IMPLEMENTACION EN METODO DE ENCRIPTAMIENTO

"PARA LOS SERVICIOS QUE OFRECE LA RED DE LA CORPORACION UNIVERSITARIA UNITEC"

ANTONIO ANDRES OSORIO SANCHEZ

CORPORACION UNIVERSITARIA UNITEC
FACULTAD DE SISTEMAS
LINEA DE INVESTIGACION
SANTAFE DE BOGOTA, DC
2005

IMPLEMENTACION EN METODO DE ENCRIPTAMIENTO

"PARA LOS SERVICIOS QUE OFRECE LA RED DE LA CORPORACION UNIVERSITARIA UNITEC"

ANTONIO ANDRES OSORIO SANCHEZ

Trabajo de investigación dirigida para optar al titulo de Tecnólogo en Sistemas

Tutor: Diana Astrid Bolívar Castillo
Doctora: Liliana J. Barrera

Corporación Universitaria Unitec
Facultad de sistemas
Línea de investigación
Santa fe de Bogota D.C
2005

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág

AGRADECIMIENTOS

A mis padres, por todo el amor, paciencia y comprensión, por confiar en mi y por ser las personas que mas quiero en el mundo.

A mi hermano, que siempre ha sido un gran apoyo, por lo mucho que lo quiero.

A toda mi familia.

A mi tutora Diana la cual me brindo su apoyo y amplios conocimientos por hacer realidad esta investigación.

A todos mis profesores, por guiarme en mi formación.

A Dios por que sin el nada es posible.

A todos gracias.

INTRODUCCION

Cada vez más escuchamos de violaciones a las redes de datos de las empresas. Intrusos que entran a sitios web y modifican información; robos de contraseñas, acceso a información confidencial; acceso a cuentas bancarias; esto solo mencionando los casos que mas se escuchan diariamente.

La seguridad en las redes es el elemento más crítico en las empresas pues se debe garantizar la integridad y confiabilidad de los datos que viajan por ella. Al fin y al cabo es el canal de comunicación tanto interno como externo de la organización.

Durante todo el proceso de envío de la información por la red, esta viaja por diferentes computadoras y es en cualquiera de ellas en donde un "intruso", "Hacker", "rompedores de sistemas" como se quiera llamarlos pueden interceptar, leer y disponer fácilmente de la información que se envió por un correo electrónico ó los datos que se digitaron para ingresar a un sitio web ó la contraseña que se escribió para la transferencia de un archivo, es decir, acceder a la información confidencial que viaje a través de cualquier servicio y que no transmita los datos encriptados.

Por estas razones las empresas deben reforzar sus sistemas de seguridad en las redes y la Corporación Universitaria Unitec no debe ser ajena a esta situación. Por tal motivo la presente investigación busca diagnosticar la situación de los servicios que ofrece la red de la universidad y proponer alternativas de solución a las falencias encontradas.

PLANTEAMIENTO Y FORMULACION DEL PROBLEMA

En la actualidad algunos de los servicios que ofrece la red de datos de la Corporación Universitaria UNITEC no cuentan con mecanismos de encriptamiento adecuados para la transmisión segura de la información, es decir, diariamente viajan millones de paquetes llevando y recibiendo datos en forma plana.

El envío de información totalmente plana por la red es un factor de alto riesgo ya que facilita la interpretación y manipulación de los datos por personas no autorizadas las cuales pueden acceder a ella a través de programas que capturan los paquetes transmitidos. Aunque este riesgo es minimizado en gran parte por la estructura física de la red la cual interconecta los equipos por medio de dispositivos activos como son los switches los cuales no permiten que los datos se envíen a computadores no destinatarios de la información.

La presentación de esta falencia en la transmisión de los datos puede generar suplantación de datos, manipulación de información confidencial, envió de información a través de usuarios, es decir, suplantación de identidades; esto para el caso del correo electrónico por medio del cual se puede enviar información utilizando el nombre de usuario y contraseña capturada. Entre muchas otras cosas que se pueden llegar a realizar teniendo la información confidencial de los usuarios.

Entendiendo el riesgo al cual puede verse comprometida la información que viaja por la red de la Universidad se hace necesaria la implementación de medidas de encriptamiento en la transmisión de los datos por medio de la instalación de certificados digitales y de la migración a versiones seguras de los protocolos utilizados.

FORMULACION DEL PROBLEMA

¿Cuales serian los métodos o algoritmos de encriptamiento adecuados a implementar en los servicios que ofrece la red?

¿Es necesario implementar mecanismos de encriptamiento a nivel de capa de aplicación, a nivel de capa de red ó en ambas?.

¿Que servicios son los que no cuentan con un nivel de encriptamiento y que método seria el mas acertado implementar para garantizar la confiabilidad e integridad de la información?

¿Que pasaría si no se corrigen estas fallas en los servicios prestados?.

¿En que se afectarían los portales web de la universidad ó el envio de información por el correo electrónico ó la transferencia de archivos?

OBJETIVOS

GENERAL

Proponer soluciones de encriptamiento para los datos que viajan por la red mediante la actualización de las versiones de los protocolos y la configuración de certificados digitales para garantizarles a los usuarios confidencialidad y confiabilidad en los datos transmitidos entre los diferentes servicios que ofrece la Universidad.

ESPECIFICOS

- Instalar software de captura de paquetes en la red para conocer el nivel de encriptamiento de los datos enviados.
- Analizar los diversos protocolos que utilizan los servicios que ofrece la red e identificar aquellos que transmiten los datos sin utilizar algoritmos de encriptamiento.
- Analizar la estructura interna de los paquetes para conocer la versión IP que utilizan los datos para su transmisión.
- Investigar sobre técnicas y algoritmos de encriptamiento de datos utilizados en la actualidad para los servicios vulnerables de la red de la universidad.
- Plantear posibles soluciones de transmisión de datos de forma ininteligible que garanticen la seguridad de los mismos tan pronto los datos salen de la terminal de trabajo.

JUSTIFICACION

Con la presentación de alternativas de encriptamiento en los datos transmitidos por la red se busca que la información viaje de forma ininteligible dificultando de esta forma la extracción de información confidencial por personas no autorizadas.

Se presenta un panorama general del tema de seguridad en los datos, algoritmos, técnicas y soluciones de encriptamiento para que las personas encargadas de la gestión y administración de la red de la Corporación Universitaria Unitec amplíen sus conocimientos e implemente soluciones criptográficas que pueden mejorar la situación actual de algunos servicios como el correo electrónico via POP3 e IMAP, el ingreso a los portales, la administración por web de los usuarios de la red, la transferencia de archivos los cuales en el diagnostico realizado presentaron un alto grado de vulnerabilidad al transmitir la información en texto plano.

Con la implementación de estas medidas se busca que los datos que viajan por la red presenten integridad y privacidad para que a futuro no sean vulnerables de ataques que perjudiquen el funcionamiento de ella. Por ultimo es importante aclarar que las soluciones propuestas en esta investigación no solucionan todas las falencias que se pueden llegar a presentar en el diario vivir de una red por lo tanto se debe evaluar y diagnosticar periódicamente la transmisión de información para determinar nuevas vulnerabilidades las cuales no están exentas de presentarse teniendo en cuenta que la tecnología cada dia crece y por lo tanto los servicios que se puedan ofrecer en una red también.

MARCO TEORICO

1. CRIPTOGRAFIA

1.1 HISTORIA

La primera aplicación conocida de la criptografía se remonta a 4000 años atrás, cuando los Egipcios utilizaban jeroglíficos crípticos para narrar la vida y hazañas de sus faraones. La encriptación no se empleaba para esconder el significado del texto sino para darle un carácter más solemne.
En la antigua China, el carácter ideográfico del idioma servía para esconder el significado de las palabras, aunque no parece que esta particularidad se hubiera empleado para encriptar/desencriptar mensajes.
Varios pueblos de la antigüedad emplearon diversos métodos de encriptación/ desencriptación de escritos, como los Griegos, los Espartanos y los Hebreos, pero los Árabes y los Indios fueron los que mayor desarrollo lograron en este campo, destacándose un Árabe, Muhammad al-Qalqashandi, quien inventó una técnica para descifrar mensajes *que todavía se usa en la actualidad.*

La criptografía se tornó importante durante la Edad Media, cuando los gobiernos se comunicaban con sus embajadores por medio de mensajes cifrados. En 1453, el gobierno Italiano establece un grupo dedicado exclusivamente al estudio de la criptografía, con el fin de perfeccionar los métodos de encriptación de sus mensajes, así como para descifrar los de sus enemigos.

Con el tiempo, además de los métodos manuales aparecieron máquinas simples, como la rueda de Thomas Jefferson. La llegada del telégrafo significó un importante avance en la criptografía, al generalizarse el uso de máquinas electromecánicas para la encriptación de mensajes. Las dos guerras mundiales también impulsaron significativamente el avance de la criptografía y del criptoanálisis.

El desarrollo de los computadores marcó otro hito en el desarrollo de la criptografía, al permitir efectuar complejos cálculos matemáticos en corto tiempo, tanto para encriptar, como para descifrar mensajes.

1.2 TIPOS DE CRIPTOGRAFIA

1.2.1 CRIPTOGRAFÍA SIMÉTRICA (CLAVE SECRETA)

Es el sistema de cifrado más antiguo y consiste en que tanto el emisor como el receptor encriptan y desencriptan la información con una misma clave *k* (clave secreta) que ambos comparten. El funcionamiento es muy sencillo: el emisor cifra el mensaje con la clave *k* y se lo envía al receptor. Este último, que conoce dicha clave, la utiliza para desencriptar la información. Es importante considerar que para que el sistema sea razonablemente robusto contra ataques de tipo criptoanálisis, esta clave *k* ha de ser mayor de 40 bits, lo cual choca con las restricciones de exportación de tecnología criptográfica del gobierno americano, que marca los 40 bits como límite de clave para programas que utilicen este tipo de tecnología.

Criptografía de Llave Privada
(Simétrica)

Algoritmos típicos que utilizan cifrado simétrico son DES, IDEA, RC5, etc, El criptosistema de clave secreta más utilizado es el Data Encryption Standard (DES) desarrollado por IBM y adoptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977.

Este sistema de cifrado tiene la ventaja de que es altamente eficiente, dado que los algoritmos utilizados son muy rápidos al poder implementarse tanto en hardware como en software de una forma fácil.

El mayor inconveniente de la criptografía simétrica es que esta clave *k*, al ser compartida, ha de ser comunicada de forma segura entre las dos partes de la comunicación (por teléfono, correo certificado, etc.), previamente a ésta. Si este secreto fuese enviado por un canal inseguro, como por ejemplo Internet, la seguridad del sistema sería bastante pobre, dado que cualquiera podría interceptarla y comprometer todo el sistema. También hay que tener en cuenta la frecuencia con la que esta clave debe ser renovada para evitar que sea desvelada.

Otro gran problema a tener en cuenta es el manejo de estas claves, ya que en una red de n usuarios, cada pareja necesita tener su clave secreta particular, lo que hace un total de n(n-1)/2 claves para esa red (es decir, combinaciones de n usuarios tomadas de 2 en 2); Esto supone unas cinco mil claves en una red de sólo cien usuarios, medio millón en una de mil, y varios billones en una red tan grande como el sistema de telefonía convencional de cualquier país desarrollado. Es económicamente inaceptable el que se puedan distribuir todas estas claves por anticipado, e indeseable el tener que posponer las comunicaciones seguras mientras las claves están siendo trasladadas de una a otra parte.

1.2.2 SISTEMAS DE CIFRADO ASIMETRICO

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siguiera el que ha cifrado el mensaje puede volver a descifrarlo.

Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

Criptografía de Llave Pública (Asimétrica)

Un sistema de cifrado de clave publica basado en la factorización de números primos se base en que la clave publica contiene un número compuesto de dos números primos muy grandes. Para cifrar un mensaje, el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. Para descifrar el mensaje, el algoritmo de descifrado requiere conocer los factores primos, y la clave privada tiene uno de esos factores, con lo que puede fácilmente descifrar el mensaje.

Es fácil, con los ordenadores de hoy en día, multiplicar dos números grandes para conseguir un número compuesto, pero es muy difícil la operación inversa, dado ese número compuesto, factorizarlo para conocer dada uno de los dos números. Mientras que 128 bits se considera suficiente en las claves de cifrado simétrico, y dado que la tecnología de hoy en día se encuentra muy avanzada, se recomienda en este caso que la clave publica tenga un mínimo de 1024 bits. Para un ataque de fuerza bruta, por ejemplo, sobre una clave publica de 512 bits, se debe factorizar un número compuesto de hasta 155 cifras decimales.

1.2.3 Sistemas de cifrado híbridos

Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica, Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente por lo que si un atacante pudiera descubrir la clave simétrica, solo le valdría para ese mensaje y no para los restantes. Tanto PGP como GnupPG usan sistemas de cifrado híbridos. La clave simétrica es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un solo paquete. El destinatario usa su clave privada para descifrar la clave simétrica y acto seguido usa la clave simétrica para descifrar el mensaje.

1.3 ALGORITMOS DE ENCRIPTAMIENTO

Es una fórmula matemática que se aplica para encriptar y luego desencriptar un mensaje.

1.3.1 DES

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.
Los principales inconvenientes que presenta DES son:

La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se cree que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.

No permite longitud de clave variable, con lo que sus posibilidades de configuración son muy limitadas, además de permitirse con ello la creación de limitaciones legales.
La seguridad del sistema se ve reducida considerablemente si se conoce un número suficiente textos elegidos, ya que existe un sistema matemático, llamado Criptoanálisis Diferencial, que puede en ese caso romper el sistema en 2 elevado a 47 iteraciones.
Entre sus ventajas cabe citar:

- Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.
- Es muy rápido y fácil de implementar.
- Desde su aparición nunca ha sido roto con un sistema práctico.

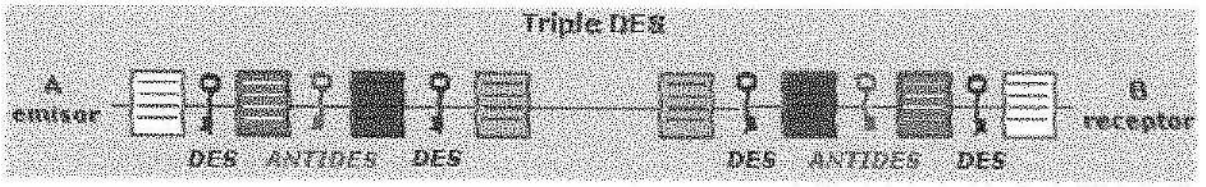
Actualmente DES ya no es estándar y fue roto en Enero de 1999 con un poder de cómputo que efectuaba aproximadamente 250 mil millones de ensayos en un segundo.

Triple DES

Como hemos visto, el sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (**TDES**), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se encripta el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:



Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.

Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.
Si la clave de 128 bits está formada por dos claves iguales de 64 bits (C1=C2), entonces el sistema se comporta como un DES simple.

Tras un proceso inicial de búsqueda de compatibilidad con DES, que ha durado 3 años, actualmente TDES usa 3 claves diferentes, lo que hace el sistema mucho más robusto, al conseguirse longitudes de clave de 192 bits (de los cuales son efectivos 168), mientras que el uso de DES simple no está aconsejado.

RC5

El sistema criptográfico simétrico RC5 es el sucesor de RC4, frente al que presenta numerosas mejoras. RC4 consiste en hacer un XOR al mensaje con una arreglo que se supone aleatorio y que se desprende de la clave, mientras que RC5 usa otra operación, llamada dependencia de datos, que aplica sifths a los datos para obtener así el mensaje cifrado. Ambos han sido creados por RSA Data Security Inc., la empresa creada por los autores del sistema RSA, que es actualmente una de las más importantes en el campo de los sistemas de cifrado y protección de datos.

Permite diferentes longitudes de clave (aunque está prohibida su exportación fuera de EEUU con longitudes superiores a 56 bits), y funciona como un generador de números aleatorios que se suman al texto mediante una operación de tipo OR-Exclusiva.

Es además ampliamente configurable, permitiendo fijar diferentes longitudes de clave, número de iteraciones y tamaño de los bloques a cifrar, por lo que le permite adaptarse a cualquier aplicación. Por ejemplo, este algoritmo es el usado por Nestcape para implementar su sistema de seguridad en comunicaciones SSL (Secure Socket Layer).

En cuanto a su seguridad, aún es pronto para afirmar nada concluyente, aunque en 1996 una universidad francesa consiguió romper el sistema RC4 con clave de 40 bits, lo que hace sospechar que RC5 con longitudes de clave de 56 bits no es lo suficientemente seguro.

IDEA

Sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como OR-Exclusiva y suma y multiplicación de enteros.

