ESCUELA MILITAR DE INGENIERÍA
"MCAL. ANTONIO JOSÉ DE SUCRE"
INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO

"DESARROLLO DE UNA APLICACIÓN PARA ADMINISTRACIÓN DE FIRMAS Y CERTIFICADOS DIGITALES CASO: SUPERINTENDENCIA DE TELECOMUNICACIONES"

POSTULANTE: MARCELO INVERT PALMA SALAS

TUTOR: MSC. ING. GUIDO ROSALES URIONA

TUTOR COLECTIVO: MSC. LIC. FERNANDO YAÑEZ ROMERO

LA PAZ – BOLIVIA

2005

ESCUELA MILITAR DE INGENIERÍA
"MCAL. ANTONIO JOSÉ DE SUCRE"
INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO

"DESARROLLO DE UNA APLICACIÓN PARA ADMINISTRACIÓN DE FIRMAS Y CERTIFICADOS DIGITALES CASO: SUPERINTENDENCIA DE TELECOMUNICACIONES"

POSTULANTE: MARCELO INVERT PALMA SALAS

Trabajo de Grado, modalidad Proyecto de Grado, presentado como requisito para optar al título de licenciatura en Ingeniería de Sistemas.

Tutor: Msc. Ing. Guido Rosales Uriona

Tutor Col: Msc. Lic. Fernando Yañez Romero

LA PAZ – BOLIVIA
2005

DOCUMENTACIÓN ACADÉMICA

DESARROLLO DEL PROYECTO DE GRADO

DEDICATORIA

A mi Abuelo Deo, por ser la inspiración de ser mejor persona durante toda mi vida recorrida y que Dios lo tenga en su regazo, para que siga cuidando de nosotros y nosotros sigamos recordándole.

AGRADECIMIENTOS

A Dios por concederme la gracia de vivir, por darme la oportunidad de llegar a 5º año y ayudarme a levantarme de mis caídas.

A la Escuela Militar de Ingeniería por la enseñanza, la disciplina y el nivel académico impartida a lo largo de los años de estudio

Al Msc. Lic. Fernando Yañez Romero, por su constante apoyo en beneficio del desarrollo del presente trabajo.

Al My. DIM. Álvaro Ríos Oliver, por sus concejos y su apoyo los cuatro últimos años.

Al. Msc. Ing. Guido Rosales Uriona por ser un amigo y concejero en el desarrollo del presente trabajo.

A la Msc. Lic. Amparo Subiera por la confianza y su colaboración puesta en mi persona.

Al Msc. Lic. Jesús Rocha por apoyarme cuando más lo necesitaba durante los cuatro años.

Al Msc. Ing. Freddy Mercado por haberme llevada a una Institución tan prestigiosa como la Superintendencia de Telecomunicaciones

Y a todos aquellos que me ayudaron aunque sea con un granito de Arena
Gracias…

INDICE DE CONTENIDO

CAPÍTULO 4

FACTIBLIDAD DEL PROYECTO

CAPÍTULO 5

INGENIERÍA DEL PROYECTO

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La Superintendencia de Telecomunicaciones (SITTEL) tiene la potestad otorgada por el gobierno para administrar las telecomunicaciones en Bolivia desde 1995, entre sus principales Departamentos se encuentra el Dep. de Tecnologías de Información y Comunicación (TIC), quien es nuestro objeto de estudio en el presente trabajo.

El Departamento de TIC surgió de la necesidad de administrar las tecnologías que apoyan el intercambio de información entre los diferentes usuarios internos e instituciones externas relacionadas con SITTEL, desde su creación como departamento de Sistemas fue adquiriendo nuevas tareas en pro de la Sociedad de la Información Boliviana.

Coadyuvado por la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) desde el 2002, el Dep. de TIC de SITTEL participa en proyecto que proponen políticas, implementan estrategias y coordinan acciones tendientes a lograr un uso y aprovechamiento óptimos de las Tecnologías de Información y Comunicación en contextos como la Estrategia Boliviana de Reducción de la Pobreza, los planes y acciones nacionales y/o regionales de desarrollo o estrategias consultivas como el Diálogo Nacional.

Para el logro de estos propósitos, resulta de gran utilidad proteger la información que genera SITTEL, a través de herramientas de tecnológicas que brinden seguridad en las intercomunicaciones internas y externas.

El contenido del presente proyecto de grado realiza un análisis de seguridad al Dep. de TIC de SITTEL orientado hacia el uso de herramientas de control criptográfico para incrementar el nivel de seguridad de la información frente al uso de herramientas convencional como Firewall y productos de seguridad Microsoft que están orientados hacia la protección de la información externa de la institución gubernamental.

Al respecto las organizaciones mundiales en seguridad como la Asociación de Internautas (AI), International Communication Union (ITU), International Standard Association (ISO)

determinaron que más de la mitad de los ataques informáticos son realizados dentro de las empresas y organizaciones (robo de paquetes de información para ser vendida a la competencia, violación de la seguridad física y lógica, fraude a los sistemas, entre otros).

Las Normativas Internacionales y los Sistemas de Gestión de Seguridad de la Información (SGSI) desarrollados por la Norma Boliviana ISO/IEC 17799 hacen hincapié en el uso de herramientas criptográficas que coadyuvan al control por riesgos internos en la seguridad de la información en la empresas y organizaciones anteriormente mencionados, evitando que los mismos se materialicen en amenazas que pongan en riesgo la continuidad del negocio.

Los controles criptográficos son herramientas que aseguran la **integridad** (salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento), **disponibilidad** (garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera) y **autentificación de la información** (garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella), los cuales son conceptos son la base de la Norma Boliviana ISO/IEC 17799 para los Sistemas de Gestión de Seguridad que fueron implantados en SITTEL a través de un Sistema de Administración de Firmas y Certificados Digitales.

Capítulo 1
Generalidades

"La formulación de un problema es

Más importante que su solución"

Albert Einstein

1.1. Introducción

A lo largo de la historia el ser humano ha desarrollado sistemas de seguridad que le permitían comprobar la identidad del interlocutor en una comunicación (por ejemplo tarjetas de identificación y firmas manuscritas).

Con el fin de asegurar la información del destinatario seleccionado se utilizo correo certificado y para evitar su modificación se utilizó mensajes notariados[1], pero el envió y recepción de información por las redes de computadoras bajo medios de comunicación inseguros y no supervisados generaron un problema de seguridad en las tecnología de intercomunicación en la actualidad (el empresario moderno busca siempre estar comunicado, a él le interesa tener una comunicación segura, como se observa en la figura 1.1).

Figura 1.1: La seguridad en la Transferencia de la Información

Fuente: Microsoft Corporation

En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad.

En contraste las actividades ofimáticas como el intercambio de información se están trasladando al mundo electrónico a través de Internet, los programas de seguridad de la información son importantes para las organizaciones que quieren progresar y crecer en un mundo en línea cada vez más peligroso.

El crecimiento de los medios de comunicación trajo consigo el incrementando de medios de intercepción de información por Sniffer y Hackers por cable, inalámbrica y satélites creando inseguridad en la transferencia de la información (ver la Figura 1.2).

[1] Mensaje Notariado: Correo enviado con firmas en el registro del sobre o carta y reenvió de la copia al firmada al remitente.

Las noticias suelen referirse a la inseguridad de la información como ataques que sufren los administradores cuando sus servidores han sido allanados, se modifico la información de su página Web como ser el portal, se infiltraron a su Base de Datos, extrajeron información confidencial, etc.

Figura 1.2: Sistemas de Comunicación por Satélite

Fuente: Conferencia Internacional “Echelon y los Sistemas de Espionaje Global Electrónico”

Aunque estos ataques pueden parecer dramáticos, los intrusos reales no suelen anunciar su presencia ni hacen alarde de lo que consiguen, sino que instalan dispositivos ocultos de monitoreo que furtivamente recogen información de la red.

Detallando algunas de las intrusiones típicas que ocurren dentro de nuestras redes informáticas tenemos:

- Un intruso monitorea el tráfico de un medio de comunicación y recoge la información confidencial que genera un usuario, el intruso podría leer el número, la fecha de caducidad y el nombre del titular de una tarjeta de crédito. Y, a continuación, utiliza esta información para realizar pedidos a través de Internet.
- Un Hacker podría ingresar a la base de datos de un sistema bancario y cambiar el balance de una cuenta, transfiriendo fondos a otra.
- Un empleado externo, conociendo la infraestructura de la empresa podría capturar la información de una transferencia que pasa por algún medio de comunicación y alterar la instrucción de un cliente.
- Un ex empleado, envía un programa al servidor web de la compañía, monopolizando el tiempo del procesador del sistema, pasando gradualmente de servidor a servidor hasta que el sistema queda inutilizado. Esta es una forma de ataque conocido como denegación de servicio (DoS).

