Consultas aplicativos web(SUNAT, SUNARF, BN, MEF, otros)			
Consultas Financieras (Bancos)			
Música y Videos			
Correo electrónico (email)			
Otros.(Especifique):……..			

2. Conoce sobre la seguridad en la redes INTERNET

   SI…….. ☐ NO…….. ☐

3. ¿Le preocupa la seguridad en las transacciones de datos y su privacidad sobre internet? ☐ ☐

   SI…….. NO……..

4. ¿Está de acuerdo que la seguridad en internet sea trasmitida al usuario?

   SI…….. ☐ NO…….. ☐

5. ¿Conoce las oportunidades que tiene el usuario para diagnosticar la seguridad en una página web?

   SI…….. ☐ NO…….. ☐

6. ¿Conoce los servicios de SSL?

SI…….. ☐ NO…….. ☐

7. Considera el cifrado como factor importante de la seguridad en las transacciones

SI…….. ☐ NO…….. ☐

8. ¿Le da importancia a las políticas de seguridad en sus proyectos de tecnologías de información?

SI…….. ☐ NO…….. ☐

9. ¿Sigue las buenas practicas relacionadas con la seguridad informática (restringir acceso, auditar, etc.)?

SI…….. ☐ NO…….. ☐

10. ¿Ha realizado consultas a productos y/o servicios que involucren transacciones en internet (compras, remates, etc.)?.

SI…….. ☐ NO…….. ☐

11. ¿Cuáles de los siguientes rubros ha consultado en Internet?

Rubros	
Transacciones bancarias	
Inscripciones a cursos / eventos	
Libros	
Hardware y Software	
Cursos Online	
Otros.	

¿La información obtenida es confiable?

SI…….. ☐ NO…….. ☐

12. Cómo considera la experiencia de navegar en Internet

Muy Buena	
Buena	
Regular	
Pésima	

ANEXO 02

PROCEDIMIENTO PARA OBTENER CERTIFICADO DE SEGURIDAD SSL

CERTIFICADO DE SEGURIDAD

Cuando se transfiere información de un servidor a otro, en una "puerta de enlace" de pagos, existen cierto tipo de ataques como el ataque "hombre en el medio" (man in the middle) que emplean las URLs de envío para infectar o robar nuestra información. La información en la web viaja desprotegida y visible a todo el mundo todo el tiempo. Entonces necesita cifrar para que solo el servidor y el usuario final lo puedan ver. Un certificado de seguridad hace imposible este tipo de ataques. Consta de dos partes:

- ✓ Certificado en el servidor de envío
- ✓ Certificado en el otro servidor de recepción

El certificado o ".cert" o ".crt" es un archivo cifrado que contiene la llave privada. Es necesario instalar el certificado en nuestro servidor (servidor de recepción entrega el certificado). Uno de los certificados más conocidos es VeriSign. Poseen sus respectivos manuales.

Private Key (llave privada) y Public Key(llave publica)

Tenemos el certificado instalado (que muchas veces lo instala nuestro server/hosting). Pero para usarlo debemos entender cómo lo usaremos. El certificado tiene llave privada, el cual es una cadena codificada con algún algoritmo. Usaremos el PKCS#12 con un hash RSA de 1024 bits. Usará un password (**********).

¿Qué es la Llave Publica? es el certificado que usaremos para enviar la información cifrada. La llave privada queda en el servidor, la llave pública es la que viaja por internet. Existe la diferencia, la privada es siempre igual y la pública es dinámica y varía en cada inicio de sesión.

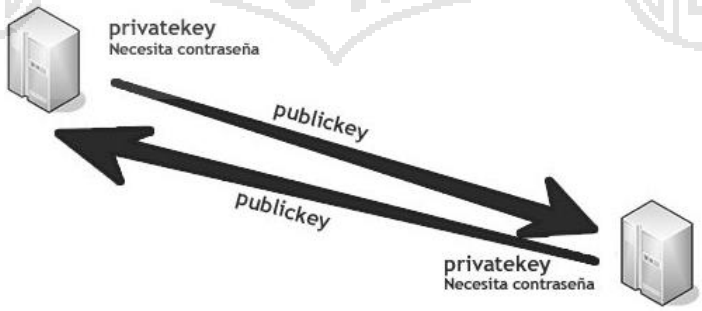


Figura 01: Llave privada y llave publica sobre la red

PASO 1. Configuración del Servidor

Configurar nuestro servidor, si está en un hosting, se solicita para realizar.