El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

EL FUTURO ESTÁNDAR

El NIST de EEUU, en busca de un nuevo sistema de encriptación simétrico que reúna las características funcionales y de seguridad necesarias, decidió convocar en 1977 un concurso a nivel mundial, invitando a los principales desarrolladores de este tipo de sistemas a crear un algoritmo que pueda ser tomado como estándar para los próximos años.

Este nuevo sistema de llamará AES (Advanced Encryption Standard), y el algoritmo que utilice se denominará AEA (Advanced Encryption Algorithm).

A este concurso se presentaron numerosos autores, y tras un largo proceso de selección el ha seleccionado como futuro estándar el denominado Rijndael, creado por los belgas Vincent Rijmen y Joan Daemen.

Rijndael es un cifrador de bloque que opera con bloques y claves de longitudes variables, que pueden ser especificadas independientemente a 128, 192 ó 256 bits. El resultado intermedio del cifrado se denomina Estado, que puede representarse como una matriz de bytes de cuatro filas.

A partir de ésta base se realiza una serie de bucles de cifrado, cada uno de ellos consistente en las siguientes operaciones:

1. Sustitución de bytes no lineal, operando independientemente sobre cada uno de los bytes del Estado.

2. Desplazamiento de las filas del Estado cíclicamente con offsets diferentes.

3. Mezcla de columnas, que se realiza multiplicando las columnas del Estado módulo x4+1, consideradas como polinomios en GF(28), por un polinomio fijo c(x).

4. Adición de la clave de vuelta, en la que se aplica al Estado por medio de un simple XOR. La clave de cada vuelta se deriva de la clave de cifrado mediante el esquema de clave.

El esquema de clave consiste en dos operaciones, expansión de clave y selección de clave de vuelta de cifrado, y el proceso de cifrado consta de tres pasos: una adición inicial de la clave de vuelta, n-1 vueltas de cifrado y una vuelta final.

RSA

El algoritmo de clave pública RSA fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. Estos señores se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública, crearon su algoritmo y fundaron la empresa RSA Data Security Inc., que es actualmente una de las más prestigiosas en el entorno de la protección de datos.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

Ahora bien, si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), tendremos que para factorizarlo habría que empezar por 1, 2, 3,..... hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

Se buscan dos números primos lo suficientemente grandes: **p** y **q** (de entre 100 y 300 dígitos).
Se obtienen los números $\mathbf{n} = p * q$ y $\mathbf{X} = (p-1) * (q-1)$.

Se busca un número **e** tal que no tenga múltiplos comunes con X.

Se calcula $\mathbf{d} = e^{-1} \bmod X$, con mod = resto de la división de números enteros.

Y ya con estos números obtenidos, **n es la clave pública y d es la clave privada**. Los números p, q y X se destruyen. También se hace público el número e, necesario para alimentar el algoritmo.

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

RSA basa su seguridad es ser una función computacionelmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo X no es factible a menos que se conozca la factorización de e, clave privada del sistema.
RSA es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

1.4 Funciones hash

Si imaginamos el envío de un documento extenso que queremos firmar digitalmente, nos daremos cuenta de que cifrar el documento entero es una pérdida de tiempo, ya que los medios de encriptación de llave pública son lentos, pues precisan un gran proceso de cómputo.

Para solventar éste aspecto aparecen las funciones hash, que son unas funciones matemáticas que realizan un resumen del documento a firmar. Su forma de operar es comprimir el documento en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real. Tanto es así que por definición las funciones hash son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, y si no es así no es una función hash. Estas funciones son además de dominio público.

A un mensaje resumido mediante una función hash y encriptado con una llave privada es lo que en la vida real se denomina firma digital.

Las funciones hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los Certificados Digitales.

Para que una función pueda considerarse como función hash debe cumplir:

- Debe transformar un texto de longitud variable en un bloque de longitud fija, que generalmente es pequeña (algunas son de 16 bits).
- Debe ser cómoda de usar e implementar
- Debe ser irreversible, es decir, no se puede obtener el texto original del resumen hash.
- Debe ser imposible encontrar dos mensajes diferentes cuya firma digital mediante la función hash sea la misma (no-colisión).
- Si se desea además mantener un intercambio de información con Confidencialidad, basta con cifrar el documento a enviar con la clave pública del receptor.

Las funciones hash más conocidas y usadas son:

MD2: Abreviatura de Message Digest 2, diseñado para ordenadores con procesador de 8 bits. Todavía se usa, pero no es recomendable, debido a su lentitud de proceso.

MD4: Abreviatura de Message Digest 4, desarrollado por Ron Rivest, uno de los fundadores de RSA Data Security Inc. y padre del sistema asimétrico RSA. Aunque se considera un sistema inseguro, es importante porque ha servido de base para la creación de otras funciones hash. Un sistema de ataque desarrollado por Hans Dobbertin posibilita el crear mensajes aleatorios con los mismos valores de hash (colisiones), por lo que ya no se usa. De hecho, existe un algoritmo que encuentra una colisión en segundos.

MD5: Abreviatura de Message Digest 5, también obra de Ron Rivest, que se creó para dar seguridad a MD4, y que ha sido ampliamente usado en diversos campos, como autenticador de mensajes en el protocolo SSL y como firmador de mensajes en el programa de correo PGP. Si embargo, fué reventado en 1996 por el mismo investigador que lo hizo con MD4, el señor Dobbertin, que consiguió crear colisiones en el sistema MD5, aunque por medio de ataques parciales. Pero lo peor es que también consiguió realizar ataques que comprometian la no-colisión, por lo que se podían obtener mensajes con igual hash que otro determinado. A pesar de todo esto, MD5 se sigue usando bastante en la actualidad.

SHA-1: Secure Hash Algorithm, desarrollado como parte integrante del Secure Hash Standar (SHS) y el Digital Signature Standar (DSS) por la Agencia de Seguridad Nacional Norteamericana, NSA. Sus creadores afirman que la base de este sistema es similar a la de MD4 de Rivest, y ha sido mejorado debido a ataques nunca desvelados. La versión actual se considera segura (por lo menos hasta que se demuestre lo contrario) y es muy utilizada algoritmo de firma, como en el programa PGP en sus nuevas claves DH/DSS (Diffie-Hellman/Digital Signature Standar). Destacar también que en la actualidad se están estudiando versiones de SHA con longitudes de clave de 256, 384 y 512 bits.

1.5 EL PROTOCOLO IPSEC

IPSec es un estándar de gran utilidad que se encarga de ofrecer servicios de seguridad avanzados en redes IP de cualquier índole.

IPSec está formado por un conjunto de estándares del IETF que conjuntamente proporcionan servicios de seguridad en la capa IP de las comunicaciones entre sistemas electrónicos, y por añadidura a todos los protocolos de niveles superiores que están basados en IP (TCP, UDP, ICMP, y otros).

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección al envío de datos

1.6 Protocolos de encriptamiento

Los protocolos utilizados en la actualidad para intercambiar información de manera que sea difícil que esta sea interceptada por terceros son SSH, SSL TSL y HTTPS.

SSH (Secure Shell)

Este protocolo fue diseñado para dar seguridad al acceso a computadores en forma remota. Cumple la misma función que telnet o rlogin pero además, usando criptografía, logra seguridad con los datos.

A diferencia de telnet u otro servicio similar, SSH utiliza el puerto 22 para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el sshd. El cliente debe ser un software tipo TeraTerm o Putty que permita la hacer pedidos a este puerto 22 de forma cifrada.

La forma en que se entabla una comunicación es en base la misma para todos los protocolos seguros:

- El cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido y le envía la llave pública al cliente para que pueda descifrar los mensajes.

- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

SSL (Secure Socket Layer) y TLS(Transport Layer Secure)

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL es una capa por debajo de HTTP y tal como lo indica su nombre está a nivel de socket por lo que permite ser usado no tan solo para proteger documentos de hipertexto sino también servicios como FTP, SMTP, TELNET entre otros.

La idea que persigue SSL es encriptar la comunicación entre servidor y cliente mediante el uso de llaves y algoritmos de encriptación.

El protocolo TLS esta basado en SSL y son similares en el modo de operar.

Es importante señalar que ambos protocolos se ejecutan sobre una capa de transporte definida, pero no determinada. Esto indica que pueden ser utilizados para cualquier tipo de comunicaciones. La capa de transporte más usada es TCP sobre la cual pueden implementar seguridad en HTTP.

Como punto de diferencia se puede mencionar que existen protocolos implementados sobre la capa de red, por ejemplo sobre IP. Tal es el caso de IPSec.

1. ¿De que están compuestos?

Estos protocolos se componen de dos capas: el Record Protocol y el Handshake Protocol.

El Record Protocol es la capa inmediatamente superior a TCP y proporciona una comunicación segura. Principalmente esta capa toma los mensajes y los codifica con algoritmos de encriptación de llave simétrica como DES, RC4 aplicándole una MAC (Message Authentication Code) para verificar la integridad, logrando así encapsular la seguridad para niveles superiores.

El Handshake protocol es la capa superior a la anterior y es usada para gestionar la conexión inicial.

2. ¿Cómo funcionan?

Después que se solicita una comunicación segura, servidor y el cliente se deben poner de acuerdo en como se comunicaran (SSL Handshake) para luego comenzar la comunicación encriptada. Luego de terminada la transacción, SSL termina.

a. Solicitud de SSL:

Tipicamente este proceso ocurre en el momento que un cliente accede a un servidor seguro, identificado con "https://...", pero como se mencionó, no necesariamente es usado para HTTP. La comunicación se establecerá por un puerto distinto al utilizado por el servicio normalmente. Luego de esta petición, se procede al SSL Handshake.

b. SSL Handshake:

En este momento, servidor y cliente se ponen de acuerdo en varios parámetros de la comunicación. Se puede dividir el proceso en distintos pasos:

- Client Hello: El cliente se presenta. Le pide al servidor que se presente (certifique quien es)y le comunica que algoritmos de encriptación soporta y le envía un número aleatorio para el caso que el servidor no pueda certificar su validez y que aun así se pueda realizar la comunicación segura.

- Server Hello: El servidor se presenta. Le responde al cliente con su identificador digital encriptado, su llave pública, el algoritmo que se usará, y otro número aleatorio. El algoritmo usado será el más poderoso que soporte tanto el servidor como el cliente.

- Aceptación del cliente: El cliente recibe el identificador digital del servidor, lo desencripta usando la llave pública también recibida y verifica que dicha identificación proviene de una empresa certificadora segura. Luego se procede a realizar verificaciones del certificado (identificador) por medio de fechas, URL del servidor, etc. Finalmente el cliente genera una llave aleatoria usando la llave pública del servidor y el algoritmo seleccionado y se la envía al servidor.

- Verificación: Ahora tanto el cliente y el servidor conocen la llave aleatoria (El cliente la generó y el servidor la recibió y desencripto con su llave privada). Para asegurar que nada ha cambiado, ambas partes se envían las llaves. Si coinciden, el Handshake concluye y comienza la transacción.

1.7 CERTIFICADOS DIGITALES

Los Certificados electrónicos son documentos digitales que sirven para asegurar la Veracidad de la Clave Pública perteneciente al propietario del certificado ó de la entidad, con la que se firman digitalmente documentos que puedan proporcionar las más absolutas garantías de seguridad respecto a cuatro elementos fundamentales:

- La autentificación del usuario/entidad (es quien asegura ser).
- La confidencialidad del mensaje (que sólo lo podrá leer el destinatario).
- La integridad del documento (nadie los ha modificado).
- El no repudio (el mensaje una vez aceptado, no puede ser rechazado por el emisor).

Es, por tanto, muy importante estar realmente seguros de que la Clave Pública que manejamos para verificar una firma o cifrar un texto, pertenece realmente a quien creemos que pertenece.

Un certificado electrónico contiene una **clave pública**, y una **firma digital.**
Para su correcto funcionamiento, los certificados contienen además la siguiente información:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.
- Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
- Dos fechas, una de inicio y otra de fin del periodo de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

Además de servir como mecanismo confiable y seguro de identificación en la red, el certificado de identidad digital le permite disfrutar de otra serie de beneficios:

- Puede enviar y recibir información confidencial, asegurándose que sólo el remitente pueda leer el mensaje enviado
- Puede acceder a sitios Web de manera segura con su identidad digital, sin tener que usar el peligroso mecanismo de passwords;
- Puede firmar digitalmente documentos, garantizando la integridad del contenido y autoría del documento y todas aquellas aplicaciones en que se necesiten mecanismos seguros para garantizar la identidad de las partes y confidencialidad e integridad de la información intercambiada, como comercio electrónico, declaración de impuestos, pagos,provisionales, uso en la banca, etc.

La Autoridad de Certificación (CA), es quien firma digitalmente los certificados, asegurando su integridad y certificando la relación existente entre la Clave Pública contenida y la identidad del propietario. La firma de la CA es la que garantiza la validez de los certificados.

1.8 TIPOS DE CERTIFICADOS

Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en:

1. **Certificados SSL para cliente:** usados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

2. **Certificados SSL para servidor:** usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor.
La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

3. **Certificados S/MIME** : usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autenticación, Integridad y No Rechazo. También se puede cifrar el mensaje con la llave pública del destinatario, lo que proporciona confidencialidad al envío.

4. **Certificados de firma de objetos**: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de éste tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.

5. **Certificados para AC**: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.Toda persona o entidad que deseé obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de
comprobación de datos (clase mayor), más costará el certificado.

1.9 PROTOCOLO HTTPS.

Generalmente la transferencia de datos que se realiza mediante el protocolo HTTP es en texto claro. Eso quiere decir que los ordenadores intermedios que enrutan la conexión podrían leer lo que enviamos. Esto puede preocuparnos o no cuando estamos leyendo un periódico on-line, pero sin lugar a dudas nos importará si lo que estamos haciendo es digitando nuestros datos de usuario y contraseña ,mandando nuestros datos. Para solucionar este problema, se usa el protocolo HTTPS que es el protocolo HTTP, pero cifrado. De esta manera, nuestro navegador enviará las peticiones y los datos encriptados y el servidor los desencriptará convenientemente. Los nodos intermedios podrán mirar en los paquetes, pero no entenderán nada porque su contenido estará cifrado.

Uno de los usos comunes de ssl es el de establecer una comunicación Web segura entre un browser y un Webserver. Es aquí donde se usa https que es básicamente http sobre ssl con un esquema de invocación por medio de url. Es importante hacer notar que el uso del protocolo https no impide en caso alguno que se pueda utilizar http, por lo que la mayoría de los browsers advierten cuando una página tiene elementos que no son seguros en entornos seguros, como también advierten cuando se invoca un protocolo distinto al de la pagina actual

PROTOCOLO DE CORREO SMTP

SMTP son las siglas de Protocolo Simple de Transmisión de Correo ("Simple Mail Transfer Protocol"). Este protocolo es un estándar de Internet para el intercambio de correo electrónico. Para ser un poco más claro, usted al momento de enviar un correo electrónico utiliza como medio un servidor SMTP que es el encargado de hacer llegar el correo a su destino, lo podemos comparar con el servicio postal, para hacer entrega del correo necesitamos de tres datos importantes el origen, el destino y el medio que es el servidor SMTP. A continuación se explica por qué usted debe configurar la Autenticación SMTP.

¿POR QUÉ CONFIGURAR LA AUTENTICACIÓN SMTP?

La Autenticación SMTP se configura con el fin de elevar los niveles de seguridad y eficacia del servicio de correo electrónico y con el objetivo de minimizar la posibilidad que su cuenta sea utilizada sin autorización desde su PC o desde otras, asimismo disminuirá la posibilidad que su PC sea utilizada como "puente" para el envio de correos masivos a través de nuestros servidores. Si usted es usuario del servicio Ipass le permitirá el envió y revisión de correo desde cualquier parte del mundo.

POSTAL OFFICE PROTOCOL. Conocido comúnmente por sus siglas, POP, se trata de un protocolo de correo electrónico, que permite que los mensajes de correo pendientes se almacenen hasta que el usuario se conecte y los solicite. Existen 3 versiones del protocolo: POP, POP2 y POP3, siendo esta última la más utilizada en la actualidad.

El protocolo POP permite almacenar los mensajes de correo en el ordenador del propio usuario, pudiendo consultarlo cuantas veces desee. Obviamente, esto contrasta fundamentalmente con la filosofia del correo IMAP, o del hoy tan en boga correo web.Frente a la ventaja de estos dos últimos sistemas, que posibilitan al usuario leer sus mensajes en cualquier ordenador, está un lo que en mi opinión resulta un inconveniente básico: se debe estar conectado para poder leer el correo; de modo que siempre que estemos leyendo correo, estaremos pagando. Si tenemos muy pocos mensajes, este protocolo puede ser adecuado, máxime en las personas que por su trabajo o funciones no tengan otra posibilidad. Sin embargo, el usuario que reciba muchos mensajes, o que quiera tenerlos guardados, deberia descartar su uso e inclinarse por el protocolo POP.