La mejor solución ante todos estos ataques es prevenir estableciendo políticas de seguridad de la información mediante la implementación de técnicas de autenticidad de usuarios e integridad de la información, auditoria de sistemas en periodos no mayores a un año, implantación de normas de seguridad, etc.

Se necesita documentos digitales que ofrezcan las mismas funcionalidades que los documentos físicos con el plus de ofrecer garantías aún sin presencia física

¿Cómo se resuelve el problema? Gracias a mecanismo criptográficos siendo los elementos fundamentales el certificado digital y la firma digital.

El propósito del trabajo de grado es desarrollar una herramienta que genere certificados digitales con su correspondiente llave pública y privada, integrándose a las firmas digitales para el envió de documentos seguros por la Web, asegurando la integridad del documento y mediante el certificado se podrá determinar a quien pertenece las firmas digitales.

Lo novedoso del trabajo es el desarrollo de un software que sea tan robusto como el que ofrece la empresa VeriSign y la integración de dos herramientas como son los certificados digitales y las firmas digitales.

1.2. Antecedentes

La creación de la *firma manuscrita* (como se observa en la figura 1.3) buscaba medios de autentificación para el envió de su información además de ser utilizada en la identificación de documentos personales, por esta razón se le dio un sustento jurídico en el código civil para poseer un valor material [2].

Figura 1.3: Firma Manuscrita

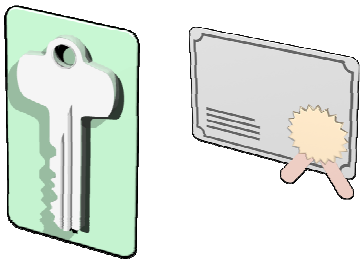
Fuente: Microsoft Company

[2] Código Civil en Bolivia.

Los inicios de los *certificados* tal como lo conocemos existen a partir de creación de la *firmas manuscrita*, utilizados como instrumentos (documento, diploma, cedula, personaría jurídica) que afirma la veracidad de un hecho, el cual puede ser la obtención de un bien material, un diploma académico, contratos de trabajo, etc.

El origen de la firma y certificado digital empezó con la creación de la criptografía de clave pública que fue introducido por James Ellis[3] el año de 1969 al tratar de vislumbrar el concepto de criptografía asimétrica. En 1973 el matemático Clifford Cocks plantea la posibilidad de utilizar números primos y la factorización como base del sistema, un año más tarde comentó sus avances a Malcom Williamsom (que acababa de incorporarse al GCHQ[4] como criptógrafo). Para 1975 James Ellis, Clifford Cocks y Malcolm Williamson habían descubierto todos los aspectos fundamentales de la criptografía de clave pública incluyendo las técnicas RSA y Diffie-Hellman con algoritmos computacionales. Mientras Whitfield Diffie y Martin Hellman en el año de 1975 a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro, logran redescubrir la Criptografía Asimétrica, el cual fue el principio de las firmas digitales. Este sistema utilizaba dos claves diferentes: una para cifrar y otra para descifrar. En 1978 aparece el algoritmo de criptografía más utilizado y extendido en el mundo, conocido como RSA[5] (ver figura 1.4).

Figura 1.4: Llave Pública y Certificado Digital



Fuente: Microsoft Company

El Internet nos ofrece beneficios en transferencia de información a altas velocidades, razón por la cual se empezó a digitalizar la información desde la aparición de la computadora y para 1996 se empezó a hablar de la creación de la Nueva Sociedad de la Información por el uso masivo del Internet, los mencionados mecanismos empezaron a tener problemas con el

[3] Criptógrafo gubernamental del Reino Unido
[4] GCHQ: Government Communications Headquarters – Oficina General de Comunicaciones Gubernamentales del Reino Unido, se formo con los restos del Bletchley Park después de la II Guerra Mundial.
[5] RSA: Criptosistema de llave pública, su nombre proviene de sus tres inventores: Ronald **R**ivest, Adi **S**hamir y Leonard **A**dleman.

tiempo de envió y recepción de la información de un punto a otro respecto a la velocidad del Internet, como también el creciente número de mensajes interceptados y modificados.

Para 1993 se introdujo el concepto de certificados digitales con el fin de entregar a máquinas y a usuarios medios de autentificación a través del Internet y otras redes de comunicación.

Las firmas digitales fueron creadas en 1997 con el objetivo de suministrar al mercado productos eficientes en lo referente a algoritmos criptográficos fuertes[6] generados a partir del concepto de firmas holográficas.

Gracias a la firma y certificado digital, gobiernos y entidades financieras ofrecen servicios de transacciones en línea de información, abriéndose la posibilidad de obtener documentos como la cédula de identidad, carnet de conducir, pasaporte, certificados de nacimiento, o votar en los próximos comicios desde la comodidad su computadora y trajo consigo la creación de empresas que se ocupan de la investigación y desarrollo de productos de seguridad informática como VeriSign[7] (ver la figura 1.5), Entrust, RSA Security, Thawte las cuales desarrollan certificados y firmas digitales bajo distintas técnicas de encriptación (RSA, MD5, SHA, ElGamal, Rabin, PGP, etc.) y soportan las principales plataformas tecnológicas (Windows, Unix, Linux).

Figura 1.5: Logotipo de VeriSign

Fuente: www.verisign.com

VeriSign es la empresa más difundida en el ámbito global, tiene servicios de infraestructura inteligente que permiten a las personas y compañías conocerse, conectarse y reforzar la

[6] Método Desarrollado por RSA.
[7] www.verisign.com

seguridad de las transacciones comerciales que se realizan en las redes globales. Se hace posible unas 14.000 millones de interacciones en Internet, 3.000 millones de interacciones telefónicas y favorece un volumen de comercio electrónico por valor de 100 millones de dólares [Verisign, ©2005].

En la tabla 1.1 se presenta los costos de las firmas digitales obtenidos en la página de VeriSign[8].

Tabla 1.1: Lista de Precios de Firmas Digitales

Tipos	Cantidad	Precio por Unidad (U$S)
Firma Digital (VeriSign) 1 año	1-10	35.00
Firma Digital (VeriSign) 1 año	11-35	20.00
Firma Digital (VeriSign) 1 año	35-más	10.50

Fuente: elaboración propia

Mientras que los costos para certificados digitales se observa en la tabla 1.2:

Tabla 1.2: Lista de Costos de emisión de Certificados Digitales de VeriSign

Tipos	Nivel de cifrado	Precio (US$)
Alta Certificado Global (VeriSign) 1 año	128 bits	840,00
Renovación Certificado Global (VeriSign) 1 año	128 bits	840,00
Alta Certificado Global (VeriSign) 2 años	128 bits	1650,00
Renovación Certificado Global (VeriSign) 2 años	128 bits	1650,00
Alta Certificado Internacional (VeriSign) 1 año	40 bits	470,00
Renovación Certificado Internacional (VeriSign) 1 año	40 bits	370,00
Alta Certificado Internacional (VeriSign) 2 años	40 bits	840,00
Renovación Certificado Internacional (VeriSign) 2 años	40 bits	730,00

Fuente elaboración propia

En cambio empresas como Thawte, desarrollan productos similares con precios menores, además que no utilizan los mismos criptosistemas para la protección de la información (comparar las tablas 1.1, 1.2 de Verisign con la tabla 1.3 de Thawte, ambas empresas desarrollan firmas y certificados digitales).

[8] Costos relativos a la cantidad de firmas digitales necesarias por empresas o instituciones para España y Estados Unidos.

Tabla 1.3: Lista de Costos de emisión de Certificados Digitales de Thawte

Tipos	Nivel de cifrado	Precio (US$)
Alta Certificado SGC SuperCert (Thawte) 1 año	128 bits	470,00
Renovación Certificado SGC SuperCert (Thawte) 1 año	128 bits	420,00
Alta Certificado SGC SuperCert (Thawte) 2 años	128 bits	890,00
Renovación Certificado SGC SuperCert (Thawte) 2 años	128 bits	790,00
Alta Certificado SSL Web Server (Thawte) 1 año	40/56/128 bits	210,00
Renovación Certificado SSL Web Server (Thawte) 1 año	40/56/128 bits	170,00
Alta Certificado SSL Web Server (Thawte) 2 años	40/56/128 bits	480,00
Renovación Certificado SSL Web Server (Thawte) 2 años	40/56/128 bits	320,00
Alta Certificado SSL123 (Thawte) 1 año	40/56/128 bits	170,00
Renovación Certificado SSL123 (Thawte) 1 año	40/56/128 bits	170,00
Alta Certificado SSL123 (Thawte) 2 años	40/56/128 bits	320,00
Renovación Certificado SSL123 (Thawte) 2 años	40/56/128 bits	320,00

Fuente elaboración propia

El pionero en la utilización de firmas y certificados digitales en nuestro país fue el Departamento de Sistemas de **Banco Central de Bolivia**, quién en fecha 13 de diciembre de 2001 publico un estatuto que regula la utilización de dicha tecnología en las entidades financieras, a partir del estatuto el Banco Nacional de Bolivia para el 2004 pública una Resolución de Directorio[9] el cual reglamenta su utilización para sistemas de pago y la utilización de certificados digitales [BNB, ©2005].