Paso 2. cURL

Debemos tener esta librería, actualizada que permite enviar HTTP encabezados desde PHP. Para habilitarla en el servidor se realiza en el *php.ini* lo siguiente:

- ✓ Buscar la línea "extension=php_curl.dll"
- ✓ Quitar el **;** (punto y coma) de delante
- ✓ Reiniciar el servicio

Paso 3. openSSL

Esta librería, sirve para mantener sesiones seguras SSL mediante certificados de seguridad. Para instalar se debe seguir los siguientes pasos:

- ✓ Descargar OpenSSL
- ✓ Si están en Windows Server seguramente tengan que instalar la librería del C++
- ✓ Seguir los pasos de instalación
- ✓ Buscar en el **php.ini** "extension=php_openssl.dll"
- ✓ Quiten el ;(punto y coma) de delante
- ✓ Reinicien el servicio

Paso 4. Uso de OpenSSL

Escribiremos el código base en PHP para abrir el certificado y obtener la llave privada, generar llave publica, luego cifrar el texto y descifrar.

Paso 5. Abrir el certificado como si fuera un archivo más.

CODIGO

```
$file = 'nombre_certificado.p12';
//puede ser .crt o .cert también
$fd = fopen($file, 'r');
$p12buf = fread($fd, filesize($file));
fclose($fd);
```

Paso 6. Extraemos la Llave privada con la información dada en el paso 5

CODIGO

```
$p12cert = array();
$pass = "**********";
//En este array almacenaremos la información
//de la llave privada
openssl_pkcs12_read($p12buf, $p12cert, $pass);
```

La función *openssl_pkcs12_read* nos permite extraer del buffer de lectura la información pasándole el pass para autentificarlo. Si se usa otro tipo de certificado diferente a PKCS#12, puede tener varias funciones para extraer la información, pero básicamente siempre es la misma.

Paso 7. Validamos la sentencia *openssl_pkcs12_read*.

CODIGO

```
if(openssl_pkcs12_read($p12buf, $p12cert, $pass))
{
  //Código Creación PrivateKey
}
else
{
   //Código Error
}
```

Como se apreciaba que el parámetro array estaba vacío, ahora contiene la información de la llave. De esta manera con realizar.

CODIGO

```
$p12cert["pkey"];
```

Obtenemos el resultado de nuestra llave, que a simple vista se ve así:

CODIGO

```
-----BEGIN CERTIFICATE-----PORQUERIA ENCRIPTADA-----END CERTIFICATE---
```

Paso 8. Almacenando la Llave privada

CODIGO

```
$privatekey = $p12cert["pkey"];
```

Paso 9. Creación de par de llaves "asymmetric key algorithms"

CODIGO

```
$res=openssl_pkey_new();
```

Paso 10. Generamos una cadena valido para la llave

CODIGO

```
openssl_pkey_export($res, $p12cert["pkey"]);
```

Solo ejecutando la función par de llaves y validando con nuestra llave privada

Paso 11. Obteniendo la Llave Publica

CODIGO

```
$publickey=openssl_pkey_get_details($res);
$publickey=$publickey["key"];
```

La función *openssl_pkey_get_details* obtiene la información para nuestra llave pública, y luego la pasa a una variable desde el array. Se observa cómo se invocar al key_pair .

Paso 12. Creación de información y cifrarlo

CODIGO

```
$texto_a_convertir = htmlentities("Modelo de sistema critpografia asimétrica con openSSL");
openssl_public_encrypt($texto_a_convertir, $crypt, $publickey);
```

Se utiliza una variable de texto primero usando htmlentities y luego emplear la función openssl_public_encrypt, pasando que valor queremos convertir, en que variable almacenar la conversión y con qué llave publica hacerlo.

Paso 13. Descifrando la Información

CODIGO

```
$PK12=openssl_get_privatekey($p12cert["pkey"]);
openssl_private_decrypt($crypt,$decrypt,$PK12);
```

Primero se obtiene la llave privada en formato key (la tenemos en cadena), para esta usaremos openssl_get_privatekey y luego descifraremos con la función openssl_private_decrypt, donde obtendremos que valor descifrar, en donde almacenar y con qué llave privada hacerlo. De esta manera se logra la conexión segura en la red.