IMAP 4.

IMAP es la abreviatura de Internet Message Access Protocol.Es un método de acceso al correo electrónico que se mantiene en el servidor correspondiente.A diferencia del protocolo POP 3 que retira los mensajes del servidor al conectarse y los almacena en el servidor local, IMAP 4 los deja en el servidor remoto, con lo que es posible acceder a los mismos desde diferentes puntos(oficina, casa etc.).

Su particularidad es que deja crear múltiples buzones en la máquina remota, es útil para alguien que viaja para no tener la necesidad de llevarse un equipo consigo, sino poder bajar los mensajes desde cualquier otro equipo, e inclusive permite que varios usuarios entren al mismo buzón a las vez a ver los mismos mensajes.

SMTPS

Es lo mismo que SMTP pero con una capa SSL que permite encriptar la conexión

POP3S

Lo mismo que POP3 pero con una capa SSL que permite encriptar la conexión

IMAPS
Lo mismo que IMAP pero con una capa SSL que permite encriptar la conexión

TECNICAS DE FRAUDE

EAVESDROPPING Y PACKET SNIFFING

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Este método es muy utilizado para capturar nombres y claves de usuarios, que generalmente viajan claros (sin encriptar). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos una descarga de la información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

TAMPERING O DATA DIDDLING

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliverada.

PHISHING

Es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

De forma más general, el nombre phishing también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito, haciéndose pasar por alguien digno de confianza con una necesidad verdadera de tal información en un e-mail parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque de la ingeniería social.

2. ANALISIS DE LOS DATOS QUE VIAJAN POR ALGUNOS DE LOS SERVICIOS QUE OFRECE LA RED DE LA CORPORACION UNIVERSITARIA UNITEC

La Red de la Corporación Universitaria Unitec esta conformada por varias subredes las cuales están distribuidas en las diversas sedes que hacen parte de la universidad, estas subredes se integran en el nodo principal el cual las intercomunica y les da salida hacia Internet.

Los usuarios de la red de Unitec son los alumnos, docentes, egresados y personal administrativo los cuales utilizan servicios muy diferentes de la misma, por tal motivo la red se ha incrementado no solo en terminales de trabajos sino también en servicios ofrecidos

Este crecimiento en servicios no solo se ve influenciado por el crecimiento pedagógico y tecnológico de la universidad sino por el avance en la tecnología de los servicios ofrecidos a través de Internet por todas las empresas del país; transacciones en línea, comercio electrónico, transacciones bancarias, comunicación virtual, foros de discusión, consulta de información en línea, etc. son algunas facilidades que Internet ha traído consigo pero con ellas también han llegado algunos aspectos no tan positivos los cuales han generado intranquilidad en los usuarios que utilizan estos servicios.

Este miedo es originado porque la gran mayoría de servicios no ofrecen métodos confiables y seguros de encriptamiento de la información que viaja de una terminal a otra y de un servidor a otro.

Entendiendo la situación que se presenta en la actualidad se quiso evaluar los datos que viajan a través de los diferentes servicios de la red de la Corporación Universitaria UNITEC, para ello se dejo corriendo un programa de tipo sniffer llamado Iris Network 4.7 en los siguientes puntos de la red de unitec:

- Dos maquinas del laboratorio 5 de la sede C por un tiempo de 8 horas
- Una máquina del Departamento de Informática por un tiempo de 24 horas.

Con el levantamiento de la información recolectada por este programa se pudo evaluar la situación actual de los datos que viajan por los diferentes servicios que se trabajan en la red de unitec.

A continuación se realizará una descripción detallada de los servicios que ofrece la red explicando el protocolo con el cual trabaja el servicio, la funcionalidad del servicio y la forma como viajan los datos.

2.1 Correo electrónico

El servicio de correo electrónico se ofrece en la universidad a través de dos protocolos el Post Office Protocol versión 3 (POP3) y el Internet Message Access Protocol versión 4 (IMAP4)

2.1.1 POP3

Diseñado para la gestión, el acceso y la transferencia de mensajes de correo electrónico entre dos máquinas, habitualmente un servidor y una máquina de usuario. Los servidores POP3 permiten tener acceso a una sola bandeja de entrada. Este protocolo es fuera de línea por ello los mensajes se quedan en espera en el servidor hasta que este se conecte y luego por medio de un programa de correo (Outlook, Thunderbird, netscape mail, etc.) instalado en la maquina del cliente se descargan al disco duro los correos eliminándolos del servidor. El protocolo POP3 utiliza el puerto 110 del servidor para su comunicación con los clientes. En la red de unitec este servicio lo ofrece un servidor con sistema operacional Linux RedHat 9.0 e identificado con la dirección IP 192.168.1.7.

El servicio de correo electrónico a través de POP3 en la red de la universidad es utilizado por la parte administrativa, es decir, funcionarios, ejecutivos y directivos que conforman la institución.
Para analizar este servicio se evaluaron 103 paquetes en los cuales se encontró que la información de validación del usuario en el cliente de correo para su consulta viaja totalmente plana, es decir, que aunque la información que digita el usuario cuando el cliente de correo le pide un usuario y una contraseña no se visualiza la información sale de la máquina sin ningún tipo de encriptamiento.

A continuación se puede observar en los gráficos la forma como viaja la información para el servicio de POP3.

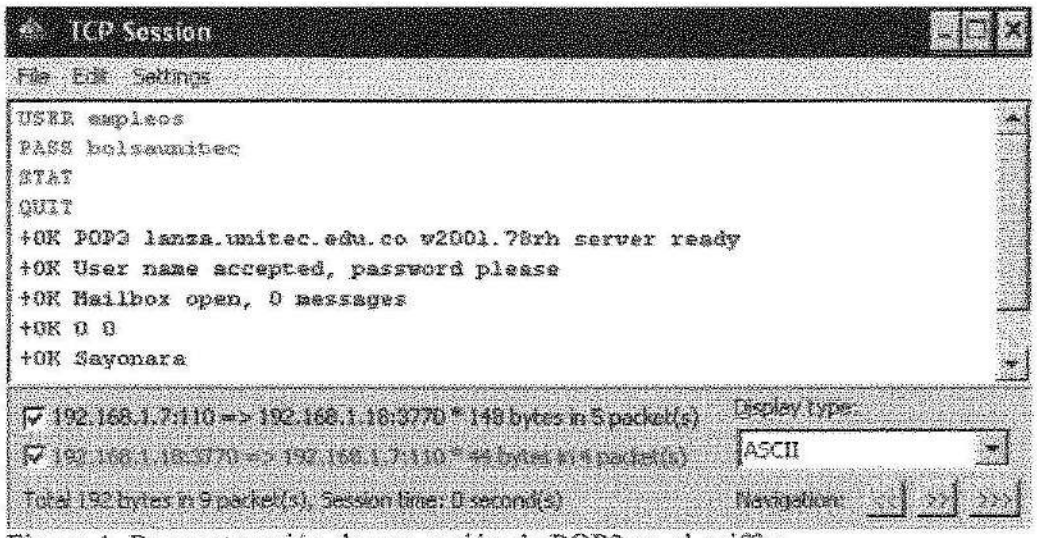


Figura 1. Reconstrucción de una sesión de POP3 en el sniffer

Información de los paquetes que envían la información sin encriptar

---

Packet #195, Direction: Pass-through, Time:09:46:19,730000, Size: 68
Ethernet II
Destination MAC: 00:E0:7D:9F:52:64
Source MAC: 00:0D:56:4E:C9:F8
Ethertype: 0x0800 (2048) - IP
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Precedence: 000 - Routine
Delay: 0 - Normal delay
Throughput: 0 - Normal throughput
Reliability: 0 - Normal reliability
Total length: 0x0036 (54)
ID: 0x6D2B (27947)
Flags
Don't fragment bit: 1 - Don't fragment
More fragments bit: 0 - Last fragment
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x06 (6) - TCP
Checksum: 0x0A2D (2605) - correct
Source IP: 192.168.1.18
Destination IP: 192.168.1.7
IP Options: None
TCP
Source port: 3772
Destination port: 110
Sequence: 0x05DC44B1 (98321585)
Acknowledgement: 0x98076378 (2550621048)
Header length: 0x05 (5) - 20 bytes
Flags: PSH ACK
URG: 0
ACK: 1
PSH: 1
RST: 0

```
                SYN: 0
                FIN: 0
        Window: 0xFFC9 (65481)
        Checksum: 0x8392 (33682) - incorrect
        Urgent Pointer: 0x0000 (0)
        TCP Options: None
POP3
        Username: admins
================================================================================

Packet #198, Direction: Pass-through, Time:09:46:19,731000, Size: 68
Ethernet II
        Destination MAC: 00:E0:7D:9F:52:64
        Source MAC: 00:0D:56:4E:C9:F8
        Ethertype: 0x0800 (2048) - IP
IP
        IP version: 0x04 (4)
        Header length: 0x05 (5) - 20 bytes
        Type of service: 0x00 (0)
                Precedence: 000 - Routine
                Delay: 0 - Normal delay
                Throughput: 0 - Normal throughput
                Reliability: 0 - Normal reliability
        Total length: 0x0036 (54)
        ID: 0x6D30 (27952)
        Flags
                Don't fragment bit: 1 - Don't fragment
                More fragments bit: 0 - Last fragment
        Fragment offset: 0x0000 (0)
        Time to live: 0x80 (128)
        Protocol: 0x06 (6) - TCP
        Checksum: 0x0A28 (2600) - correct
        Source IP: 192.168.1.18
        Destination IP: 192.168.1.7
        IP Options: None
TCP
        Source port: 3772
        Destination port: 110
        Sequence: 0x05DC44BF (98321599)
        Acknowledgement: 0x980753A1 (2550621089)
        Header length: 0x05 (5) - 20 bytes
        Flags: PSH ACK
                URG: 0
                ACK: 1
                PSH: 1
                RST: 0
                SYN: 0
                FIN: 0
        Window: 0xFFA0 (65440)
        Checksum: 0x8392 (33682) - incorrect
        Urgent Pointer: 0x0000 (0)
        TCP Options: None
POP3
        Password: admins
Raw Data:
0x0000  00 E0 7D 9F 52 64 00 0D-56 4E C9 F8 08 00 45 00   .à}ŸRd..VNÉø..E.
0x0010  00 36 6D 30 40 00 80 06-0A 28 C0 A8 01 12 C0 A8   .6m0@.€..(À¨..À¨
0x0020  01 07 0E BC 00 6E 05 DC-44 BF 98 07 63 A1 50 18   ...¼.n.ÜD¿˜.c¡P.
0x0030  FF A0 83 92 00 00 50 41-53 53 20 61 64 6D 69 6E   ÿ ƒ'..PASS admin
0x0040  69 73 0D 0A                                       is..

================================================================================
```

2.1.2 IMAP4

Es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.
A diferencia del POP3 el correo no es descargado inmediatamente sino que es leído o consultado directamente en el servidor y permanece en este hasta que el usuario lo elimine.
Como los correos permanecen en el servidor se pueden consultar desde cualquier computador ya sea a través de un cliente de correo o por una página web.

El protocolo IMAP4 utiliza el puerto 143 del servidor para su consulta. En la red de Unitec este servicio lo ofrece el mismo servidor Linux que ofrece POP3 a través de una aplicación de consulta vía web llamada squirrelmail.

Los usuarios de este servicio son los estudiantes, docentes y algunos administrativos que consultan su correo desde la casa.

En el análisis realizado a los paquetes que utiliza este servicio se encontró que la información que viaja entre el servidor y el cliente no utiliza ningún método de encriptamiento, viaja totalmente plana.

A continuación se puede observar en el gráfico y en la información de los paquetes la forma como viajan los datos para el servicio de IMAP4.