La mencionada resolución es aprobada el 11 de noviembre de 2004, convirtiéndose en la primera entidad financiera pública que permite a sus clientes hacer uso de firmas y certificados digitales para pagos de alto valor.

Con el fin de reglamentar la utilización de firmas y certificados digitales en Bolivia, se empezó a elaborar un anteproyecto de ley el 2003 realizado por el e-Tic[10] junto con las empresas que lo conforman el proyecto de la Sociedad de la Información Boliviana (ADSIB, SITTEL y PNUD), en junio de 2004 se termina el anteproyecto de ley denominado “Ley de

[9] Resolución de Directorio Nº 086/2004 - Reglamento de Firma Digital Para el Sistema de Pagos. www.bnb.com.bo
[10] Sociedad de empresas públicas en Tecnología de la Información y Comunicación – www.bolnet.bo

Comunicación Electrónica de Datos, Contratación Electrónica y Firmas Electrónicas", al momento se encuentra en la etapa de revisión.

Sobre los proyectos realizados en áreas afines al trabajo tenemos:

- "Emisión de Certificados de Nacimiento On-Line en la ciudad de La Paz con Tecnología VPN" realizado por el Ing. Flores. Se enfoca hacia la conexión de la Oficina de Registro Civil y la Corte Nacional Electoral por VPN para obtener certificados de nacimiento digitales, habla de protocolos seguros de comunicación. Se diferencia por nivel de importancia que a la transferencia segura de información, evitando su modificación en el camino y brindando una autentificación al registro en la base de datos. [FLORES GUILLEN, ©2000]

- "Encriptador de Texto aplicando Autómatas Celulares Lineales" realizado por el Ing. Veizaga. Desarrolla un nuevo método de encriptación de texto a través de algoritmos reversibles. Igual que mi proyecto genera un Algoritmo de Resumen o Hash pero no hace hincapié en la transferencia por medios seguros. [VEIZAGA MACHICADO, ©2001]

- "Diseño de un Sistema Integrado de Seguridad y Control de Acceso Biométrico" realizado por el Ing. Loza. Utiliza huellas dactilares para el reconocimiento de "Patrones Típicos Encontrados en la Huella Digital". Haciendo énfasis en la autentificación de la persona a través de la digitalización de su Huella Dactilar. No hace el uso de herramientas de seguridad de protección de la información, metodología orientada hacia la solución a través de sistemas biométricos de autentificación. [LOZA LUNA, ©2004]

En el ámbito internacional es amplia la lista de proyectos realizados en el área de Firmas y Certificados Digitales, de los cuales destacamos los siguientes:

- Infraestructura de Llave Pública para el Estado Peruano (PKI) Framework. Diciembre del 2002.

- Certificados Digitales para Individuos CertiSur Authentication Bureau – Clase 2. [www.CertiSur.com]

- Autentificación de Firmas Digitales. Tema presentado en el curso de verano Seguridad en Redes Informáticas y de Telecomunicaciones, celebrado en la Universidad de Cantabria, Laredo agosto de 2003, por D. Juan Tena Ayuso, Universidad de Valladolid – España.

- Delimitación de Responsabilidades en Caso de Revocación de un Certificado de Firmas Electrónicas. Ponencia en la que se profundiza en este tema de revocación de certificados según el desarrollo temporal de este proceso, presentada en el I Simposio Español de Negocio Electrónico SNE'01 por Dña. Martínez Nadal y D. José Luís Ferrer Gomilla, Universidad de las Islas Baleares - España.
- Entorno de Firma Digital Confiable basado en PDA. Ponencia presentada en el I Simposio Español de Negocio Electrónico SNE'01 por Sra. Sonia Matamoros en la que se describe la realización de un entorno de firma digital que cumple con los requisitos de la legislación vigente. Con la participación de los coautores Dr. Jesús Martínez y Dr. Antonio Maña Gómez, de la Universidad de Málaga - España.
- Certificados X.509. Artículo en el que se explican los formatos de los certificados X.509 de D. Federico García Crespí, Universidad de Alicante - España.
- Tutorial de PGP. software de laboratorio corresponde a un proyecto docente de la asignatura de **Seguridad Informática** del Departamento de Lenguajes, Proyectos y Sistemas Informáticos de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid (España) que lleva por nombre **Criptolab** y contempla algoritmos de cifrado clásico o simétrico, de cifrado moderna o asimétrico, teoría de la información, aritmética modular, libros electrónicos, cuaderno de prácticas, tutoriales, protocolos, interfaces, etc. Más información sobre este proyecto y otras aplicaciones puede encontrarlas en la página Web de la asignatura Seguridad Informática.

Dentro de las empresas y organizaciones que investigan y desarrollan nuevos estándares en el área de la criptografía, seguridad de sistemas y protección de la información tenemos:

- Agencia de Protección de Datos (https://www.agpd.es/). Desarrolla políticas y normas de seguridad de sistemas y protección de la información.
- ATI - Asociación de Técnicos de Informática (http://www.ati.es/gt/seguridad/). Conformada por expertos en seguridad informática de diversas empresas y universidades españolas.
- Belt Ibérica (http://www.belt.es/). Portal de profesionales de la Seguridad Informática.
- Grupo Seguridad Internet-2 (http://seguridad.internet2.ulsa.mx/). Creado en México y con participación de universidades y organismos internacionales. Su objetivo

principal es establecer, desarrollar y recomendar los esquemas de seguridad dentro de Internet-2.

- Kriptópolis. (http://www.kriptopolis.com/). Página con reconocimiento mundial en el área de seguridad de la información y criptografía.
- CriptoRed (http://www.criptored.upm.es). Portal con información de entidades nacionales e internacionales en el área de la Criptografía, Seguridad de Sistemas y Protección de la Información. Su finalidad es unir esfuerzos en el desarrollo, establecimiento, investigación y recomendaciones en las área mencionadas, con alrededor de 500 organizaciones públicas y privadas, y 4000 especialistas en distintas áreas.

1.3. Planteamiento del Problema

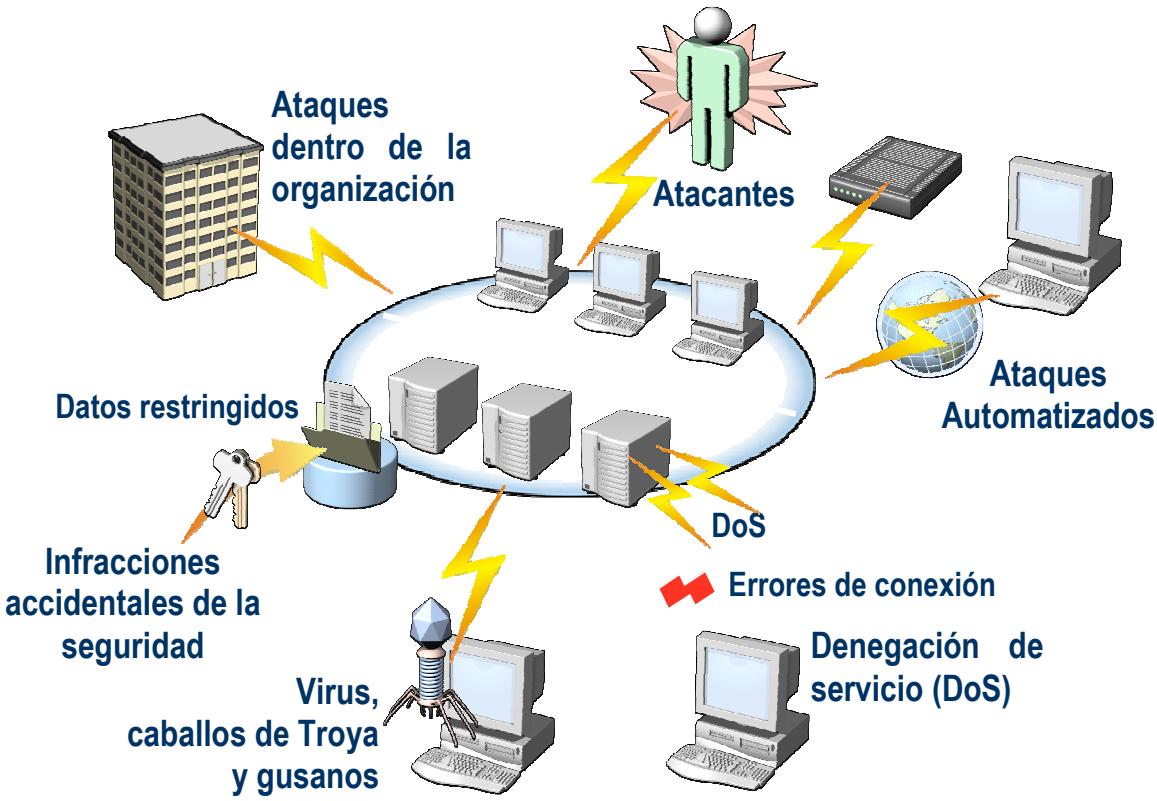
La Seguridad Informática en las Comunicaciones en nuestro país no está orientadas al aprovechamiento máximo de los recursos disponibles mediante la utilización de diversas herramientas y técnicas, SITTEL como organismo regulador de las comunicaciones en Bolivia tiene a la función de proteger y brindar privacidad en las telecomunicaciones.