Paso 14. Código completado

```
<?php
$p12cert = array();
$file = 'certificado.p12';
$pass = "**********";
$fd = fopen($file, 'r');
$p12buf = fread($fd, filesize($file));
fclose($fd);
echo "<h1>test criptografia asimetrica</h1>";
if ( openssl_pkcs12_read($p12buf, $p12cert, $pass) )
{
   echo "Funciona";
}
else
{
    echo "No funciona";
}
$privatekey = $p12cert["pkey"];
$res=openssl_pkey_new();
openssl_pkey_export($res, $p12cert["pkey"]);
$publickey=openssl_pkey_get_details($res);
$publickey=$publickey["key"];
echo "<h2>Llave privada:</h2>$privatekey<br><h2>Llave
publica:</h2>$publickey<BR>";
$cleartext = htmlentities('<center><b>Texto HTML</b></center>');
echo "<h2>Original:</h2>$cleartext<BR><BR>";
openssl_public_encrypt($cleartext, $crypttext, $publickey);
echo "<h2>cifrada:</h2>$crypttext<BR><BR>";
$PK2=openssl_get_privatekey($p12cert["pkey"]);
$Crypted=openssl_private_decrypt($crypttext,$Decrypted,$PK2);
if (!$Crypted) {
   $MSG.="<p class='error'>Imposible descifrar ($CCID).</p>";
}else{
   echo "<h2>Descifrada:</h2>" . $Decrypted;
}
?>
```

ANEXO 03

SECUENCIA DE PROCESO PARA CIFRAR DATOS CON CERTIFICADO SSL VERISGN

Cuando se realiza transacciones sobre redes, en la cual es muy sensible la seguridad de los datos que se manejan, por lo tanto se necesita proteger estas con *tecnologías de criptografía asimétrica*, o más concretamente con certificados digitales SSL.

LOS PROCEDIMIENTOS NECESARIOS SON:

PASO 1.

Requerimos tener certificado digital SSL, para cifrar y descifrar los datos

PASO 2.

Ciframos con la llave pública y desciframos con la llave privada, para que de esta manera nuestros datos (guardando en una base de datos) no tengan ningún tipo de valor, sin que se cuente con la llave privada y su correspondiente password.

PASO 3.

Generación de certificados o llaves pública y privada. Se inicia a generar un certificado firmado. Para ello se necesita tener instalado el OpenSSL y en seguida escribimos:

```
pablot$ openssl req -new -x509 -out certificado.pem
```

PASO 4.

Una vez realizado esta tarea, seguiremos la secuencia de pasos que se presentan a continuación, con salida del comando anterior completaremos la información solicitada según corresponda.

```
Generating a 1024 bit RSA private key
.............................++++++
..........++++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase: < aquí podemos ingresar una clave>
Verifying - Enter PEM pass phrase: < aquí debemos repetir la clave
ingresada>
-----
You are about to be asked to enter information that will be
```

```
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PU
State or Province Name (full name) [Some-State]:puno
Locality Name (eg, city) []:juliaca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:tesucsa
erltda
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:tiburcio Mamani
Email Address []:timat2003@hotmail.com
```

PASO 5.

Una vez completado obtendremos nuestro certificado en el archivo `certificado.pem` y la llave privada en el archivo `privkey.pem`.

PASO 6.

Visualizamos el contenido de los dos archivos:

Contenido del archivo `certificado.pem`

```
-----BEGIN CERTIFICATE-----
MIIDADCCAmmgAwIBAgIBADANBgkqhkiG9w0BAQQFADBkMQswCQYDVQQGEwJBUjER
MA8GA1UECBMIU2FudGEgRmUxEDAOBg1VBAcTB1Jvc2FyaW8xEzARBgNVBAoTCk1p
IGVtcHJlc2ExCzAJBgNVBAsTAklUMQ4wDAYDVQQDEwVQYWJsbzAeFw0wODA2Mjcw
ODI4MzBaFw0wODA3MjcwODI4MzBaMGQxCzAJBgNVBAYTAkFSMREwDwYDVQQIEwhT
YW50YSBGZTEQMA4GA1UEBxMHUm9zYXJpbzETMBEGA1UEChMKTWkgZW1wcmVzYTEL
MAkGA1UECxMCSVQxDjAMBgNVBAMTBVBhYmxvMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQC9Hh9+H5+sBUCJklI+U5H7jVILZT21D9LtHqxeVtaBZUheLHJ1tJH6
rCKH/rToMYgNHPthHORQFif5+RMZJxev7o2F16osfwwkF4ak1+2xP7mTOPpT7n1o
t7DUZPNzhV4W9U2wGG7s8k8vX1XZ7KjQSsm0M1Wi7TJLUk+r2z/S7QIDAQABo4HB
MIG+MB0GA1UdDgQWBBTi3lAeHK6M0E0tXmxThxQcYGL5zDCBjgYDVR0jBIGGMIGD
gBTi3lAeHK6M0E0tXmxThxQcYGL5zKFopGYwZDELHAkGA1UEBhMCQVIxETAPBgNV
BAgTCFNhbnRhIEZlM2RAwDgYDVQQHEwSb3NhcmlvMRMwEQYDVQQKEwpNaSBlbXBy
ZXNhMQswCQYDVQQLEwJJVDEOMAwGA1UEAxMFUGFibG+CAQAwDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQQFAAOBgQB+F7QLGre/v8tu0UZzBCauuygGjPk2KYddJC5/
```

```
gcaV5xpgHoyxIXkYkwzfuV+v+S33Ju+mTmXczt5UgPztYOxFdocGFUF0QBs6VGfk
uVSsANaT3TVS8lF/dqiy0M8e0/rsT4PdCvidalvZNMOEcHAl+7TALLzg53FU2bF2
O+Wujw==
-----END CERTIFICATE-----
```

Contenido del archivo: `privkey.pem`

```
      -----BEGIN RSA PRIVATE KEY-----
      Proc-Type: 4,ENCRYPTED
      DEK-Info: DES-EDE3-CBC,7269B348F1BAA2D9
RC+B4fUTgQx5qCGmC1VXvlErXmnpbqE+DLGq8dqZYlwTksKnDnMv32uRc3rAeyNc
Eg+aNU6KWhEnu3WYfcHTJsW4R3aILNX2vKF/zOXHHSxBA1zJRgyMzqKrRPfB4BEj
5Enn48ehgG/DwKBcXcQSsNAQ121qJf4QBG3rj6H6jE8wNcIiV7AI5ZKcOB25V/9q
Q7IgplPKX+PfF/piQUDIjNDQ1Nfrfn59qdewkxRQiCoEeJKwXpn6je2JCLDTV5cz
4ZUc5hT/1IePjWHY8TkRnma4v4obBCd8N3fEqkTP5nLBhGAcor9RuBcusmKyhlxt
ftiWTgBs6k15HuCcmzIuARQ/PE5elJMeGYJfrcby40QPLcTdlz9wqR2ULmpAUxTe
g9e1EKTOTAGjF+oUpCrDEIN5Txru6Q8hDQ6NuV9b0baeFJare7dlcqrzcjm2Lwin
Sq3N78xdOiA4kMJ1AKDM6cBXbFvZ92XeUFEZPH53wDC+aiNc4urlqew06uwAgHDu
Br60ODWnhw3babNWQaM5nxAIs5nR8DJZmdzrj2c4zYkYKLmcoaJzsSTGn466kqce
96F4503ev2+/iCgSh9h8lFU9JRRsQnbs4IaxemboHU5MY5Fu3h7MZXSejgUbZ2Z7
3rI9T/VQUyJyxcuzHIKeEJNMwxwUBE+3xqffluZXAxPP8GuyWHSn9owErCPg9RhU
xeBl+MYZi2zzSscdVZ6ZxDbsNRYiGlAdqPBWofv+UTej7ch0vggrhjzkONuGTJn/
IiJB4QUAjkiuDCtZR8OVutxrebmPNnRZmiFHx8L7QYw=
-----END RSA PRIVATE KEY-----
```

Se recuerda que si queremos tener un certificado digital otorgado por una entidad certificante como Verisign, debemos generar un CSR o Certificate Sign Request (con el comando `openssl req -new -out cert.csr`) que debe ser enviado (el archivo cert.csr) a la autoridad certificante realizando previo pago, nos emite un certificado como el que tenemos en el archivo certificado.pem.

PASO 7.

Una vez obtenido el certificado y nuestra llave privada, podemos cifrar nuestros datos con la llave privada, y luego grabarlos en una base de datos.