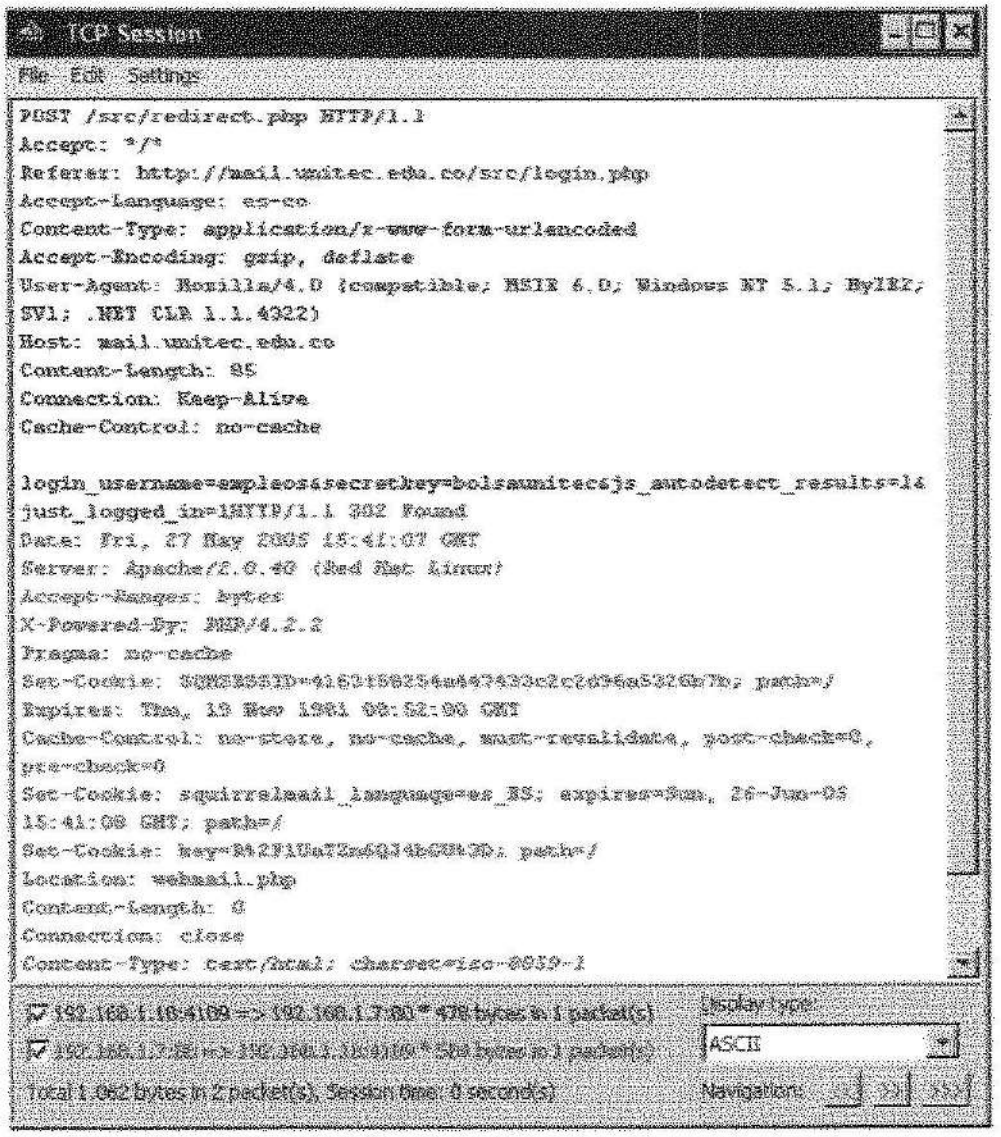


Figura 2. Reconstrucción de una sesión de IMAP4 en el sniffer

Información de los paquetes que envían la información sin encriptar

```
================================================================================
Packet #8996, Direction: Pass-through, Time:10:37:30,777000, Size: 532
Ethernet II
        Destination MAC: 00:E0:7D:9F:52:64
        Source MAC: 00:0D:56:4E:C9:F8
        Ethertype: 0x0800 (2048) - IP
IP
        IP version: 0x04 (4)
        Header length: 0x05 (5) - 20 bytes
        Type of service: 0x00 (0)
                Precedence: 000 - Routine
```

```
                Delay: 0 - Normal delay
                Throughput: 0 - Normal throughput
                Reliability: 0 - Normal reliability
        Total length: 0x0206 (518)
        ID: 0xF8D1 (63697)
        Flags
                Don't fragment bit: 1 - Don't fragment
                More fragments bit: 0 - Last fragment
        Fragment offset: 0x0000 (0)
        Time to live: 0x80 (128)
        Protocol: 0x06 (6) - TCP
        Checksum: 0x7CB6 (31926) - correct
        Source IP: 192.168.1.18
        Destination IP: 192.168.1.7
        IP Options: None
TCP
        Source port: 4109
        Destination port: 80
        Sequence: 0x0E668560 (241612141)
        Acknowledgement: 0x595754F5 (1498895605)
        Header length: 0x05 (5) - 20 bytes
        Flags: PSH ACK
                URG: 0
                ACK: 1
                PSH: 1
                RST: 0
                SYN: 0
                FIN: 0
        Window: 0xFFFF (65535)
        Checksum: 0x8582 (34146) - incorrect
        Urgent Pointer: 0x0000 (0)
        TCP Options: None
HTTP
        Version: HTTP/1.1
        Method: POST
        URI: /src/redirect.php
        Accept: */*
        Referer: http://mail.unitec.edu.co/src/login.php
        Accept-Language: es-co
        Content-Type: application/x-www-form-urlencoded
        Accept-Encoding: gzip, deflate
        User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; MyIE2; SV1; .NET CLR 1.1.4322)
        Host: mail.unitec.edu.co
        Content-Length: 85
        Connection: Keep-Alive
        Cache-Control: no-cache
        Data
Raw Data:
0x0000  00 E0 7D 9F 52 64 00 0D-56 4E C9 F8 08 00 45 00  .à}ŸRd..VNÉø..E.
0x0010  02 06 F8 D1 40 00 80 06-7C B6 C0 A8 01 12 C0 A8  ..øÑ@.€.|¶À¨..À¨
0x0020  01 07 10 0D 00 50 0E 66-B5 6D 59 57 54 F5 50 18  .....P.fµmYWTõP.
0x0030  FF FF 85 82 00 00 50 4F-53 54 20 2F 73 72 63 2F  ÿÿ...b..POST /src/
0x0040  72 65 64 69 72 65 63 74-2E 70 68 70 20 48 54 54  redirect.php HTT
0x0050  50 2F 31 2E 31 0D 0A 41-63 63 65 70 74 3A 20 2A  P/1.1..Accept: *
0x0060  2F 2A 0D 0A 52 65 66 65-72 65 72 3A 20 68 74 74  /*..Referer: htt
0x0070  70 3A 2F 2F 6D 61 69 6C-2E 75 6E 69 74 65 63 2E  p://mail.unitec.
0x0080  65 64 75 2E 63 6F 2F 73-72 63 2F 6C 6F 67 69 6E  edu.co/src/login
0x0090  2E 70 68 70 0D 0A 41 63-63 65 70 74 2D 4C 61 6E  .php..Accept-Lan
0x00A0  67 75 61 67 65 3A 20 65-73 2D 63 6F 0D 0A 43 6F  guage: es-co..Co
0x00B0  6E 74 65 6E 74 2D 54 79-70 65 3A 20 61 70 70 6C  ntent-Type: appl
0x00C0  69 63 61 74 69 6F 6E 2F-78 2D 77 77 77 2D 66 6F  ication/x-www-fo
0x00D0  72 6D 2D 75 72 6C 65 6E-63 6F 64 65 64 0D 0A 41  rm-urlencoded..A
0x00E0  63 63 65 70 74 2D 45 6E-63 6F 64 69 6E 67 3A 20  ccept-Encoding:
0x00F0  67 7A 69 70 2C 20 64 65-66 6C 61 74 65 0D 0A 55  gzip, deflate..U
```

```
0x0100  73 65 72 2D 41 67 65 6E-74 3A 20 4D 6F 7A 69 6C  ser-Agent: Mozil
0x0110  6C 61 2F 34 2E 30 20 28-63 6F 6D 70 61 74 69 62  la/4.0 (compatib
0x0120  6C 65 3B 20 4D 53 49 45-20 36 2E 30 3B 20 57 69  le; MSIE 6.0; Wi
0x0130  6E 64 6F 77 73 20 4E 54-20 35 2E 31 3B 20 4D 79  ndows NT 5.1; My
0x0140  49 45 32 3B 20 53 56 31-3B 20 2E 4E 45 54 20 43  IE2; SV1; .NET C
0x0150  4C 52 20 31 2E 31 2E 34-33 32 32 29 0D 0A 48 6F  LR 1.1.4322)..Ho
0x0160  73 74 3A 20 6D 61 69 6C-2E 75 6E 69 74 65 63 2E  st: mail.unitec.
0x0170  65 64 75 2E 63 6F 0D 0A-43 6F 6E 74 65 6E 74 2D  edu.co..Content-
0x0180  4C 65 6E 67 74 68 3A 20-38 35 0D 0A 43 6F 6E 6E  Length: 85..Conn
0x0190  65 63 74 69 6F 6E 3A 20-4B 65 65 70 2D 41 6C 69  ection: Keep-Ali
0x01A0  76 65 0D 0A 43 61 63 68-65 2D 43 6F 6E 74 72 6F  ve..Cache-Contro
0x01B0  6C 3A 20 6E 6F 2D 63 61-63 68 65 0D 0A 0D 0A 6C  l: no-cache....l
0x01C0  6F 67 69 6E 5F 75 73 65-72 6E 61 6D 65 3D 65 6D  ogin_username=em
0x01D0  70 6C 65 6F 73 26 73 65-63 72 65 74 6B 65 79 3D  pleos&secretkey=
0x01E0  62 6F 6C 73 61 75 6E 69-74 65 63 26 6A 73 5F 61  bolsaunitec&js_a
0x01F0  75 74 6F 64 65 74 65 63-74 5F 72 65 73 75 6C 74  utodetect_result
0x0200  73 3D 31 26 6A 75 73 74-5F 6C 6F 67 67 65 64 5F  s=1&just_logged_
0x0210  69 6E 3D 31
```

2.2 Aplicaciones WEB

HTTP(Hyper Text Transfer Protocol) Es el protocolo de la Web (WWW), usado en cada transacción. Las letras significan Hyper Text Transfer Protocol, es decir, protocolo de transferencia de hipertexto. El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. También sirve el protocolo para enviar información adicional en ambos sentidos. El protocolo HTTP utiliza el puerto 80 para la comunicación con el cliente.
En la red de Unitec este servicio lo ofrece un servidor Windows 2000 a través de Internet Information Server 5.0. Los sitios creados que viajan por medio del puerto 80 son los siguientes:

2.2.1 alumnos.unitec.edu.co

Este portal consolida información y servicios académicos como consulta de notas, registro de materias, consulta de horario, aplicación de evaluaciones, reservas de medios audiovisuales, actualización de datos entre otros, para todos los alumnos activos de la institución.

El objetivo de este sitio es ofrecer día a día más servicios a los estudiantes para facilitar y agilizar procesos ó procedimientos que el estudiante debe desarrollar durante su vida académica en el semestre.

Analizando la información capturada en los paquetes enviados por este servicio se pudo observar que el proceso de validación del estudiante en el portal se realiza de una forma segura. Los datos enviados desde la terminal al servidor viajan encriptados mediante una

función HASH asimétrica utilizando el algoritmo MD5 para su codificación. La encriptación de la información la realiza antes de salir de la máquina cliente utilizando un script de javascript.

A continuación se puede observar el gráfico en donde se aprecia que la información viaja de forma segura:

Figura 3. Proceso de encriptación de la información por medio del algoritmo MD5

En el gráfico que se observa a continuación se puede apreciar como el campo pasword envía la información encriptada.

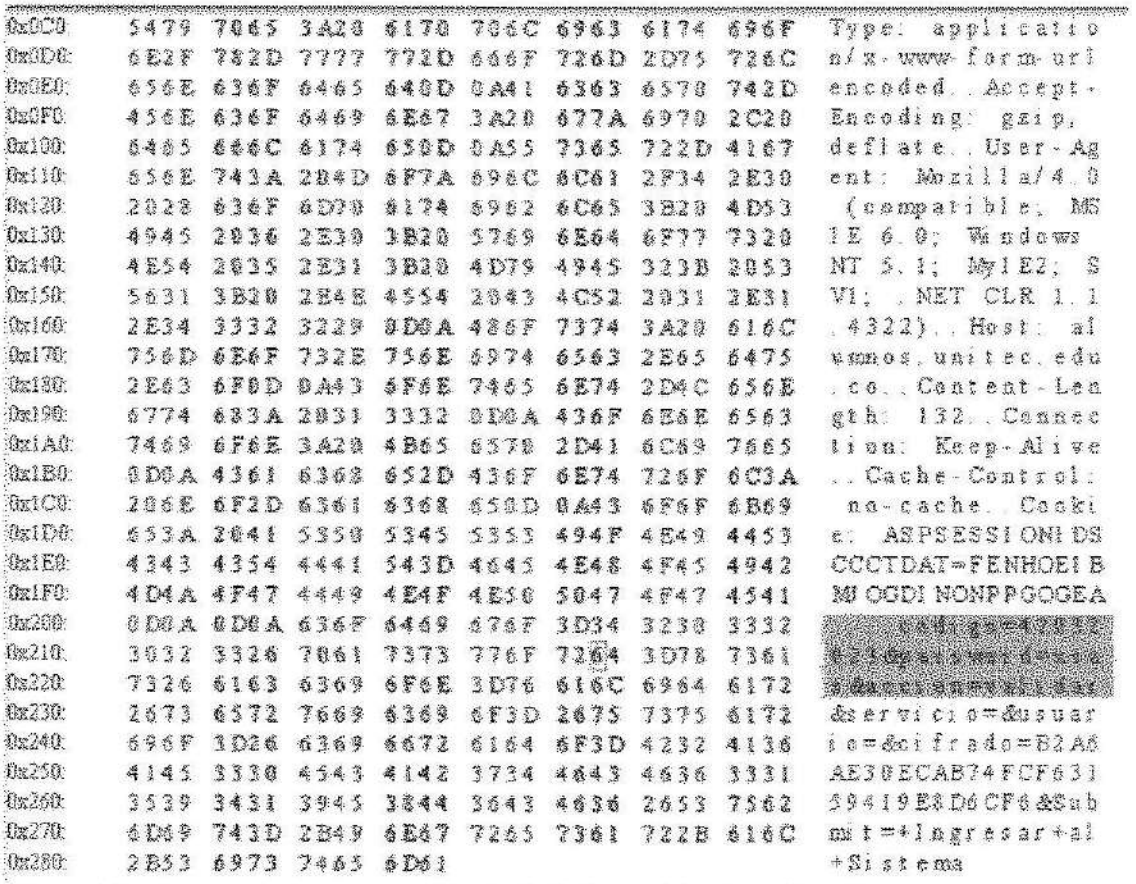


Figura No. 4 proceso de encriptación de la información de sesión alumnos

2.2.2 docentes.unitec.edu.co

Portal creado para la consolidación de información y servicios académicos a los docentes. Entre los servicios que puede utilizar el docente en este sitio están: consulta de carga académica, consulta de estudiantes por módulo, evaluación de módulos, captura de notas, reserva de audiovisuales, actualización de datos, consulta de correo.

Al igual que el portal de alumnos la universidad tiene proyectado ofrecer diversos servicios en este portal que faciliten, agilicen y optimicen los procesos académicos y administrativos que el docente debe realizar durante el semestre.

De la muestra recolectada (18 paquetes) se pudo analizar que la información de validación del profesor contenida en ellos no viaja encriptada, es decir que los datos transmitidos entre el cliente y el servidor viaja totalmente plana.

A continuación se puede observar el gráfico en donde se aprecia que la información viaja de forma insegura:

Time	Src IP	Dest IP	Pr	Len	Src Port	Dest Port
14:25:36:442	192.168.1.18	192.168.1.8	TCP	172	1420	445
14:25:36:458	192.168.1.8	192.168.1.18	TCP	148	445	1420
14:25:36:458	192.168.1.18	192.168.1.8	TCP	172	1420	445
14:25:36:458	192.168.1.8	192.168.1.18	TCP	148	445	1420
14:25:36:458	192.168.1.18	192.168.1.8	TCP	85	1420	445
14:25:36:458	192.168.1.8	192.168.1.18	TCP	79	445	1420
14:25:36:614	192.168.1.18	192.168.1.8	TCP	40	1420	445
14:25:36:723	192.168.1.18	192.168.1.8	TCP	48	3955	80
14:25:36:739	192.168.1.18	192.168.1.8	TCP	40	3955	80
14:25:36:739	192.168.1.8	192.168.1.18	TCP	48	80	3955
14:25:36:739	192.168.1.18	192.168.1.8	TCP	557	3955	80
14:25:36:739	192.168.1.8	192.168.1.18	TCP	129	80	3955
14:25:36:848	192.168.1.18	192.168.1.8	TCP	144	1420	445
14:25:36:848	192.168.1.8	192.168.1.18	TCP	179	445	1420

0x130:	204D	7949	4532	3B20	5356	313B	202E	4E45	My IE2; SV1; . NE
0x140:	5420	434C	5220	312E	312E	3433	3232	290D	T CLR 1.1.4322).
0x150:	0A48	6F73	743A	2064	6F63	656E	7465	732E	.Host: docentes.
0x160:	756E	6974	6563	2E65	6475	2E63	6F0D	0A43	unitec.edu.co..C
0x170:	6F6E	7465	6E74	2D4C	656E	6774	683A	2036	ontent-Length: 6
0x180:	3420	0A43	6F6E	6E65	6374	696F	6E3A	204B	4..Connection: K
0x190:	6565	702D	416C	6976	650D	0A43	6163	6865	eep-Alive..Cache
0x1A0:	2D43	6F6E	7472	6F6C	3A20	6E6F	2D63	6163	-Control: no-cac
0x1B0:	6865	0D0A	436F	6F6B	6965	3A20	4153	5053	he..Cookie: ASPS
0x1C0:	4553	5349	4F4E	4944	5343	4343	5444	4154	ESSIONIDSCCCTDAT
0x1D0:	3D4D	414F	4848	4549	4248	4D46	4C41	414D	=MAOHOEIBHMFLAAM
0x1E0:	4444	4944	4C49	4B4F	450D	0A0D	0A63	6564	DDIDLIKOE....ced
0x1F0:	756C	613D	3032	3038	3434	3526	636F	6E74	ula=20244&cont
0x200:	7261	3D73	636F	7461	7163	6869	2653	7562	ra=scotaquichi&Sub
0x210:	6D69	743D	456E	7472	6172	2673	6553	7669	mit=Entrar&eServi
0x220:	6369	6F3D	2675	7375	6172	696F	3D		cio=&usuario=

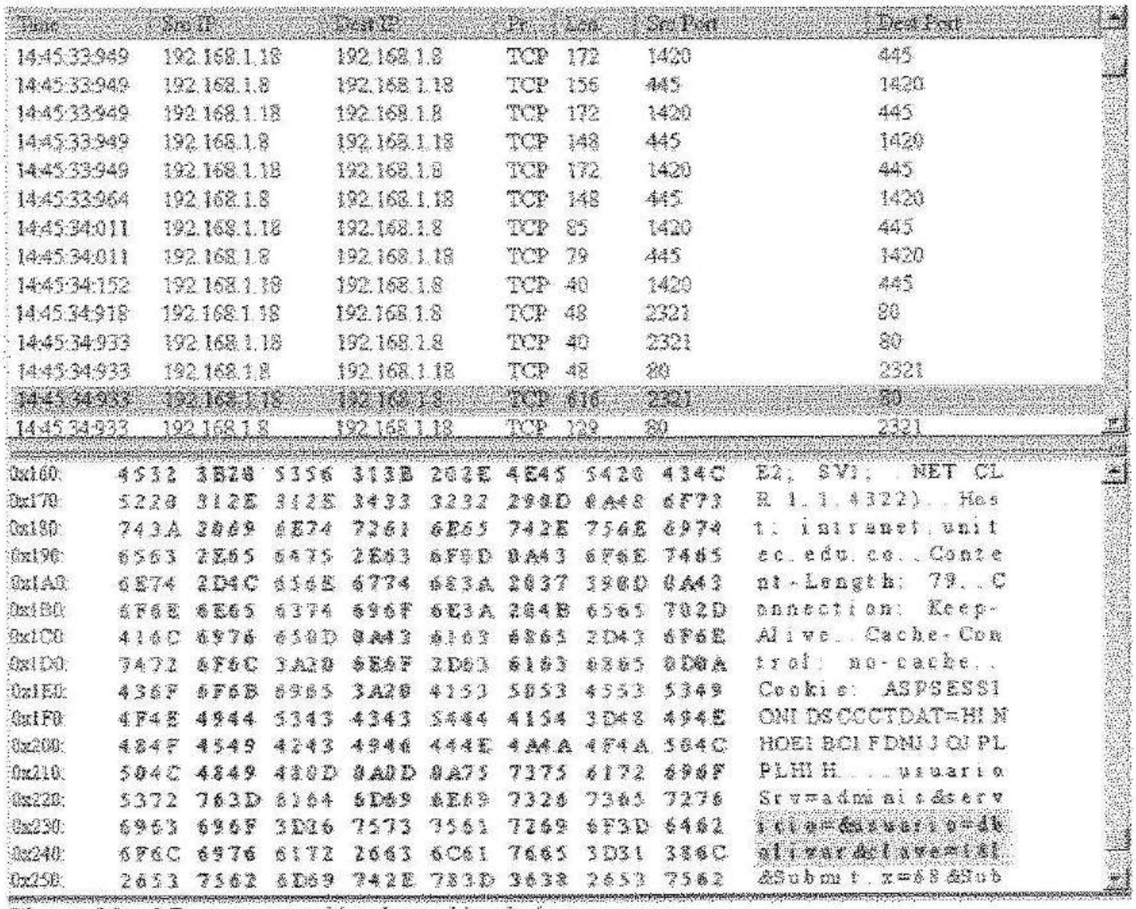
Figura No 5 Reconstrucción de sesión por el portal docentes

2.2.3. intranet.unitec.edu.co

En este portal los empleados de la universidad pueden consultar información de interés general y realizar una serie de transacciones a servicios implementados para agilizar algunos procesos establecidos internamente en las áreas académicas y administrativas de la institución.