El Departamento de Tecnologías de la Información y Comunicación de SITTEL esta encargado de la administración de las tecnologías de información y comunicación en la Superintendencia de Telecomunicaciones.

A continuación se presenta la lista de potenciales problemas de seguridad informática en la SITTEL (como se observa en la figura 1.6):

- Virus informáticos.
- Problemas con la integridad de documentos por la modificación de los datos en forma intencional o accidental.
- Ignorar el origen del mensaje por el receptor y repudio del mismo.
- Posibilidad de la suplantación de envió de mensajes al no existir sistemas informáticos de identificación.
- Denegación de Servicios.
- Obtención de Password y Códigos: métodos utilizados para hallar la clave que permita el ingreso a servidores, aplicaciones, cuentas, etc.
- Robo de paquetes de información por Sniffers en las empresas y organizaciones.

Figura 1. 6: Tipos de Ataques Informáticos



Fuente: 1º Foro Latinoamericano de Seguridad Informática en Tecnologías de la Información

Entre otros problemas institucionales relacionados al tema en SITTEL tenemos:

- Uno de los fines de la SITTEL es salvaguardar la seguridad en las comunicaciones electrónicas de los bolivianos, la cual no es cumplida en la actualidad por falta de herramientas que pueden controlar la seguridad de transferencia de información.
- Si el anteproyecto de ley es aprobado en el Congreso, entonces la SITTEL tendrá que ser la AC[11] y no podrá cumplir con su papel al no contar con herramientas que ayuden en la regulación del anteproyecto de Ley de Firmas y Certificados Electrónicos.

Afines a la problemática por efecto de la creación de la Sociedad de la Información tenemos:

- Inexistencia de políticas ni normas en las creaciones de AC públicas y privadas.
- Carencia de iniciativas que normen el Comercio Electrónico en Bolivia.

[11] Autoridad Certificadora

- ❖ No hay iniciativas en normar el desarrollo de herramientas de seguridad.

Una vez efectuado el análisis del listado de problemas se establece el problema central, los problemas secundarios y el árbol de problemas (Anexo A) considerando los sistemas de información, el equipamiento tecnológico, el software de desarrollo y la parte jurídica para el desarrollar software acorde a las necesidades de la SITTEL.

1.3.1. Problema Central

SITTEL cuenta con un nivel de seguridad informática susceptible a mejoras tomando en cuenta el constante incremento de riesgos en la transferencia de la información a través de medios de comunicación, además no contar con herramientas que garanticen la integridad y la autenticidad del origen del mensaje generando vulnerabilidades en la protección de la información, equipos y recursos humanos, siendo la posible causa de pérdida y modificación de la información.

1.3.2. Problemas Secundarios

a) Interceptación y modificación de la información en la red interna de la SITTEL a causa de la inexistencia de herramientas de seguridad, creando una posible pérdida de información.

b) Acceso y sustracción indebida a documentos impresos, generada por compartir impresoras en red.

c) SITTEL no cuenta con aplicaciones de administración de firmas y certificados digitales, originando problemas en la implementación de nuevas tecnologías como la infraestructura de llave pública para entidades certificantes.

d) Carencia de herramientas que garanticen la integridad de la información y la autenticidad del origen del mensaje simultáneamente.

e) Inseguridad de las Tecnologías de la Información en SITTEL, causado por inapropiados controles de seguridad frente a los nuevos peligros informáticos.

A continuación se desarrolla los objetivos que ayudan a solucionar los problemas planteados anteriormente.

1.4. Objetivos

Una vez efectuado el análisis del listado de propósitos, construido el árbol de objetivos (Anexo B), considerando los medios y fines se determina encarar los siguientes objetivos

para el presente proyecto.

1.4.1. Objetivo General

Contribuir a la seguridad de la Información en SITTEL a través del desarrollo de firmas y certificados digitales a ser evaluados por la ISO/IEC 9126[12], utilizando la NB ISO/IEC 177999 para afianzar la integridad de la información, autenticidad del origen del mensaje y tener un mayor nivel de confiabilidad que los sistemas actuales.

1.4.2. Objetivos Específicos

a) Evaluar y aplicar criptosistemas que aseguren la integridad de la información y la autenticidad del origen del mensaje mediante el desarrollo de firmas y certificados digitales para mejorara la seguridad de la información en SITTEL.

b) Evitar la pérdida de documentos físicos por la autentificación de documentos lógicos por firmas digitales.

c) Desarrollar aplicaciones de administración de firmas y certificados digitales, con el fin de poder utilizar herramientas tecnológicas adecuadas a las necesidades de SITTEL.

d) Evaluar y aplicar criptosistemas que aseguren la integridad de la información y la autenticidad del origen del mensaje mediante el desarrollo de firmas y certificados digitales.

e) Realizar una auditoria de sistemas a la SITTEL con la NB-ISO-IEC 17799 con el fin de obtener los niveles de seguridad de información actuales y después de haber implementado el software.

1.5. Hipótesis

La aplicación de firmas y certificados digitales acorde a la **NB ISO/IEC 17799** para los **procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones** permite tener un **mayor nivel de confiabilidad que los sistemas actuales** y **conserva la integridad de la información** como también **verifica la autenticidad del origen del mensaje**.

1.5.1. Variable Independiente

[12] El producto resultante será evaluado contra los parámetros indicados por el estándar ISO/IEC 9126 (funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y transportabilidad) – **Ver Anexo D**.

La aplicación de firmas y certificados digitales

1.5.2. Variable Dependiente

Mejorar el nivel de confiabilidad que los sistemas actuales, conservar la integridad de la información y verificar la autenticidad del origen del mensaje.

1.5.3. Variable Interviniente

Proceso internos de intercambio de información en la Superintendencia de Telecomunicaciones.

1.5.4. Variable Moderante

NB ISO-IEC 17799.

1.6. Justificación

1.6.1. Justificación Técnica

Se justifica técnicamente por que el desarrollo de firmas y certificados digitales son una solución a las amenazas de intercepción, modificación, interrupción y generación de nueva información. Además de brindar herramientas adecuadas a las necesidades de protección de la transferencia de información en SITTEL.

1.6.2. Justificación Científica

Se justifica científicamente por su desarrollo en entorno de software libre sobre plataforma propietaria[13] con el fin de demostrar que el producto es tan robusto como los que existen en el mercado y garantizando su efectividad a través de la norma ITU X.509 para la interconexión de sistemas abiertos sobre lenguajes de programación.

1.6.3. Justificación Económica

Se justifica económicamente porque la pérdida de información en los sistemas informáticos puede ocasionar gastos de recuperación de información que pueden ser prevenidos con software de seguridad. La pérdida de la información en la SITTEL se compararía con la pérdida de muchos años de trabajo y duplicación de esfuerzos por recuperarla o volver a generarla.

Además el costo de comprar firmas y cerificados digitales es alto, disminuiría el costo si se desarrollo en software libre y plataforma Microsoft.

[13] El software libre en el mayor de los casos siempre esta relacionado con plataforma libre (Linux)

Y habría una disminución de utilización de papel para imprimir informes de conocimiento público través de documentos electrónicos y la firma digital.

1.6.4. Justificación Institucional

Se justifica institucionalmente porque SITTEL no cuentan con herramientas de seguridad para los Sistemas de Comunicación, por tanto cumplirá con el fin de proteger la confidenciabilidad, integridad y autenticidad en las comunicaciones en Bolivia.

Además coadyuvara en los siguientes objetivos de regulación que tiene la Superintendencia de Telecomunicaciones con las empresas:

- Este medio servirá como base para futuros desarrollos de sistemas que permitan interactuar con los operadores de telecomunicaciones y usuarios, en labores de otorgación de derechos, declaraciones juradas, información estadística, e-Gob.
- Impulsará al desarrollo de la Sociedad de la Información dentro de SITTEL.

1.7. Alcances y Aportes

1.7.1. Alcances

Los alcances para la realización de este proyecto de grado se enmarcan en el aspecto temporal, espacial, institucional, económico, tecnológico y de conocimiento.