PASO 8.

Cifrado de datos usando la llave publica

```
<?php
$texto_plano="Dato supersecreto que pone en riesgo la
seguridad";
$llave_publica="file://<ubicacion del archivo>certificado.pem";
openssl_public_encrypt($texto_plano, $texto_encriptado,
```

```
$llave_publica);
//Si imprimimos esta no se podrá entender nada, que en realidad
//es el dato ya cifrado.Es por esto probablemente nos conviene
//cifrarlo en base64 con
// $texto_encriptado = base64_encode($texto_encriptado)
// antes de grabarlo en un campo de una base de datos
//echo $texto_encriptado;
?>
```

PASO 9.

Descifrado de datos usando la llave privada

```
<?php
$fp=fopen("./privkey.pem","r");
$llave_privada=fread($fp,8192);
fclose($fp);
//El segundo parámetro es la clave que ingresamos al crear el certificado
//si es que optamos por hacerlo.
//Si antes codificamos en base64 el texto cifrado, hay que recordarse de
//hacerlo un $texto_encriptado=base64_decode($texto_encriptado)
//antes de descifrarlo
$res = openssl_get_privatekey($llave_privada,"miclave");
openssl_private_decrypt($texto_encriptado, $texto_desencriptado, $res);
//Esto debe dar como salida el mismo texto que antes estaba en la
//variable $texto_plano
echo $texto_desencriptado;
?>
```

Se debe tener en cuenta antes de grabar un dato crítico en la base de datos y lo que tenemos que hacer luego de recuperarlo de la base para poder descifrar. De esta manera la base de datos será ilegible para cualquiera que no tenga la llave privada y su correspondiente clave o password.

El largo de la cadena de datos a cifrar está limitado por el tamaño de la clave, por lo cual para una clave de 1024 bits como la del caso OpenSSL permite cifrar hasta 936 bits, o sea *936/8=117* caracteres. En consecuencia para claves de 1024 bits solo podremos cifrar hasta 117 caracteres, pero el límite se incrementa si usamos claves de 2048 o 4096 bits.

Se recomienda una clave mínima de 2048 bits, pero con OpenSSL hay la posibilidad de generar claves de 4096 bits.

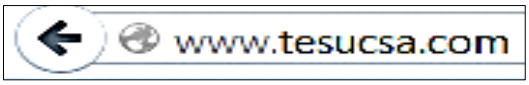
CIFRADO DE PAGINA WEB TESUCSA

Para resguardar la seguridad de los datos que se manejan, en los proyectos de la empresa TESUCSA EIRLtda. Se realiza la protección de utilizando *tecnologías de criptografía asimétrica*, o más concretamente con certificado de seguridad digital SSL Verisign.

La finalidad es tener una página web segura en www.tesucsa.com de dicha empresa. De esta manera el acceso es restringido solo para persona autorizadas de la institución para realizar operaciones sobre el referido sitio web.

GRAFICO 01: Página web de la empresa Tesucsa no cifrada

Si en la **barra de direcciones** de la página web TESUCSA se muestra la dirección URL de la forma siguiente.



El sitio no usa SSL**.** La mayoría de los sitios no necesitan usar SSL porque no solicitan información confidencial. Entonces de evita introducir información confidencial, como nombres de usuario y contraseñas, en la página.

Para lograr el cifrado de esta página web se debe tener en cuenta la parte técnica siguiente:

- ✓ Poseer o estar disponible con un servidor.
- ✓ Tener alojado nuestra página web en el servidor.
- ✓ Solicitar código de acceso a la entidad autorizada.
- ✓ Con el código CSR (huella digital exclusiva de nuestro servidor, incluida con la clave pública) nos ofrece autenticación y conexión segura.
- ✓ Con CSR unimos la solicitud de Firma de certificado

Todas estas operaciones se realizan en panel de control de la página web www.tesucsa.com y en el lado del servidor y como resultado se obtiene una página web segura como se muestra en gráfico.

Grafico 02: Página web de la empresa Tesucsa Cifrada

Cuando una página web se encuentra cifrada, en la barra de direcciones se muestra de la siguiente forma

Se ha establecido correctamente una conexión segura con el sitio**.** Se debe tener en cuenta este tipo de icono y asegurarse de que la URL tenga el dominio correcto, entonces si se puede acceder al sitio o introducir información confidencial en la página.