Al analizar la información de los paquetes que viajan por la red y llevan información de este servicio (26 paquetes) se observo que el proceso de validación del personal administrativo al sitio se realiza por medio de un archivo de encriptación de claves creado por programación para el sitio.

La información del paquete en donde se envia la contraseña es el siguiente:



Time	Src IP	Dest IP	Pr	Len	Src Port	Dest Port
14:45:33:949	192.168.1.18	192.168.1.8	TCP	172	1420	445
14:45:33:949	192.168.1.8	192.168.1.18	TCP	156	445	1420
14:45:33:949	192.168.1.18	192.168.1.8	TCP	172	1420	445
14:45:33:949	192.168.1.8	192.168.1.18	TCP	148	445	1420
14:45:33:949	192.168.1.18	192.168.1.8	TCP	172	1420	445
14:45:33:964	192.168.1.8	192.168.1.18	TCP	148	445	1420
14:45:34:011	192.168.1.18	192.168.1.8	TCP	85	1420	445
14:45:34:011	192.168.1.8	192.168.1.18	TCP	79	445	1420
14:45:34:152	192.168.1.18	192.168.1.8	TCP	40	1420	445
14:45:34:918	192.168.1.18	192.168.1.8	TCP	48	2321	80
14:45:34:933	192.168.1.18	192.168.1.8	TCP	40	2321	80
14:45:34:933	192.168.1.8	192.168.1.18	TCP	48	80	2321
14:45:34:933	192.168.1.18	192.168.1.8	TCP	616	2321	80
14:45:34:933	192.168.1.8	192.168.1.18	TCP	129	80	2321

```
0x160: 4532 3B20 5356 313B 202E 4E45 5420 434C  E2; SV1; .NET CL
0x170: 5220 312E 312E 3433 3232 290D 0A48 6F73  R 1.1.4322)..Hos
0x180: 743A 2069 6E74 7261 6E65 742E 756E 6974  t: intranet.unit
0x190: 6563 2E65 6475 2E63 6F0D 0A43 6F6E 7465  ec.edu.co..Conte
0x1A0: 6E74 2D4C 656E 6774 683A 2037 390D 0A43  nt-Length: 79..C
0x1B0: 6F6E 6E65 6374 696F 6E3A 204B 6565 702D  onnection: Keep-
0x1C0: 416C 6976 650D 0A43 6163 6865 2D43 6F6E  Alive..Cache-Con
0x1D0: 7472 6F6C 3A20 6E6F 2D63 6163 6865 0D0A  trol: no-cache..
0x1E0: 436F 6F6B 6965 3A20 4153 5053 4553 5349  Cookie: ASPSESSI
0x1F0: 4F4E 4944 5343 4343 5444 4154 3D48 494E  ONIDSCCCTDAT=HIN
0x200: 484F 4549 4243 4946 444E 4A4A 4F4A 504C  HOEIBCIFDNJJOJPL
0x210: 504C 4849 480D 0A0D 0A75 7375 6172 696F  PLHIH....usuario
0x220: 5372 763D 6164 6D69 6E69 7326 7365 7276  Srv=adminis&serv
0x230: 6963 696F 3D26 7573 7561 7269 6F3D 6462  icio=&usuario=db
0x240: 6F6C 6976 6172 2663 6C61 7665 3D31 386C  olivar&clave=18l
0x250: 2653 7562 6D69 742E 783D 3638 2653 7562  &Submit.x=68&Sub
```

Figura No 6 Reconstrucción de sesión de intranet

2.2.4. adsi.unitec.edu.co

Este sitio permite consultar vía web el directorio activos de Windows. Por medio de este sitio el administrador de la red puede crear, restaurar y borrar cuentas de usuarios de la red, restaurar y cambiar contraseñas de las cuentas, buscar y comprobar la existencia de usuarios en la red.

Este sitio permite de forma fácil la administración de las cuentas de la red sin necesidad de estar ubicado directamente en el servidor principal.

Al realizar el análisis de los paquetes utilizados por este servicio en las diversas opciones del sitio se observo que en todas aquellas en donde el usuario digita claves para validación, comprobación o cambio la información viaja sin encriptar.

En la gráfica que se muestra a continuación se puede observar como los datos que viajan en un paquete de la opción del sitio cambiar contraseña viaja totalmente plana.

El usuario **proa** digita la contraseña actual la cual es **cascabel** y asigna una nueva contraseña confirmándola en la casilla siguiente, como se observa en la figura la nueva contraseña es **katrion.**

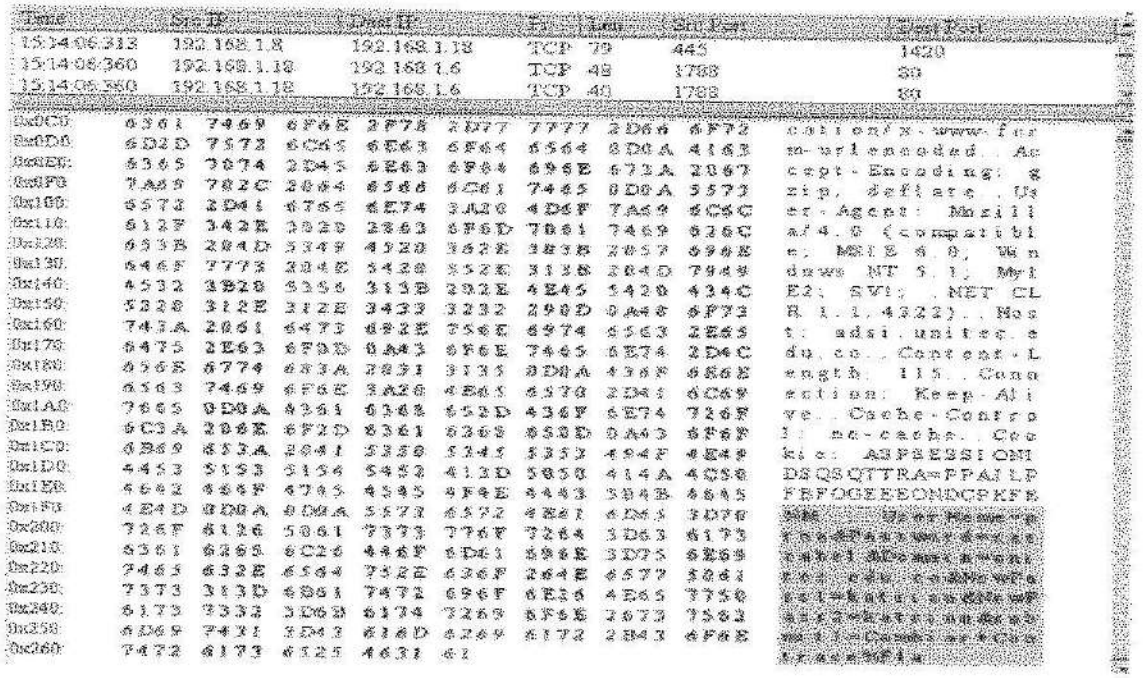


Figura No 7 Validación de usuario desde adsi.unitec.edu.co

2.3. Transferencia de Archivos - FTP

FTP es un acrónimo de File Transfer Protocol o Protocolo de Transferencia de Archivos. Este servicio es utilizado para transferir archivos entre los distintos equipos conectados en una red.

Para poder comunicarse mediante este protocolo es preciso que un PC se conecte como cliente y exista otro que haga de servidor. Esto quiere decir que nosotros mismos podemos realizar una comunicación como clientes hacia otro PC servidor, que puede estar en nuestra red o Internet. Esta operación se realiza con el fin de navegar e investigar qué es lo que tiene este PC servidor, para poder subir, bajar, borrar, escribir archivos dependiendo de los permisos que se tengan. Este servicio utiliza el puerto 20 y 21 del servidor.

Este servicio es utilizado en la red de unitec para copiar archivos a servidores o entre las terminales de trabajo.

Para poder conectarse al servidor o a la máquina que en el momento cumple el rol de servidor se necesita validarse como usuario de la red y aunque en algunos casos se puede realizar la validación de forma anónima lo que se pudo apreciar en los paquetes analizados es que la información en cualquiera de los casos viaja en forma plana.

En el gráfico que se muestra a continuación se puede visualizar la forma como viajan los paquetes:

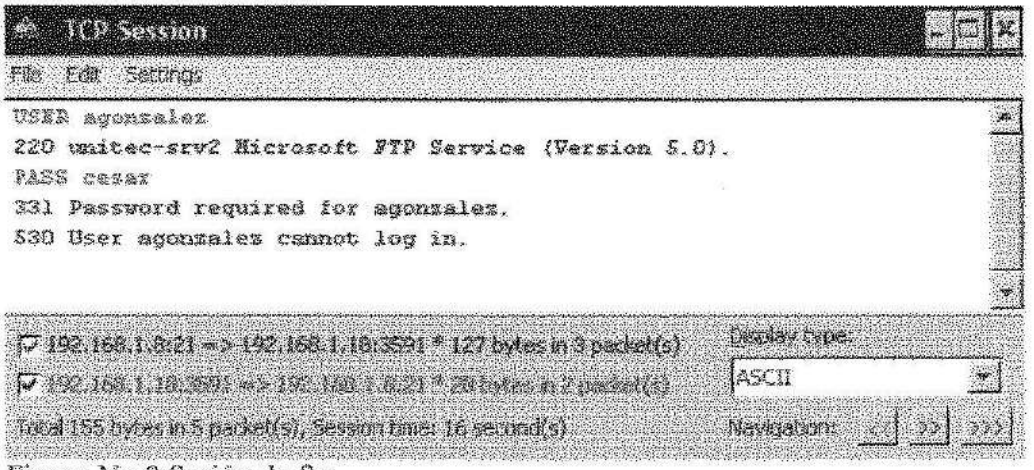


Figura No 8 Sesión de ftp

Información del paquete

Packet #1060, Direction: Pass-through, Time:10:09:41,771000, Size: 70
Ethernet II
Destination MAC: 00:04:75:B4:66:7B

Source MAC: 00:0D:56:4E:C9:F8
Ethertype: 0x0800 (2048) - IP
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Precedence: 000 - Routine
Delay: 0 - Normal delay
Throughput: 0 - Normal throughput
Reliability: 0 - Normal reliability
Total length: 0x0038 (56)
ID: 0xAD3F (44351)
Flags
Don't fragment bit: 1 - Don't fragment
More fragments bit: 0 - Last fragment
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x06 (6) - TCP
Checksum: 0xCA15 (51733) - correct
Source IP: 192.168.1.18
Destination IP: 192.168.1.8
IP Options: None
TCP
Source port: 3591
Destination port: 21
Sequence: 0x081D166A (136124010)
Acknowledgement: 0x7B6D0939 (2070743353)
Header length: 0x05 (5) - 20 bytes
Flags: PSH ACK
URG: 0
ACK: 1
PSH: 1
RST: 0
SYN: 0
FIN: 0
Window: 0xFFC9 (65481)
Checksum: 0x6395 (33685) - incorrect
Urgent Pointer: 0x0000 (0)
TCP Options: None
FTP
Command: USER
Username: agonzalez
Raw Data:
0x0000 00 04 75 B4 66 7B 00 0D-56 4E C9 F8 08 00 45 00 ..u´f{..VNÉø..E.
0x0010 00 38 AD 3F 40 00 80 06-CA 15 C0 A8 01 12 C0 A8 .8-?@.€.Ê.À¨..À¨
0x0020 01 08 0E 07 00 15 08 1D-16 6A 7B 6D 09 39 50 18 .....j{m.9P.
0x0030 FF C9 63 95 00 00 55 53-45 52 20 61 67 6F 6E 7A ÿÉc•..USER agonz
0x0040 61 6C 65 7A 0D 0A alez..

Packet #1190, Direction: Pass-through, Time:10:09:46,307000, Size: 66
Ethernet II
Destination MAC: 00:04:75:B4:66:7B
Source MAC: 00:0D:56:4E:C9:F8
Ethertype: 0x0800 (2048) - IP
IP

IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Precedence: 000 - Routine
Delay: 0 - Normal delay
Throughput: 0 - Normal throughput
Reliability: 0 - Normal reliability
Total length: 0x0034 (52)
ID: 0xAD92 (44434)
Flags
Don't fragment bit: 1 - Don't fragment
More fragments bit: 0 - Last fragment
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x06 (6) - TCP
Checksum: 0xC9C6 (51654) - correct
Source IP: 192.168.1.18
Destination IP: 192.168.1.8
IP Options: None

TCP

Source port: 3591
Destination port: 21
Sequence: 0x081D167A (136124026)
Acknowledgement: 0x7B6D095F (2070743391)
Header length: 0x05 (5) - 20 bytes
Flags: PSH ACK
URG: 0
ACK: 1
PSH: 1
RST: 0
SYN: 0
FIN: 0
Window: 0xFFA3 (65443)
Checksum: 0x8391 (33681) - incorrect
Urgent Pointer: 0x0000 (0)
TCP Options: None

FTP

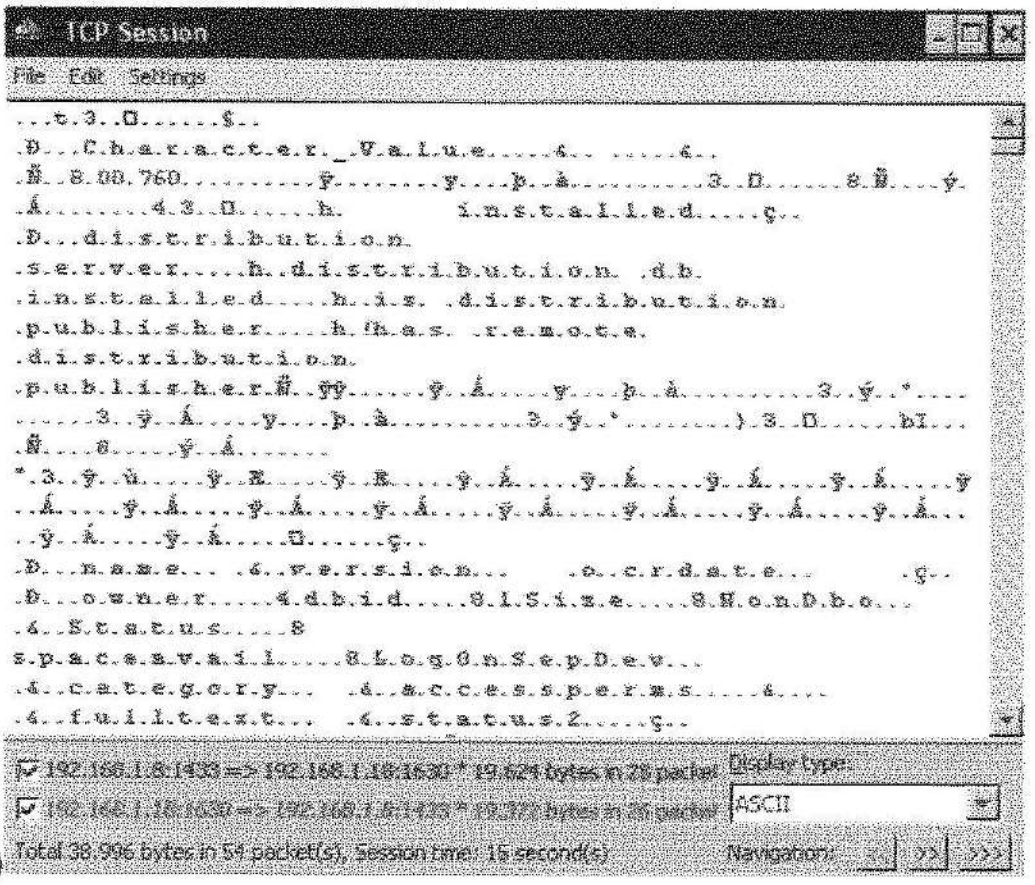
Command: PASS
Password: cesar

Raw Data:

2.4. Bases de Datos SQL

Este servicio se utiliza para acceder a la bodega de datos desde los aplicativos internos y tipo web para la gestión y ttransacción de la información académica y administrativa de la institución.
La información viaja por el puerto 1433. Este servicio envía y recibe la información encriptada.