- **En lo temporal** el proyecto debe desarrollarse en siete meses para justificar el mismo ante la Superintendencia de Telecomunicaciones.
- **En lo espacial** el proyecto se desarrollara en la ciudad de La Paz, en el Departamento de Tecnologías de la Información y Comunicación en la Superintendencia de Telecomunicaciones.
- **En lo institucional** debido a que se trata de un ente regulador, la información que se maneja será restringida cuando así se lo requiera, de tal modo el proyecto se basará en una información sesgada y bajo supervisión de un encargado delegado por el Departamento de Tecnologías de Información y Comunicación de la SITTEL para coadyuvar en la realización del proyecto.
- **En lo económico** debido a que el proyecto no ha sido contemplado en el Plan Operativo Anual, el proyecto se desarrollara hasta donde lo permite esta limitante, tratándose en lo posible de utilizar tecnologías de bajo costo (en hardware) o gratuitas (software).

- **En lo tecnológico:**
  - **De los Equipos:** SITTEL brindará los equipos y herramientas necesarios para la realización de este proyecto.
  - **Plataforma Tecnológica:** SITTEL utiliza en su página web. Plataforma Microsoft, y Lotus Notes en sus correos electrónicos, por lo tanto el proyecto será realizado sobre el Sistema Operativo Windows y Lotus Notes.
  - **Lenguaje de Programación:** Al ser una plataforma Microsoft se programará en Visual Basic.Net o ASP.Net.
  - **Del Criptosistema:** Se utilizará criptosistemas libres que generan claves públicas y privadas, en lo posible las llaves serán de 128 bits.
  - **De la Firma Digital:** La firma digital podrá autentificar el origen del mensaje y proteger la información a través del hash o resumen, no brindará confidenciabilidad, pues no es el fin del proyecto, la firma digital se acoplará a documentos lógicos como Microsoft Word.
  - **De los Certificados Digitales:** Se desarrollarán **Certificados Personales**[14] en función del Estándar ITU X.509[15] (Funcionan de Similar forma que el Carnet de Identidad) el cual será emitido desde una Página Web. **No se desarrollarán:**
    - Certificados de una autoridad de certificación[16].
    - Certificaciones del servicio[17].
    - Certificaciones del editor de software[18].
- **En lo cognitivo**, el proyecto se desarrollará de acuerdo a los conocimientos, destrezas y habilidades adquiridos por el postulante a lo largo de sus estudios y

[14] Certificaciones asociadas a un individuo, funcionan como un Carnet de Identidad, contendrá información física tal como la dirección del individuo junto con la dirección relacionada con la computadora como la calve pública y la dirección de correo electrónico.

[15] Tecnología de la Información – Interconexión de Sistemas Abiertos – El Directorio: Marco de Autentificación.

[16] Es una autoridad de certificación es una organización que proporciona certificados digitales a las personas y empresas, tales como Canada Post Corporation y los servicios postales de US.

[17] Estas certificaciones contienen datos tales como la clave pública del servidor, el nombre de la organización posee el servidor y la dirección del Servicio en Internet.

[18] Estos son certificados que proporcionan confianza en que el software ha sido producido por una compañía de software específica como Microsoft.

también en los que obtendrá en el estudio de la herramienta de software que servirá para el desarrollo del presente proyecto de grado.

1.7.2. Aportes

La investigación del proyecto permitirá a la SITTEL contar con una herramienta que proteja la integridad, el no repudio del origen y la autenticidad de la información, así mismos de coadyuvar en el avance de sus proyectos dentro de la e-SITTEL disminuyendo los ataques informáticos que interrumpan, modifiquen y generen nueva información.

Así mismo, este documento presenta el diseño de un prototipo de firmas y certificados digitales como parte de su aplicación, pudiendo ser utilizada como una normativa de desarrollo de las mencionadas herramientas en la SITTEL, el cual al ser implementado coadyuvara en la seguridad de la información con los siguientes aspectos:

- Mantenimiento de la integridad del documento evitando modificaciones de los datos en forma intencional o accidental.
- Contribuye en la autenticidad del origen del mensaje, aspecto que protege al receptor del documento, garantizando que el documento ha sido generado por el emisor.
- El no repudio del origen protege al receptor del documento de la negación de haberlo enviado y de las responsabilidades que contrae el documento.
- Reduce el costo de utilizar papel para ser reemplazado por el documento electrónica y la firma digital.
- Contribuye al Desarrollo del Comercio Electrónico protegiendo a la transacción de información por Internet.
- Coadyuva al desarrollo de la Sociedad de la Información, posibilitando la utilización de la firma digital como nuevo medio de autentificación, reemplazando al Carnet de Identidad.

Capítulo 2

Marco Referencial

“El sol te marcara el horizonte de tu destino y el camino que seguirás”

Anónimo

Resumen

El presente capítulo expone los fundamentos referenciales de la Superintendencia de Telecomunicaciones, el anteproyecto de “Ley de Comunicación Electrónica de Datos, Contratación Electrónica y Firmas Electrónicas” y la Norma Boliviana ISO/IEC 17999.

2.1. Superintendencia de Telecomunicaciones

En los últimos años, una verdadera revolución ha transformado el sector de las telecomunicaciones, no sólo en Bolivia, sino en toda América Latina, razón por la cual SITTEL será el **objeto de estudio** en mi proyecto de grado.

Como una parte de la ejecución de las reformas de capitalización, los gobiernos en Latinoamérica vieron la necesidad de crear sistemas regulatorios para las empresas privatizadas, en algunos casos esta acción fue previa a la privatización y en otros emergentes de ella.

2.1.1. Antecedentes Institucionales

En Bolivia, la prestación de los servicios básicos de larga distancia estaba a cargo del sector público. Como en otros campos, el Estado estaba encargado de satisfacer la demanda, a través del operador público, extender la cobertura del servicio y ofrecer tarifas accesibles a la mayor parte de la población.

La regulación era ejercida por la Dirección General de Telecomunicaciones (DGT.), emergente de la fusión de las Direcciones de Telégrafos y de Radiocomunicaciones (D.S. 05661 del 07.09.1960).

En 1965, con la creación de la Empresa Nacional de Telecomunicaciones (ENTEL) se le asignó la responsabilidad de la prestación de servicios y quedaron reservadas las funciones de fiscalización y regulación para la DGT.

A partir de 1970, el sector de las telecomunicaciones estuvo regulado por la denominada Ley General de Telecomunicaciones (D. S. No. 09740 del 2.06.71) y por el Reglamento General de Telecomunicaciones (D. S. 17730 del 20.10.80)

Una de las críticas más frecuentes a la DGT fue que era una institución poco transparente, por lo que muchas de sus decisiones se tomaban en función a determinaciones subjetivas. El Director General de Telecomunicaciones era designado por una Resolución Ministerial, sin un período definido, consecuentemente podía ser removido en cualquier momento provocando inestabilidad institucional.

La Ley General de Telecomunicaciones, así como su Decreto Reglamentario, con la evolución de las telecomunicaciones y las nuevas tendencias de la economía mundial, se tornaron obsoletas y con grandes vacíos, sobre todo respecto a los nuevos servicios que carecían de normativa. [SITTEL, ©2000]

Con el fin estudiar las características de SITTEL, explicamos a continuación la estructura de la Industria de las Telecomunicaciones antes de la privatización.

2.1.1.1. Estructura de la Industria antes de la Privatización

Figura 2. 1: La estructura de la Industria antes de Privatización

Fuente: Elaboración Propia

Antes de las reformas existían tres empresas monopólicos (ver la Figura 2.1) para los servicios de larga distancia, local y móvil celular. La empresa monopólica estatal,ENTEL prestaba los servicios de larga distancia nacional e internacional, telex, telegrafía, satélite, telefonía rural y teléfonos públicos a las nueve ciudades bolivianas y otras ciudades.

Quince Cooperativas Privadas Telefónicas tenían el monopolio del servicio local, cada una en su localidad, y una sociedad anónima constituía el único prestador del servicio móvil celular. Contrariamente a este panorama, la radiodifusión y la televisión.

En la actualidad los roles en las telecomunicaciones han cambiado.

2.1.1.2. Estructura de la Industria después de la Privatización

Esta reforma del sector de las telecomunicaciones (como se observa en la Figura 2.2) llegó aparejada con un cambio en el tipo de Estado, produciéndose una redefinición de roles de los actores más importantes.

Figura 2. 2: Redefinición de Roles

Fuente: Elaboración Propia

El Estado, que antes concentraba las tareas normativas, reguladoras y productoras, reservo para si misma las dos primeras, encargando al Poder Ejecutivo la labor normativa y creó las superintendencias sectoriales como entes autárquicos encargados exclusivamente de la regulación. A partir de ese momento, las empresas del sector privado se constituyeron en responsables de la producción y prestación de los servicios.

Como una parte de la ejecución de estas reformas se vio la necesidad de instituir la regulación. El Sistema de Regulación Sectorial fue creado mediante Ley del Sistema de Regulación Sectorial (28.10.1994), con el objetivo de regular, controlar y supervisar aquellas actividades de los sectores de telecomunicaciones, electricidad, hidrocarburos, transportes y agua.

A fin de regular el sector de telecomunicaciones en Bolivia se fundo la Superintendencia de Telecomunicaciones. [SITTEL, ©2000]

2.1.2. Creación de SITTEL

SIRESE está compuesto por cinco agencias especializadas o superintendencias sectoriales y una Superintendencia General:

Figura 2. 3: El Sistema de Regulación Sectorial - SIRESE

Personas Jurídicas de derecho público con jurisdicción nacional y autonomía de gestión técnica, administrativa y económica

Fuente: Elaboración Propia

El modelo boliviano (como se observa en la Figura 2.3) de conformación de los entes de regulación sectorial es singular, debido a su funcionamiento como sistema que instituye una competencia virtual entre las cinco superintendencias sectoriales respecto a la eficacia y eficiencia en su desempeño, aspectos que son fiscalizados por la Superintendencia General, que emite una opinión anual al respecto.

Figura 2. 4: Logotipo de la Superintendencia de Telecomunicaciones – SITTEL

Fuente: SITTEL

La Superintendencia de Telecomunicaciones (SITTEL) inició sus actividades el 24 de noviembre de 1995 como el ente regulador de las telecomunicaciones y parte integrante del Sistema de Regulación Sectorial. (Logotipo de SITTEL en la Figura 2.4)

2.1.3. Misión de SITTEL

SITTEL tiene la misión del "ejercicio regulatorio eficiente y oportuno para el desarrollo y modernización del sector y de la democratización de las telecomunicaciones", mientras que su visión viene a ser "la institución imparcial, legítima y transparente, que lideriza y promueve el proceso de desarrollo del sector de las comunicaciones hacia la construcción de la sociedad de la información" [SITTEL, ©2000]

A continuación presentamos las tareas regulatorias de SITTEL:

2.1.4. Tareas Regulatorias de SITTEL

Las principales tareas regulatorias de SITTEL son:

- Promoción de la competencia
- Otorgación de derechos
- Supervisión de los servicios
- Aprobación de tarifas y tasas contables
- Atención de reclamos y controversias
- Aplicación de sanciones
- Proposición de normas y reglamentos
- Control del espectro electromagnético
- Establecimiento de estándares técnicos
- Colección y difusión de información
- Elaboración de estándares y planes técnicos fundamentales
- Disposición del uso de normas contables[SITTEL, ©2002]

Las tareas regulatorias de SITTEL están basadas en su regulación descrita a continuación:

2.1.5. La Regulación

La regulación es una actividad fundada en normas, que constituyen el denominado marco regulatorio, destinadas a fijar las condiciones económicas, técnicas y sociales en las que deben ser prestadas aquellas actividades esenciales para la sociedad.

En el modelo de regulación seguido por Bolivia y aconsejado por expertos internacionales es el de árbitro independiente que vela por los intereses del Estado, prestadores del

servicio y usuarios, así como por la aplicación de las reglas de juego; postulados que se efectivizan a través de las atribuciones que le otorga el marco regulatorio.

En el nuevo escenario de prestación de servicios el regulador debe corregir las fallas del mercado con el fin de maximizar el beneficio para la sociedad; y el poder político debe definir las pautas estratégicas a través de la generación de normas.

Asimismo, el órgano regulador verifica el cumplimiento de las obligaciones contractuales del concesionario del servicio, resolviendo cotidianamente los asuntos emergentes de la prestación privada de los servicios, centrados en la relación entre los diversos prestadores entre sí y con sus usuarios.

Los servicios públicos de telecomunicaciones se desarrollan en régimen de concesión y su reglamentación es muy minuciosa, orientada a garantizar el suministro del servicio, presente y futuro a todo aquel que lo solicite sin discriminaciones; aprobar tarifas que respondan a costos y establecer los niveles adecuados de calidad.

El control del espectro electromagnético, como bien de dominio originario del Estado, está delegado al regulador, así como el establecimiento de estándares y planes técnicos necesarios. El ejercicio de cada una de las atribuciones del regulador puede derivar, en caso de incumplimientos o violaciones a la norma, en el ejercicio de otra atribución reguladora que es la de imponer sanciones.

La regulación de las Telecomunicaciones en Bolivia maneja:

- La regulación moderna en la Sociedad de la Información
- Otorgación de Derechos
- Promoción y Defensa de la Competencia
- Sanción a prácticas anticompetitivas
- Regulación de los Servicios y sus correspondientes tarifas
- Control del Espectro Electromagnético
- Protección de los Intereses del Consumidor
- Ventanilla Única del Operador
- Usa de Normas Contables para las Empresas de Telecomunicaciones
- Metas para Operadores PCS
- Proposición de Normas
- Difusión de la Información y Medios de Comunicación Informativos Permanentes
- Intervención en COTEL y control permanente de ENTEL

- Servicios y Acceso Universal a las Telecomunicaciones[SITTEL, ©2000]

El desempeño de SITTEL como se observo esta orientado hacia el mercado y un grupo determinado de empresas, para lo cual tiene la siguiente organización:

2.1.6. La Organización de SITTEL

El sector de las telecomunicaciones era considerado como un sector suntuario, destinado a satisfacer las necesidades de las clases altas. Asignar recursos al desarrollo de las telecomunicaciones se consideraba un desperdicio de los escasos fondos con que contaba Bolivia, que más bien podrían ser dedicados a los sectores de salud, educación y saneamiento básico, calificados como “fundamentales”.

En esos años se postulaba que una vez desarrollada la economía de nuestro país y satisfechas sus necesidades básicas, recién se podría pensar en invertir en la mejoría de las telecomunicaciones; cuando en realidad no se podía alcanzar un grado de desarrollo similar al de nuestros vecinos sino mejorábamos nuestra infraestructura sectorial.

Conseguir priorizar inversiones en el sector dentro del marco del presupuesto general de la nación era una tarea muy difícil, pues los principales actores con poder de decisión preferían las inversiones “visibles”.

Como consecuencia de esta política errónea, nuestra nación apenas contaba con servicios de telecomunicaciones en treinta localidades y solamente diez de ellas con servicios automáticos nacionales y ninguna con discado directo internacional.

A principios de la década de los 90, la concepción del gobierno cambió y consecuente con su nueva visión declaró 1990 como “El año del desarrollo de las telecomunicaciones en Bolivia”.

A partir de este impulso el panorama desolador de equipos obsoletos y vastas regiones del país incomunicadas cambió radicalmente, lográndose renovar el equipamiento y comunicar de manera automatizada a más de 350 poblaciones en tiempos realmente breves.

Actualmente, la Superintendencia de Telecomunicaciones es el órgano técnico del Estado que asume el rol fundamental de promover el desarrollo de este dinámico sector, organizado jerárquicamente (ver Anexo D).

SITTEL, como toda institución, tiene una visión, que constituye el norte de la organización y de cada uno de sus funcionarios, es la siguiente:

MÁS Y MEJORES COMUNICACIONES A MENOR COSTO

Ahora bien, la misión de SITTEL -de acuerdo a la ley del Sistema de Regulación Sectorial- puede expresarse de manera resumida de la siguiente forma:

Regular, controlar y supervisar las actividades del sector de telecomunicaciones, asegurando y promoviendo:

- Eficiencia
- Desarrollo económico
- Acceso universal a los servicios
- Efectividad en la protección legal de los intereses de las partes.

Como se puede ver, estos puntos involucran y orientan todas nuestras actividades y, nuevamente hoy como en el pasado reciente, a partir de la comprensión de la importancia del sector, la visión de SITTEL es la de lograr: Más y Mejores Comunicaciones a Menor Costo. [SITTEL, ©2002]

La funcionalidad de una empresa es importante y es la base para organizarse, la organización funcional de SITTEL en el Departamento de Tecnologías de Información y Comunicación es:

2.1.6.1. Jefatura de Tecnologías de la Información y Comunicación

La aplicación de tecnologías de la información y comunicación continúa en ascenso en la Superintendencia de Telecomunicaciones, con el objeto de desarrollar las tareas regulatorias de forma más eficiente y competitiva, y por ende, mejorar la productividad de la organización.

La red multimedia (voz y vídeo) cuenta con 1 50 puntos, que permitirá en un futuro cercano la realización de videoconferencias y otros servicios multimedia que aún no fueron implementados.

Las computadoras y los periféricos (impresoras, multimedia, etc.) son herramientas fundamentales para lograr el buen funcionamiento de SITTEL. Durante el año 2004 se tenían instalados 150 puntos de red telefónicos, 35 impresoras, 105 computadoras personales, 109 teléfonos internos y 150 puntos de red de datos e implementación del proyecto **E-SITTEL**. [SITTEL, ©2004]

2.1.6.2. E-SITTEL

Durante el primer cuatrimestre de la presente gestión, nació el proyecto de e-gobierno: e-SITTEL.