SQL – Servicio de Base de Datos



(143)

Figura No 9 reconstrucción de sesión de sql

Raw Data:

0x04A0 61 74 69 6F 6E 2C 44 43-3D 75 6E 69 74 65 63 2C ation,DC=unitec,

```
0x04B0  44 43 3D 65 64 75 2C 44-43 3D 63 6F 3F 63 65 72  DC=edu,DC=co?cer
0x04C0  74 69 66 69 63 61 74 65-52 65 76 6F 63 61 74 69  tificateRevocati
0x04D0  6F 6E 4C 69 73 74 3F 62-61 73 65 3F 6F 62 6A 65  onList?base?obje
0x04E0  63 74 63 6C 61 73 73 3D-63 52 4C 44 69 73 74 72  ctclass=cRLDistr
0x04F0  69 62 75 74 69 6F 6E 50-6F 69 6E 74 30 5E A0 5C  ibutionPoint0^ \
0x0500  A0 5A 86 58 68 74 74 70-3A 2F 2F 75 6E 69 74 65  ZtXhttp://unite
0x0510  63 2D 73 72 76 31 2E 75-6E 69 74 65 63 2E 65 64  c-srv1.unitec.ed
0x0520  75 2E 63 6F 2F 43 65 72-74 45 6E 72 6F 6C 6C 2F  u.co/CertEnroll/
0x0530  43 6F 72 70 6F 72 61 63-69 21 30 30 66 33 6E 25  Corporaci!00f3n%
0x0540  32 30 55 6E 69 76 65 72-73 69 74 61 72 69 61 25  20Universitaria%
0x0550  32 30 55 4E 49 54 45 43-2E 63 72 6C 30 82 01 61  20UNITEC.crl0..a
0x0560  06 08 2B 06 01 05 05 07-01 01 04 82 01 53 30 82  ..+.........S0,
0x0570  01 4F 30 81 CC 06 08 2B-06 01 05 05 07 30 02 86  .O0....+.....0.†
0x0580  81 BF 6C 64 61 70 3A 2F-2F 2F 43 4E 3D 43 6F 72  ..¿ldap:///CN=Cor
0x0590  70 6F 72 61 63 69 21 30-30 66 33 6E 25 32 30 55  poraci!00f3n%20U
0x05A0  6E 69 76 65 72 73 69 74-61 72 69 61 25 32 30 55  niversitaria%20U
0x05B0  4E 49 54 45 43 2C 43 4E-3D 41 49 41 2C 43 4E 3D  NITEC,CN=AIA,CN=
0x05C0  50 75 62 6C 69 63 25 32-30 4B 65 79 25 32 30 53  Public%20Key%20S
0x05D0  65 72 76 69 63 65 73 2C-43 4E 3D 53 65 72 76 69  ervices,CN=Servi
0x05E0  63 65 73 2C 43 4E 3D 43-6F 6E                    ces,CN=Con
```

2.5 Conexión remota a Servidores

SSH: El servicio de SSH es utilizado por el administrador de red y algunas personas autorizadas para ingresar remotamente a los servidores Linux de la red de la universidad. La información viaja por el puerto 23 y se transmite de forma segura

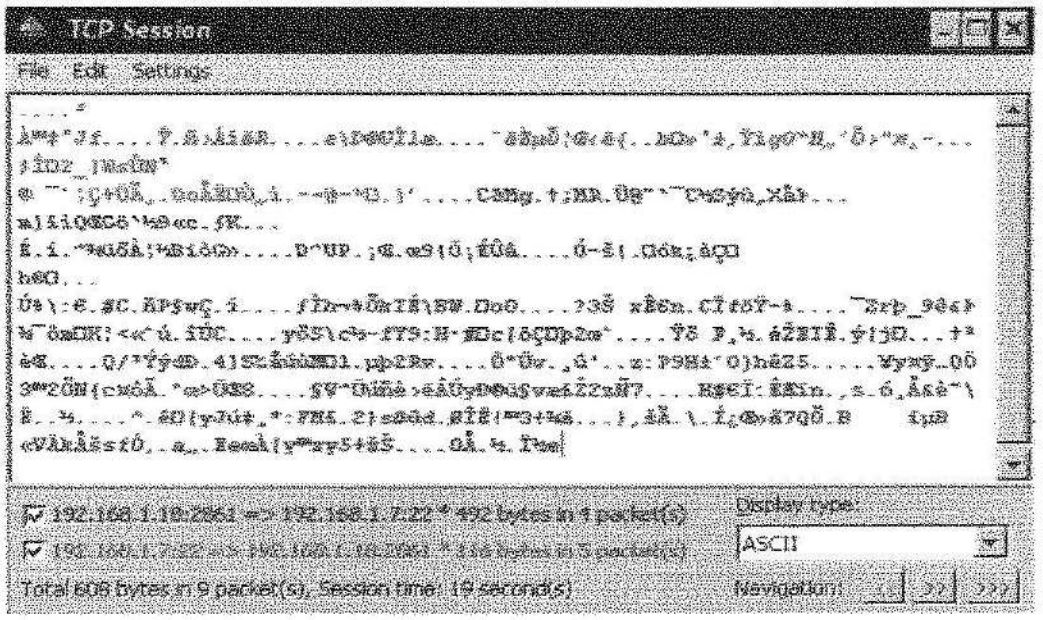


Figura No10 Proceso de encriptamiento en el servicio ssh

SSH

Identification string: SSH-1.99-OpenSSH_3.5p1

Raw Data:

```
0x0000   00 0D 56 4E C9 F8 00 E0-7D 9F 52 64 08 00 45 00   ..VNÉø.à}ŸRd..E.
0x0010   00 3F DC 3F 40 00 40 06-DB 0F C0 A8 01 07 C0 A8   .?Ü?@.@.Û.À¨..À¨
0x0020   01 12 00 16 0B 2D DF 92-A0 FA E3 4E 04 3D 50 18   .....-ß' úãN.=P.
0x0030   16 D0 35 4D 00 00 53 53-48 2D 31 2E 39 39 2D 4F   .Ð5M..SSH-1.99-O
0x0040   70 65 6E 53 53 48 5F 33-2E 35 70 31 0A           penSSH_3.5p1.
```

3. PRESENTACION DE ALTERNATIVAS DE SOLUCION

SITIOS WEB BAJO PROTOCOLO HTTP

Para los sitios WEB de la universidad alumnos.unitec.edu.co, docentes.unitec.edu.co,intranet.unitec.edu.co,adsi.unitec.edu.co y para todos aquellos sitios que requieran autenticación de usuarios se sugiere la implementacion de certificados digitales.

Las entidades que ofrecen estos certificados son las siguientes:

ABA.ECOM,INC
AOL Time Warner Inc
Addtrust AB
America Online Inc
Baltimore
Comodo CA limited
Digital Signature trust Co
Entrust.net
Equifax
Equifax Secure Inc
Gte Corporation
Geotrust inc
Globalsign Root CA
IPS Internet Publishing Services S.L
IPS Seguridad CA
RSA Data Security,Inc
Tc trustCenter for Security in data N
Thawte consulting
The User Trust Network
Unizeto sp.
Visa
Valicert.inc
Verisign,inc
betrusted

La entidad que se escogió es **Comodo** ya que es una compañía que presta servicios de Certificados digitales a un buen precio. Para contactarse con esta entidad se debe ingresar al sitio web: http://www.comodogroup.com y enviar un correo electrónico.

A continuación se explica el proceso para solicitar e implementar Certificados digitales en un sitio web

COMO VALIDAR SU SOLICITUD

Enviar un correo electrónico a DOCS@comodogroup.com solicitando la asignación de un certificado digital y informandonos sobre el nombre de dominio de su sitio web.

Cuando nosotros recibamos el correo verificamos si el nombre de dominio de la empresa que requiere el certificado esta registrado en la base de datos de la ID AUTORITY (empresa que contiene todos los dominios registrados en Internet.) si la verificación es afirmativa se le enviará a vuelta de correo el número de solicitud y el manual de instrucciones de lo contrario si no se cuenta con suficiente información de la compañía y su nombre de dominio o su aplicación no concuerda completamente con la información de el ID AUTORITY se le preguntara información adicional vía correo electrónico.

La información que se le solicitara es la siguiente

- Licencia de negocio, artículos de Asociación, o información DUNS, (dependiendo de su país o su manera que va a incorporar su certificado)
- Su derecho para usar un nombre de dominio
- Diligenciar un formulario y firmar un documento especial en el cual se verifica que la empresa tiene el derecho de usar el nombre de dominio.

Esta información será enviada por correo electrónico a DOCS@comodogroup.com ó vía fax:

- Para Estados Unidos: 1-801-409-3684
- Para Europa:+44-0870-70-66-37-8

El promedio de expedición de un certificado oscila entre media hora ó dos días.

Si ud necesita cambiar la documentación, envíe un email a SUPPORT@comodogroup.com con el numero de solicitud y la información que desea actualizar.

Después de recibir el número de solicitud y con la documentación enviada. **Comodo** enviara por correo electrónico los certificados para continuar con el proceso de instalación.

Descargue los certificados individualmente o colectivamente en un solo archivo.
Para descargar estos archivos haga clic derecho sobre el archivo y seleccione guardar como

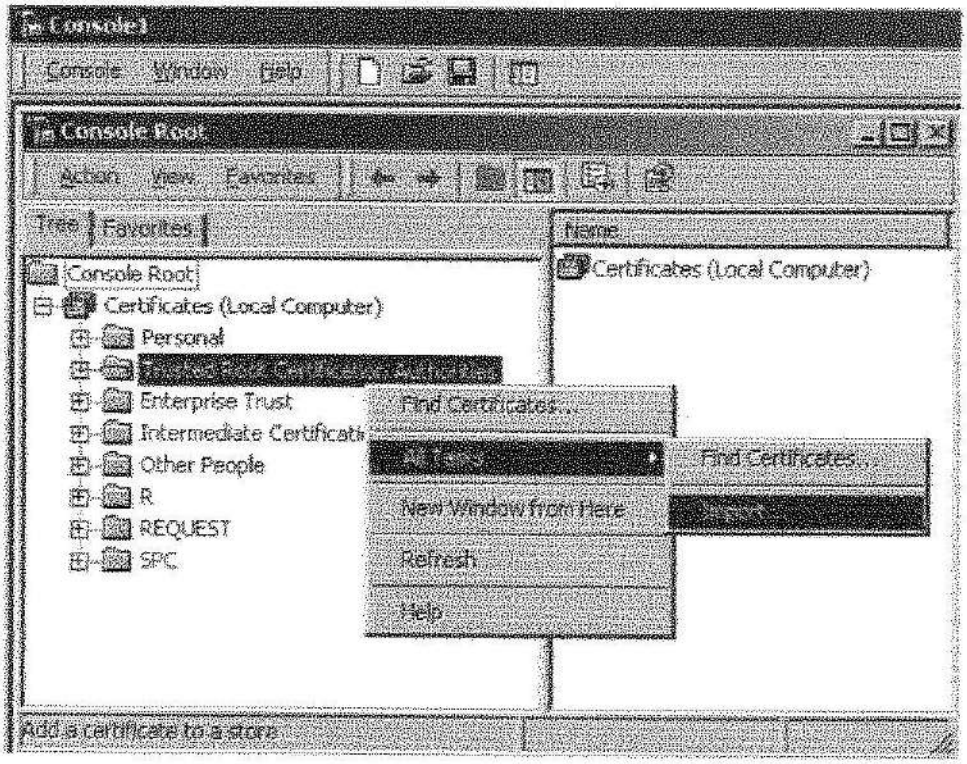
GTE CYBERTRUST GLOBAL ROOT CA.
COMODO CLASS 3 SECURITY SERVICES CA.

Recuerde que estos archivos los debe guardar en el servidor donde está configurado el sitio web.

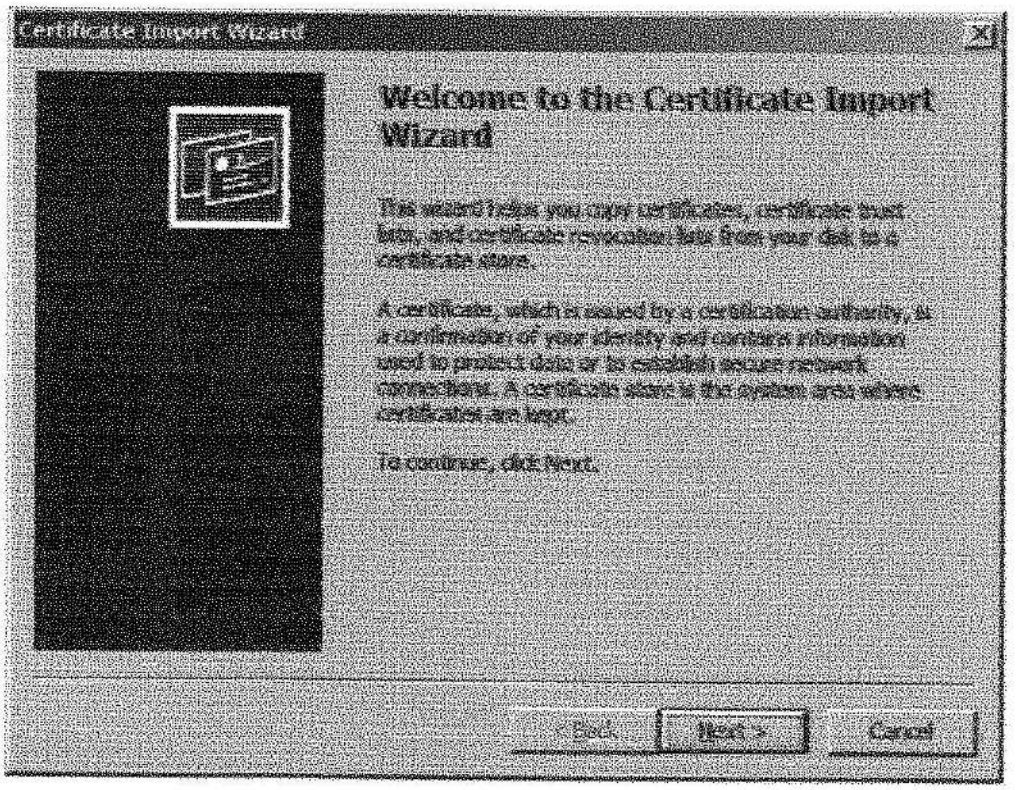
INSTALACION DE LOS CERTIFICADOS

- Haga clic en el menú inicio , luego ejecutar y escriba mmc
- Haga clic en **file** y seleccione **add/Remove snap in**
- Seleccione **certificates del add stadalone snap in** y seleccione **add**
- Seleccione **computer account** y haga clic en **finish**
- Cierre el cuadro de dialogo **add stadalone snap in**, haga clic en ok en donde diga **add/Remove snap in**
- Devuelvase al mmc

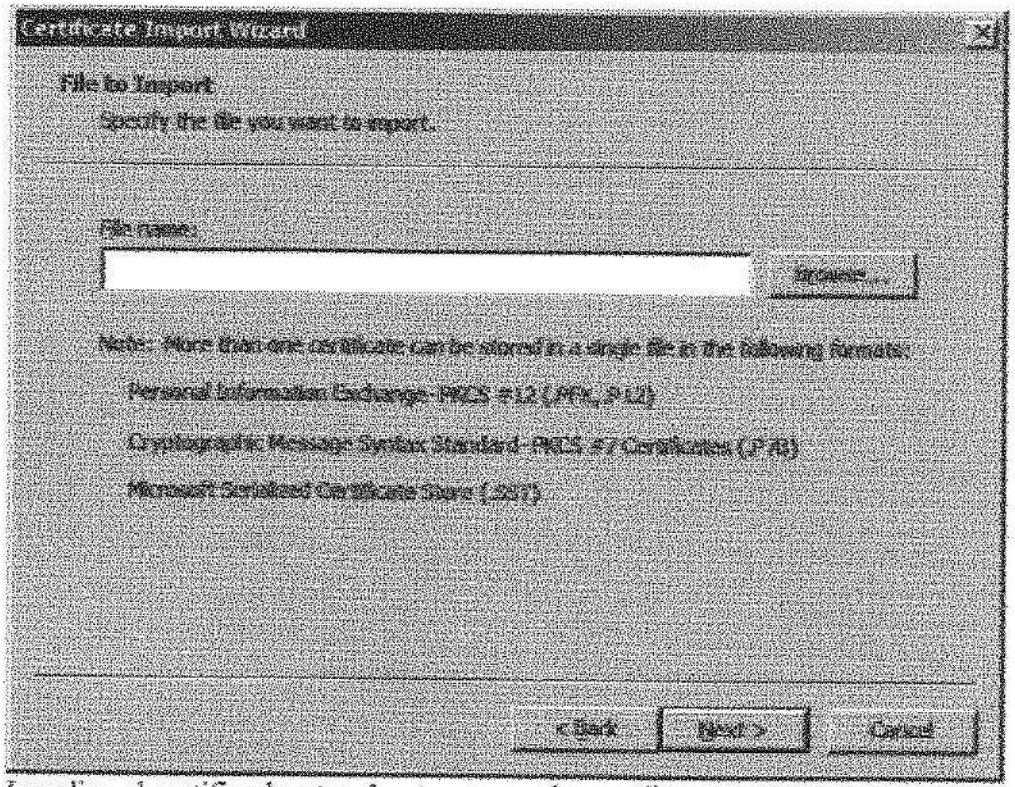
1. Instalación Certificado **GTE CYBERTRUST GLOBAL ROOT CA.**