Este proyecto busca utilizar las Tecnologías de la Información y Comunicaciones (TICs) para mejorar la entrega de los resultados de la regulación a los diferentes actores a través de procesos optimizados.

Mediante la implementación de este proyecto, SITTEL espera prestar servicios acordes a las necesidades de sus públicos externos, por medio de una constante implementación y actualización de las TICs en el funcionamiento de los procedimientos internos.

El proyecto consta de seis fases: identificación de resultados y procesos actuales, evaluación de los procesos, propuesta de procesos e-SITTEL, institucionalización de procesos e- SITTEL, implementación de procesos manuales y desarrollo de procesos automáticos y retroalimentación y control de los procesos.

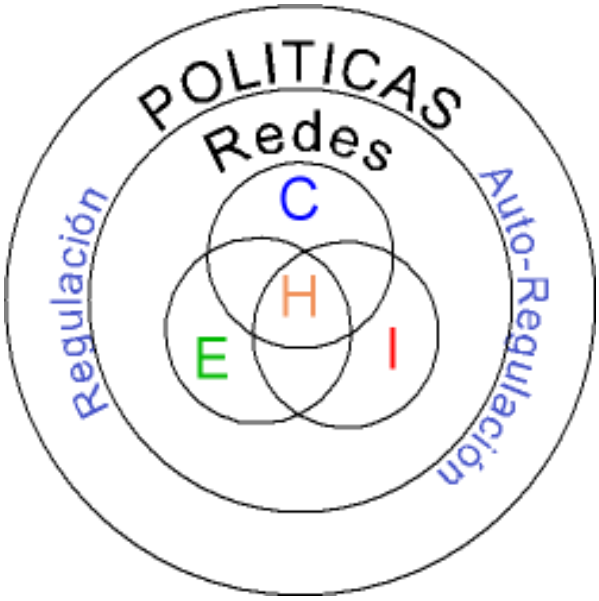
La proyección de e-SITTEL implicó la reestructuración de la Jefatura de Sistemas, ahora Jefatura de Tecnologías de Información y Comunicaciones, orientada a la administración del conocimiento institucional (para mayor información revise el Anexo F)**.** [SITTEL, ©2005]

2.2. Antecedentes Legislativos

La Sociedad de Información hace referencia a un paradigma que esta produciendo profundos cambios en nuestro mundo[19] al comienzo de este nuevo milenio respecto a las nuevas tecnologías de información y comunicación[20], las actuales leyes no sustentan a las nuevas herramientas como son las firmas y certificados digitales. [CEPAL – Conferencia Los caminos hacia una Sociedad de la Información en América Latina. ©2003]

[19] No solamente en Bolivia
[20] El Internet, los celulares, la telefonía IP.

Figura 2. 5: Componentes de la Sociedad de la Información



H: Hombre / Ser Humano

E. Enseñanza / Capacitación

I: Infraestructura / Acceso

C: Contenido

Fuente: Elaboración Propia

Con el fin de aplicar Legislaciones y Normas en América Latina (ver figura 2.5) que rijan las nuevas tecnologías de Información y Comunicación, CEPAL conformada por Organizaciones Públicas y Privadas de los Países de Latinoamérica (ver Anexo H) organizo proyectos en el área de Tecnologías de la Información y Comunicación:

- Nombres de Dominio
- Protección de Datos Personales
- Delitos Informáticos
- Firmas y Certificados Digitales
- Contratación Electrónica a través de firmas digitales
- Introducir el concepto de dinero electrónico el cual reemplazara al dinero físico y a las tarjetas de crédito a través de la utilización de su firma digital y cuentas de bancos como se observa en la Figura 2.6.[Alfa-Redi, ©2003]

Figura 2. 6: Las Tarjetas de Crédito podrán ser reemplazadas por Firmas Digitales

Fuente: elaboración propia

2.2.1. Sociedad de la Información en Latinoamérica

La Sociedad de la Información en Latinoamérica en estos años presento los siguientes avances, de los cuales destacamos a:

- **Nombres de Dominio.**
  - Registro y control de los nombres de dominio en el ámbito nacional de cada país.
  - Bolivia: Decreto Supremo Nº 26624 – Consejo de Ministros: Reglamento para el Registro de Dominios.
- **Protección de Datos Personales.**
  - Fundamentalmente se ha trabajado el concepto del *habeas data* a nivel constitucional.
  - Principales avances: Argentina, Chile y Costa Rica.
  - Existe una confrontación entre las "Centrales de Riesgo Crediticio" y la posible normativa de Protección de Datos Personales. (Prima lo económico sobre lo social)

- En Bolivia se encuentra en tratamiento con el Anteproyecto de Ley de "COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS".

- **Delitos Informáticos.**
  - La regulación esta dividida:
    - Modificación de códigos existentes, generando tipos especiales para temas informáticos.
    - Modificación y creación de agravantes por el medio tecnológico utilizado.
    - Creación de normativa específica para delitos informáticos.
  - Problema: No se tiene claro cual es el bien jurídico protegido.
    - Propuesta:
      - El bien jurídico protegido es la Información.
      - El bien jurídico protegido es el soporte informático.
  - Bolivia: Existe una propuesta de Modificación del Código Penal y se toma en cuenta en el Anteproyecto de Ley de "COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS".

- **Contratación Electrónica.**
  - Desarrollo de una Legislación Específica.
  - Modificación de Códigos Civiles.
  - Aplicación suplementaria de normas de contratación a distancia y/o entre ausentes.
  - Mayor desarrollo en relaciones estado-empresa para la contratación estatal.
  - En Bolivia se encuentra en tratamiento con el Anteproyecto de Ley de "COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS".

- **Firmas Digital: En el área de las firmas digitales en Latinoamérica CEPAL tuvo los siguientes resultados:**

- Modelos basados en la "Ley Modelo Uncitral": Puerto Rico, Colombia, Ecuador.
- Modelos Basados en UTAH: Argentina.
- Tipo Normativa Europea: Perú, Chile.
  - Diferencia entre firma electrónica y firma digital.
  - Soporte legislativo para Certificados Digitales.
- En Bolivia se encuentra en tratamiento con el Anteproyecto de Ley de "COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS".
- Soporte legislativo para Firmas Digitales.
- Soporte legislativo para Certificados Digitales.

➢ **Algunos Temas Pendientes:**

- La prueba del contrato electrónico.
- La tributación en el Comercio Electrónico.
- Propiedad Intelectual: Nombres de Dominio.
- Momento de la formación de los contratos electrónicos.
- Jurisdicción y Ley aplicable en los contratos electrónicos.
- Solución de Conflictos en los Contratos Electrónicos. [Alfa-Redi, ©2005]

2.2.2. Anteproyecto de Ley

En nuestro país se encuentra en desarrollo un anteproyecto de ley denominada "Ley de Comunicación Electrónica de Datos, Contratación Electrónica y Firmas Electrónicas" (ver anexo N) mencionado en el anterior punto. Dicho anteproyecto de ley se desarrollo con la participación del ADSIB[21], la SITTEL[22] y el PNUD[23], la cual fue publicada en Junio del 2004, dentro de los puntos más importantes que refiere el anteproyecto de ley tenemos:

❖ Referencia a los Mensajes de datos, Documentación Electrónica, Comunicación electrónica de Datos, Firma Electrónica y Certificado Electrónico, Prueba y

[21] Agencia para el Desarrollo de la Sociedad de la Información en Bolivia. www.bonet.bo
[22] Superintendencia de Telecomunicaciones. www.sittel.gov.bo
[23] Plan Estratégico de la Naciones Unidas para el desarrollo.

Notificaciones Electrónicas, Derechos de los Usuarios, Correo Electrónico, Infracciones de los Prestadores de Servicios de Certificación y Delitos Informáticos.

- El organismo Regulador de los certificados y las firmas digitales viene a ser la Superintendencia de Telecomunicaciones.
- Establece los requisitos que debe cumplir lar firmas electrónicas en Bolivia, además de procedimientos de control, obligaciones del titular o cliente, administración de empresas emitidotas de firmas y certificados digitales y el papel de SITTEL como entidad reguladora

Para su mayor estudio adjuntamos en el Anexo N el anteproyecto de ley en su Título II referente a firmas electrónicas y certificados electrónicos.