Clic en **trusted root certification authorities** seleccione **old tasks**
Luego seleccione **import**

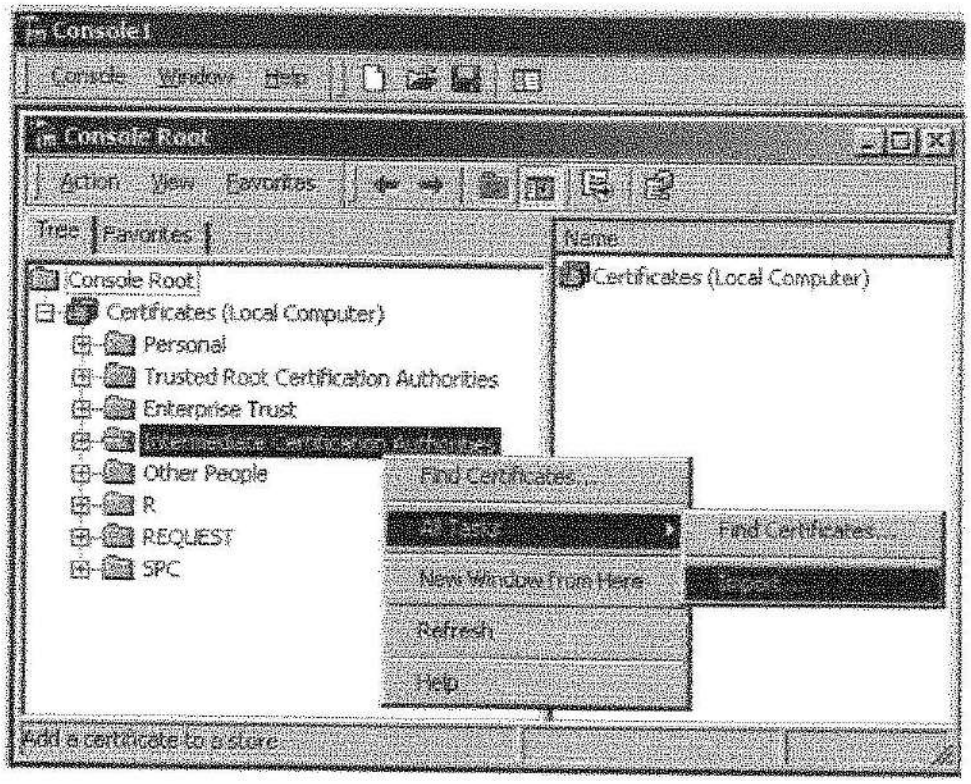

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

Clic en Next



Localice el certificado **gtecybertrust root** luego clic en **next**
Cuando el asistente haya terminado clic en **finish**

2. Instalación del certificado **COMODO CLASS 3 SECURITY SERVICES CA.**



Clic en **Intermediate Certification Authorities** , seleccione, **old tasks**
Seleccione **import**

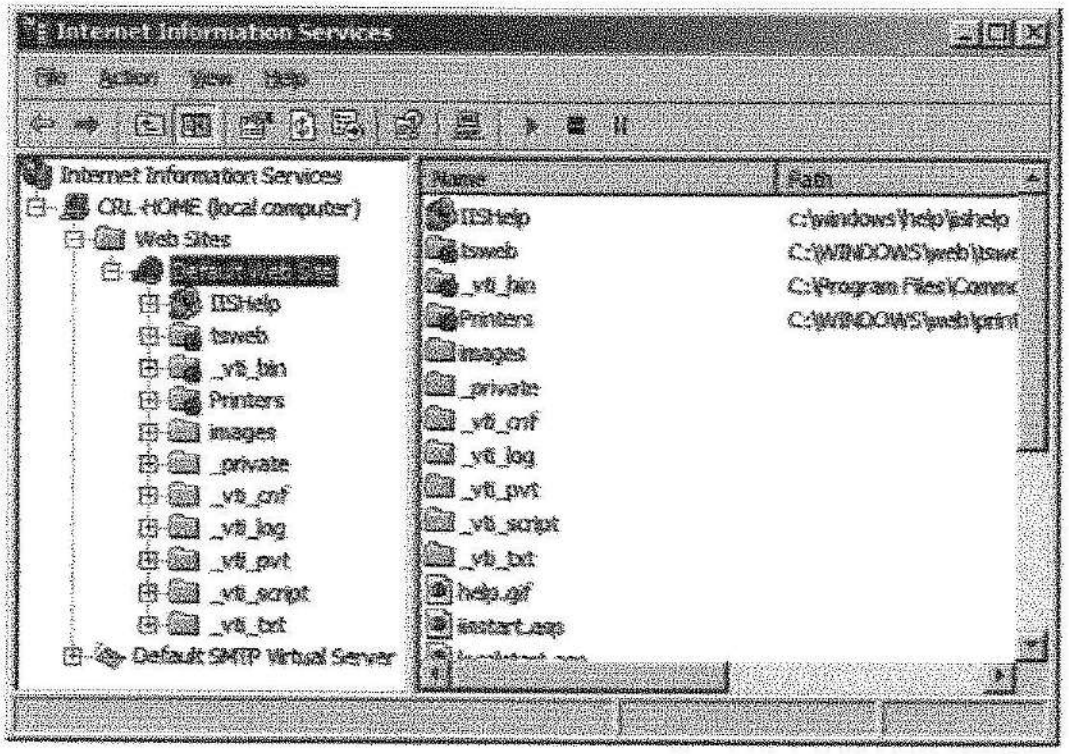
Complete el asistente de importación nuevamente, pero esta vez agregando el Certificado Comodo Class 3 Security Services CA, cuando se le pregunte por el archivo que contiene el certificado.

Compruebe que el certificado Gte Cybertrust Global Root CA aparezca bajo trusted root certification authorities

Asegurese que el certificado comodosecurityservicesca aparezca bajo
Intemediate Certification Authorities

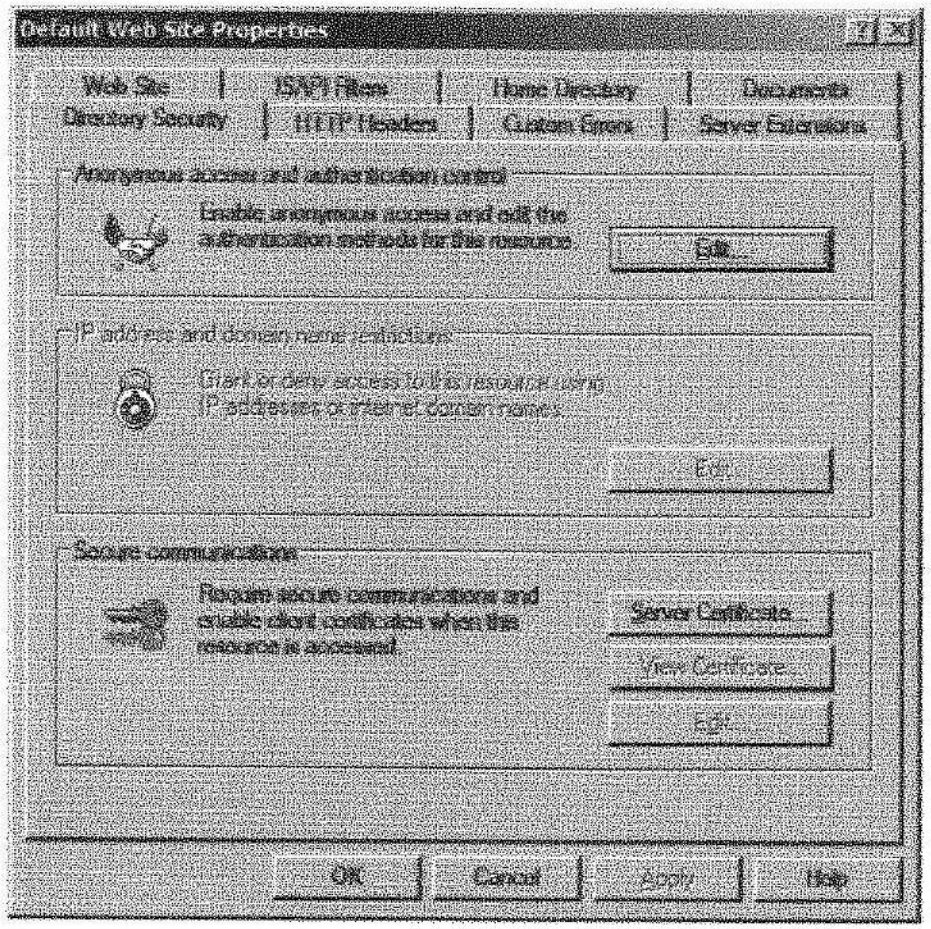
INSTALAR SUS CERTIFICADOS IIS SSL

Ingrese al Control Panel y Seleccione **Administrative Tools**
Corra el programa Internet Services Manager

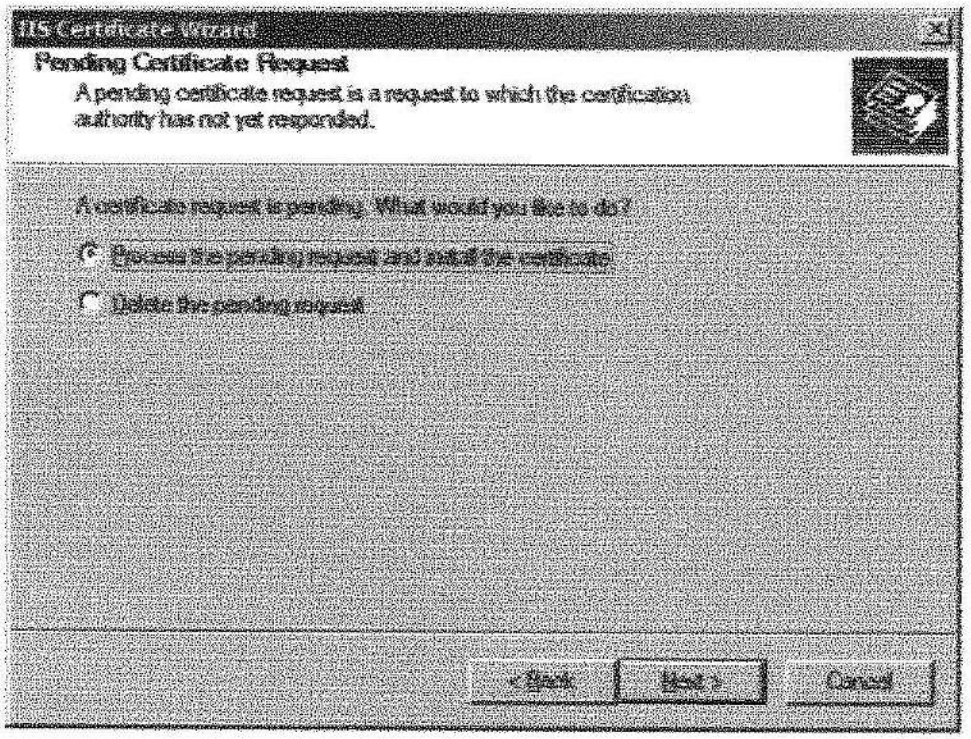


Abra el cuadro de propiedades de su web site. Ud puede hacer esto haciendo clic con el boton derecho donde dice default web site y seleccionando propiedades del menú.

Abra donde dice Directory Security haciendo clic derecho en el cuadro donde dice directory security



Haga clic en Server Certificate y aparecerá el siguiente asistente



Seleccione la opción "Process the pending request and install certificate"
Luego clic en Next

Ingrese la ruta de su certificado IIS SSL dando clic en botón Explorer
Y luego clic en Next.

Lea la pantalla de resumen para asegurarse de que ud esta procesando el
Certificado correcto y haga clic en **Next**.. Luego aparecerá una pantalla de confirmación.
Cuando haya leído esta información haga clic en **Next.**
Ahora usted tiene un certificado **IIS SSL** instalado en su sitio web.

Para finalizar el proceso de instalación reinicie la computadora.

Después que el servidor reinicie ingrese al sitio desde varios navegadores y compruebe que el sitio funcione correctamente.

EL SSL es el protocolo por el cual se van a usar el certificado o certificados que se vayan a implementar.

A continuación se describirá porque el SSL es mas seguro.

Viaja también por el protocolo SSL el cual es seguro ya que proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 se usa como algoritmo de bash.
Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

CORREO ELECTRONICO

Para el correo electrónico se sugiere dos posibles soluciones , certificado digital el cual encripta no solo nombre y contraseña de usuario sino también el contenido del mensaje y POP3S e IMAP4S los cuales realizan encriptamiento solo a nivel de autenticación

CERTIFICADOS DIGITALES POR EMAIL EN MS-OUTLOOK

Outlook 2003 utiliza el cifrado de mensajes de correo electrónico para proporcionar una comunicación más segura. Para enviar y recibir mensajes cifrados, debe obtener primero un identificador digital de una entidad emisora de certificados. El identificador digital contiene una clave privada que se almacena en el equipo del remitente y un certificado (con una clave pública). El certificado se enviará cuando firme digitalmente un mensaje para autenticar su identidad ante el destinatario. Los certificados también se utilizan para cifrar mensajes en Outlook.
Los certificados se validan mediante un sistema de jerarquía. La entidad de certificados raíz se sitúa en la parte superior de la jerarquía de certificados, ya que es la entidad emisora que ofrece más confianza. El certificado de la entidad emisora de certificados raíz está autofirmado, así que es importante que los certificados se obtengan sólo de entidades emisoras conocidas y de confianza.

https://digitalid.verisign.com/client/class1MS.htm

La entidad que emite este certificado es verisign, el identificar digital se obtiene Llenando el formulario que se expide, este se lo enviaran via email. Ver anexo I.

INSTALACIÓN DEL CERTIFICADO DIGITAL EN MICROSOFT OUTLOOK 2003

Usted recibirá un email de verisign con instrucciones para seleccionar su certificado digital.

1. Copie CTRL+C su contraseña de email
2. Siga el enlace de URL y diríjase a esa pagina
3. Pegue CTRL+V en el campo de la pagina que se abrio, esto en el paso numero 2
4. Haga clic en enviar para continuar

Nota: Usted debe usar Microsoft internet Explorer en la pagina que uno abrio en el 2 paso de tal manera que Microsoft Outook pueda identificar el certificado instalado en Internet Explorer

INSTALACION DEL CERTIFICADO DIGITAL

1. Abra Outlook 2003 y seleccione: **Herramientas-Opciones-Seguridad**
2. Haga clic en **Propiedades**
3. **Certificados y Algoritmos** hay 2 opciones. La primera opción le permite seleccionar un certificado digital para firmar los emails, la segunda opción le permite seleccionar un certificado digital para encriptar los emails
4. Haga clic en **seleccionar** y seleccione su certificado digital
5. Haga clic en **Aceptar**

ENVIO DE MENSAJES FIRMADOS

1. Abra un nuevo mensaje
2. En el menú **ver** haga clic en **opciones**
3. Haga clic en **propiedades de seguridad**

4. Haga clic en el cuadro de dialogo., **agregar un certificado digital al mensaje saliente,** y luego haga clic en **cerrar.**
5. Envie el mensaje

COMO ENVIAR UN MENSAJE ENCRIPTADO

Para enviarle a alguien un mensaje encriptado, ud necesita una copia del certificado digital de esa persona.Cuando ud recibe un mensaje firmado de esa persona siga estos pasos.

1. Abra el mensaje digital firmado
2. En el campo que se llama **de**, Haga clic en el menú **agregar a contactos**
3. Si usted tiene una entrada de esa persona dentro de la lista de contactos, haga clic en **actualizar esta dirección.** El certificado digital es guardado en la entrada de esta persona dentro de la lista de contactos. Usted ahora puede enviarle emails encriptados a esta persona.
4. Abra un **nuevo** mensaje
5. En el menú **ver** haga clic en **opciones**
6. Haga clic para seleccionar la opción **encriptar el contenido del mensaje y** sus **archivos anexos,** luego haga clic en **cerrar.**
7. Envie el mensaje

POP3S , IMAPS EN LINUX

A continuación se explicará la forma de configurar protocolos de correo seguros en un servidor Linux

Vaya al directorio /etc/xinetd.d

En este directorio debe tener los archivos POP3S e IMAPS las cuales son las versiones seguras de POP3 e IMAP. Si no los tiene en este directorio instale el paquete que los trae, este paquete se llama

imap-2000.1a-18

Este paquete lo encuentra en los CD's de instalación del Red Hat 9.0 ó en la sección de descargas del sitio oficial de Red Hat la cual es:

https://www.redhat.com/apps/download/

Activar POP3S

Para activar POP3S, edite el archivo encontrado **pop3s** en el directorio mencionado anteriormente y cambie la linea disable a NO la cual aparece por defecto deshabilitada

A continuación se muestra el contenido de l archivo :

```
# default: off
# description: The POP3S service allows remote users to access their mail \
#              using an POP3 client with SSL support such as fetchmail.
service pop3s
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/ipop3d
        log_on_success  += HOST DURATION
        log_on_failure  += HOST
        disable                 = no
}
```

Activar IMAPS

Se realiza el procedimiento anterior con el archivo **imaps** el cual se encuentra en el mismo directorio.

```
# default: off
# description: The IMAPS service allows remote users to access their mail \
#              using an IMAP client with SSL support such as Netscape \
#              Communicator or fetchmail.
service imaps
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/imapd
        log_on_success  += HOST DURATION
        log_on_failure  += HOST
        disable                 = no
}
```

Después de realizar las modificaciones reinicie el servicio teniendo en cuenta que todos los archivos que esta dentro del directorio /etc/xinetd.d dependen del demonio XINETD por lo tanto este debe ser el demonio que se debe reiniciar y se hace de la siguiente forma :

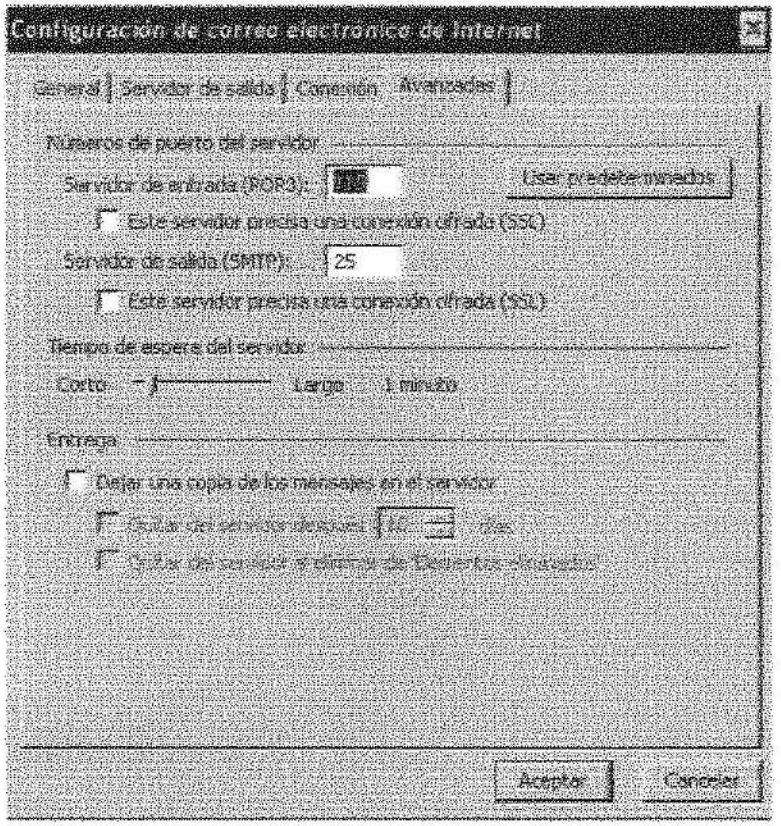
#> /etc/init.d/xinetd restart

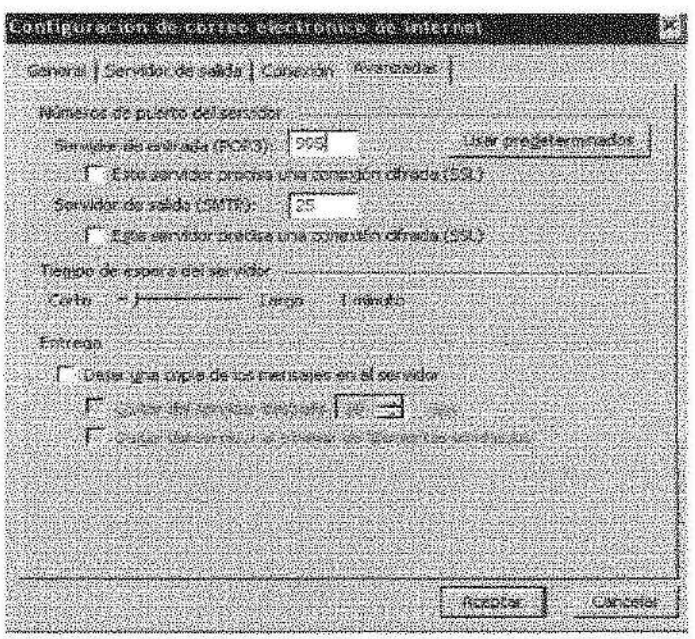
Verifique que el servicio esté corriendo correctamente.

Después de configurar y activar el servicio de POP3S e IMAPS en el servidor el paso a seguir es configurar los clientes de correo (Microsoft Outlook) los cuales están utilizando actualmente las versiones no seguras de los agentes de correo.

Antes de configurar los clientes consulte la información de los puertos que atienden los servicios de POP3S e IMAPS del archivo services el cual se encuentra en /etc/services . Con esta información ingrese a los clientes de correo y cambie la configuración de pop3 por pop3s atendiendo por el puerto 995 y los que descargan por imap por imaps atendiendo por el puerto 993

Ver la configuración en la grafica:


Configuración de correo electrónico de Internet
General
Servidor de salida
Conexión
Avanzadas
Números de puerto del servidor
Servidor de entrada (POP3):
Usar predeterminados
Este servidor precisa una conexión cifrada (SSL)
Servidor de salida (SMTP):
25
Este servidor precisa una conexión cifrada (SSL)
Tiempo de espera del servidor
Corto
Largo
1 minuto
Entrega
Dejar una copia de los mensajes en el servidor
Aceptar
Cancelar


Configuración de correo electrónico de Internet
General
Servidor de salida
Conexión
Avanzadas
Números de puerto del servidor
Servidor de entrada (POP3):
Usar predeterminados
Este servidor precisa una conexión cifrada (SSL)
Servidor de salida (SMTP):
25
Este servidor precisa una conexión cifrada (SSL)
Tiempo de espera del servidor
Corto
Largo
1 minuto
Entrega
Dejar una copia de los mensajes en el servidor
Aceptar
Cancelar

FTPS EN LINUX

SFTP

La transferencia de archivos se utiliza para enviar archivos de un cliente a un servidor en el caso de la universidad es utilizado para copiar los archivos de los sitios web de la maquina donde se desarrollan las aplicaciones al servidor donde se publican los sitios.

Según la estructura de la universidad los sitios web están publicados en el servidor Linux y en un servidor Windows 2000.

Configuración del servicio SFTP para transferir archivos al servidor Linux

SFTP puede ser usada para abrir una sesión segura interactiva de FTP.

Es similar a ftp excepto que ésta utiliza una conexión encriptada segura.

Esta utilidad esta disponible desde la versión 2.5.0p1 de Open SSH.

Como la versión que tiene el servidor de Linux de la red de Unitec es openssh-3.5p1-6 la utilidad FTPS ya viene incluida lo único que se debe hacer en los clientes es utilizar un software de Transferencia de archivos que maneje el protocolo seguro.

Como las terminales de trabajo que utilizan la transferencia de archivos hacia el servidor LINUX están sobre plataforma Windows se recomienda instalar el software FILLEZILLA el cual tiene licencia GPL la cual no tendrá ningún costo para la institución.

El software se puede descargar en la siguiente dirección:

http://sourceforge.net/projects/filezilla/

No es necesario configurar el software después de instalado pues funciona con la configuración que trae por default.

Para conectarse con el servidor se hace igual que con un programa FTP Por lo tanto no se profundiza explicando el proceso de comunicación y transferencia de la información.

Configuración del servicio SFTP para transferir archivos al servidor Windows

Descargar el servicio SSH para Windows este paquete se encuentra en:
http://www.openssh.com/portable.html

Después de descargar el archivo ejecute el instalador luego se ejecutan dos comandos que se encuentran dentro del archivo quickstart.txt
presente dentro del directorio /doc de la carpeta que acabo de instalar.

Para autorizar los usuarios debe ejecutar el siguiente comando :
C:\openssh\bin\> mkpasswd -l > ..\etc\passwd
C:\openssh\bin\> mkgroup -l > ..\etc\group

Por ultimo iniciamos el servicio ejecutando lo siguiente :

C:\openssh\bin\> net start opensshd

De esta forma queda configurado el servicio de SSH en el servidor para poder trabajar la transferencia segura de archivos. Para conectarse desde los clientes al servidor se puede utilizar el mismo software de FILLEZILLA

4. COSTO DE LA SOLUCION

4.1 SITIOS WEB

El costo de implementar un certificado digital para los sitios web es de:

US $ 1000 dólares por 10 SERVIDORES ó maquinas en las cuales este configurado el sitio.

US $ 10 dólares por cada maquina adicional.

Este pago se realiza via Internet y se debe tener en cuenta que para realizar esta transacción se debe contar con tarjeta de crédito y haber cumplido con los requisitos que se exige para poder adquirir el certificado.

La renovación del certificado varia según cada cliente , porque son politicas de discriminación de precios de la compañía, y el precio se le envian via email, hay una red que se especializa en conseguir el mejor precio de renovación para usted.

4.2 CORREO ELECTRONICO

A. SOLUCIÓN DE IDENTIFICACION DIGITAL

El costo de de implementar este certificado es de US $ 19.95 dólares por 1 año de suscripción la renovación de este servicio se hace via mail.

Este pago se realiza llenando el formulario, en donde la transacción se hará dando el numero de la tarjeta de crédito, este formulario saldrá si se a llenado el anterior con todos los requisitos que este exige.

Los costos de la renovación varian según lo que verisign especifique según lo que usted alla introducido en dicha pagina, el enlace es el siguiente.

https://digitalid.verisign.com/services/client/renew.htm

CONCLUSIONES

Se sugiere el uso de certificados digitales y versiones seguras de los protocolos utilizados en los servicios que ofrece la red de la Corporación Universitaria Unitec, para garantizar el encriptamiento de los datos transmitidos y ofrecerle a los usuarios confidencialidad y confiabilidad al utilizar los servicios

Gracias a la investigación que se hizo sobre la transmisión de información de los servicios se evitará a futuro problemas de captura y husmeo de datos confidenciales por parte de personas no autorizadas ó hackers.

La Universidad cuenta con la infraestructura tecnológica que garantiza el empleo de una gestión de seguridad eficiente por la presencia de buen equipamiento, medios de comunicación, servicios y personal calificado.

GLOSARIO Y SIGLAS

WEB: También llamada World Wide Web (WWW) es el conjunto de computadoras en el que se almacena la información que se encuentra en Internet.

HACKER: Un hacker (del inglés hack, recortar), también conocidos como sombreros blancos es el neologismo utilizado para referirse a un experto (ver: Gurú) en varias o algunas ramas relacionadas con la computación y telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz

ALGORITMO: Es un conjunto de reglas bien definidas para resolver un problema

SWITCHES: Son dispositivos de interconexión de redes de ordenadores/computadoras que operan en la capa 2 (nivel de enlace de datos) del modelo OSI. Estos interconectan dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), o sea pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los frames en la red.

TERMINAL: Un dispositivo que permite enviar comandos hacia un ordenador en cualquier lugar que éste se encuentre

SSL: SSL (Secure Sockets Layer) es un protocolo diseñado por la empresa Netscape Communications, que permite cifrar la conexión, incluso garantiza la autentificación. Se basa en la criptografía asimétrica y en el concepto de los certificados. La versión estandarizada por el IETF se conoce como TLS.

TELNET: Es el nombre de un protocolo (y del programa informático que implementa el cliente) que permite acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de internet, la máquina a la que se accedía debe tener un programa especial que reciba y gestione las conexiones.

SOCKET: Es una interfaz de comunicación que ofrece un mecanismo de comunicación general entre dos procesos cualquiera que pertenezcan a un mismo sistema oa dos sistemas diferentes

PASSWORD: Contraseña alfanumérica necesaria para acceder a un espacio o información restringida.

SNIFFER: programa que monitorea y analiza el tráfico de una red para detectar problemas o cuellos de botella. Su objetivo es mantener la eficiencia del tráfico de datos. Pero también puede ser usado ilegítimamente para capturar datos en una red.

ROUTER: Un router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

BIBLIOGRAFIA

Linux (2005) [En linea]Disponible en http://www.linuxparatodos.net/linux/como-sendmail-fetchmail.php

Comodo(2005)[En linea] http://www.comodogroup.com

Microsoft(2005)[En linea]http://www.microsoft.com

Entidad certificadora (2005) Disponible en http://www.verisign.es/

Criptografia (2005)[En linea] Disponible en http://www.kriptopolis.com

Ramiró, Aguirre Jorge (2003). **Curso de Seguridad Informática y Criptografía**. 3ra ed. Universidad Politécnica de Madrid España.

Seguridad en la red (2005) [En linea]Disponible en http://canalhanoi.iespana.es/informatica/seguridadhack.htm

Criptografia y seguridad en la red (2005) [En linea] http://www.iec.csic.es/criptonomicon/default2.html

ftps en Linux(2005)[En linea] Disponible en http://base.espora.org/tiki-index.php?page=FileZilla

ANEXOS

Anexo 1

Formulario de solicitud de certificado de email por verisign

https://digitalid.verisign.com/client/class1MS.htm

VeriSign™ Class 1 Digital ID℠
for Microsoft Internet Explorer
Step 1 of 4: Complete Enrollment Form

- Step 1: Complete Enrollment Form
- Step 2: Check E-mail
- Step 3: Pick up Digital ID
- Step 4: Install Digital ID

Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.

First Name: (Nickname or middle initial allowed (example – Jack B.)	
Last Name: (example – Doe)	
Your E-mail Address: (example – jbdoe@verisign.com)	

Challenge Phrase
This unique phrase protects you against unauthorized action on your Digital ID and should not be shared with anyone. Do not lose it! It is required to revoke, replace, renew or set preferences for your Digital ID.

Enter Challenge Phrase: Do not use any punctuation.	

Choose a Full-service Class 1 Digital ID, or a 60-day Trial Class 1 Digital ID

I'd like a one-year, full-service Digital ID for only US$19.95 per year.	◉
I'd like to test drive a 60-day trial Digital ID for free. Does not include revocation, replacement, renewal or coverage under the NetSure Protection Plan.	○

Billing Information

Your credit card will be charged US$19.95 when you click the Accept button below. All enrollment and credit card information is transmitted through a secure sockets layer (SSL) connection using a VeriSign Secure Server ID.

Card Type:	Visa
Card Number:	
Expiration Date:	Month Year
Name on Card:	
Street Address: If P.O. Box enter here.	
Apartment Number:	
City:	
State/Province:	

Zip/Postal Code:	
Country:	United States

(Optional): Select The Cryptographic Service

If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.

Cryptographic Service Provider Name	Microsoft Enhanced Cryptographic Provider v1.0

Additional Security for Your Private Key

We recommend that you protect the private key associated with your Digital ID. Checking the box below will provide you with security options for your private key. Click Here for additional information.

Check this Box to Protect Your Private Key	☐

Digital ID Subscriber Agreement and Privacy Policy

You must read this subscriber agreement and privacy policy extract before applying for, accepting, or using a Digital ID (certificate). If you do not agree to the terms of this subscriber agreement and privacy policy extract, do not apply for, accept, or use the Digital ID (certificate).