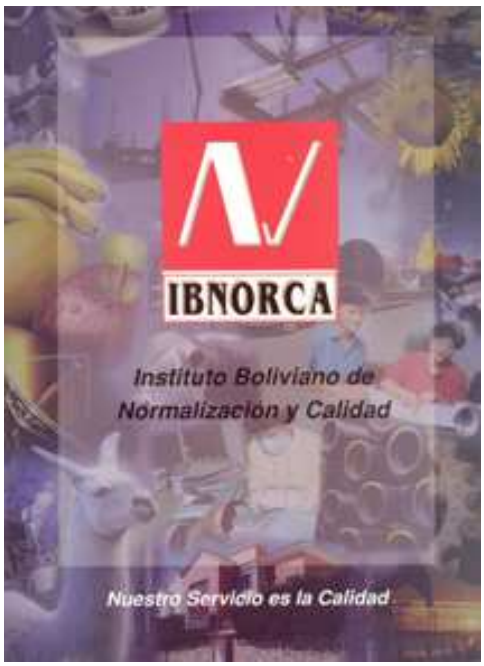
Después de realizar el análisis correspondiente al anteproyecto de ley en su Titulo II. Firmas y Certificados Electrónicos, se concluye que puede resultar delicada la implementación del software si no esta de acuerdo con el anteproyecto de ley. En SITTEL no se cuenta con herramienta alguna para su utilización y prueba ante la posible aprobación del anteproyecto de ley, demostrando una falta de conocimiento sobre las herramientas criptográficas.

2.3. Antecedentes Normativos

La norma es una regla de conducta por el cual las personas y organizaciones están regidas para actuar e interrelacionarse, se puede hablar de normas de conducta a la hora de almorzar o normas para bailar un vals, pero la referencia que hacemos al contexto es en el ámbito institucional.

Las normas en el ámbito empresarial son dadas por el Instituto Boliviano de Normalización y Calidad (IBNORCA), el cual se encarga de establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de pretender al conocimiento y la aplicación de la normalización como base de la calidad, con el fin de promover actividades de certificación de productos y de sistemas de calidad en las empresas para brindar seguridad al consumidor. [IBNORCA, ©2004]

Figura 2. 7: Logo de IBNORCA



Fuente: IBNORCA – www.ibnorca.org.bo

El Decreto Supremo Nº 23486 del 29 de Abril de 1993 promueve la creación de IBNORCA como una entidad de carácter privado sin fines de lucro y de ámbito nacional; así mismo, le otorga como funciones básicas la Normalización Técnica y la Certificación, dos pilares fundamentales de la calidad (ver figura 2.7). [IBNORCA, ©2005]

El Instituto Boliviano de Normalización y Calidad – IBNORCA fue fundado el 5 de Mayo de 1993 y la competencia de sus funciones son ratificadas mediante el Decreto Supremo Nº 24498 del 17 de Febrero de 1997 de creación del Sistema Boliviano de Normalización, Metrología, Acreditación y Certificación – SNMAC. [IBNORCA, ©2005]

Su fundación fue promovida por las siguientes instituciones:

- Cámara Nacional de Industrias
- Cámara Nacional de Comercio
- Cámara Boliviana de la Construcción
- Cámara Nacional de Exportadores de Bolivia
- Federación Nacional de la Pequeña Industria

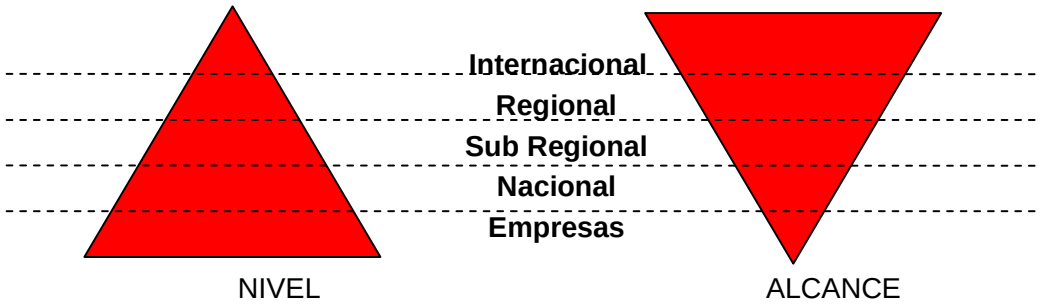
- Secretaría Nacional de Industria y Comercio

IBNORCA desarrolla la normalización para ofrecer beneficios como consecuencia de la adaptación de los productos, procesos y servicios a los fines a los que se destina, proteger la salud y el medio ambiente, prevenir los obstáculos técnicos al comercio y facilitar la cooperación tecnológica y la certificación contribuyente a la consecución de la calidad. En particular, la normalización en IBNORCA, consiste en la elaboración, adopción, armonización, difusión y aplicación de normas. Actualmente se tienen elaboradas alrededor de 1200 Normas Bolivianas.

La existencia de diferentes normas en el mundo que se diferencian por los niveles de importancia, llegan a adquirir en una institución o producto importancia por su alcance:

2.3.1. Niveles y Alcance de la Normalización

Figura 2. 8: Descripción de los Niveles de Normalización y Alcance de las Normas



Fuente: Elaboración Propia

Como se puede observar, la relación entre el nivel y el alcance es inversa, a mayor nivel de las normas de alcance menor.

2.3.2. Importancia de la Normalización

La normalización es un factor imprescindible para desarrollar una política seria de calidad. Bolivia esta tomando conciencia de que la infraestructura de la normalización, basada en referencias comunes entre los países y regiones es condición básica para mejorar la productividad, la competitividad en los mercados y la capacidad de intercambio comercial:

- Facilita la planificación en la producción
- Racionalizan los procesos y las operaciones

- Promueven calidad con economía
- Facilita el intercambio comercial nacional e internacional
- Simplifican la comunicación y la relación cliente-proveedor
- Inspiran confianza en los productos para su uso

A continuación describimos la normalización y los sistemas de calidad aplicados en Bolivia

2.3.3. Normalización y los Sistemas de Calidad

La International Organization for Standardization - ISO, dio vigencia al tema de aseguramiento de la calidad, con la aprobación de las Normas de la Serie ISO 9000, por primera vez, en el año 1987, las mismas han tenido un impacto enorme a nivel mundial, habiendo sido adoptadas y aprobadas como normas, por todos los países desarrollados, incluyendo Japón, Estados Unidos y los de la Unión Europea; obviamente, su impacto tuvo que alcanzar también a Latinoamérica, aceptando y adoptando estas normas, muchos países de la región.

La importancia de estas normas, radica en que se han constituido en la base, universalmente aceptada, para la certificación por terceras partes; asimismo, como la ISO establece que las normas internacionales deben revisarse periódicamente, la serie de normas ISO 9000, han tenido una primera revisión en el año 1994 y han sido actualizadas el año 2000.

2.3.4. *Sistemas de Gestión de Seguridad de Información*

Para el fin de la investigación haremos referencia a IBNORCA, representante de Bolivia ante la Organización Internacional de Estandarización (ISO), a quien pertenece la Norma Bolivia-ISO-IEC 17799 para TECNOLOGÍA DE INFORMACIÓN – CÓDIGO DE PRÁCTICA PARA LA GESTIÓN en correspondencia a la ISO 17799:2000 Information Technology – Code if practice for information security management.

El 2003, IBNORCA con el fin de incorporar normas que estaban siendo muy utilizadas a la fecha introdujo a su plantel el Comité Técnico en la adopción de la norma internacional ISO 17799:2000.

El Comité Técnico estaba conformado por:

Guido Rosales Uriona	COSSIM ROSALES S.R.L.
Natalia Katia Sanjines Díaz	IBNORCA

Luis Fernando Justiniano Peñaranda IBNORCA

La finalización y aprobación por el Comité Técnico fue el 15 de octubre de 2003 y a principios del 2004 la norma era Boliviana. [IBNORCA, ©2004]

Con el fin de hacer estudio en la aplicación de la Norma se desarrolla el siguiente punto:

La Norma Boliviana ISO IEC 17799 es considerada un sistema de gestión. Enfatizando, es un sistema que establece políticas y objetivos en busca de alcanzar dichos objetivos institucionales

Los sistemas de gestión son utilizados por las organizaciones para desarrollar sus políticas y hacerlas efectivas a través de sus objetivos, considerando:

- Estructura Organizacional.
- Procesos sistemáticos y recursos asociados.
- Mediciones y metodologías de evaluación.
- Examen de procesos para asegurar que los problemas son corregidos y las oportunidades de mejora son reconocidas e implementadas cuando se justifica.

En resumen *"Lo que se monitorea se debe medir, lo que se mide puede ser administrado".* [IBNORCA, ©2005]

2.3.5. *Elementos de los Sistemas de Gestión*

Para medir la efectividad de aplicación de un sistema de gestión se debe contar con los siguientes elementos:

- Políticas: demostración del compromiso y principios para la acción de la implementación de la norma en la institución.
- Planeamiento: identificación de necesidades, recursos, estructura y responsabilidades en la institución.
- Implementación y operación: concientización y entrenamiento del personal en la aplicación de la norma.
- Evaluación del desempeño: monitoreo y mediciones además del manejo de las no conformidades en la institución y las auditorias.
- Mejoras: Acciones preventivas y correctivas en busca de una mejora continua, que es el principal fin de la aplicación de estas normas.

- Revisión gerencial: con el fin de implantar normas y ser auditadas y controladas por la alta gerencia. [IBNORCA, ©2005]

Definido el concepto de Sistema de Gestión ahora se hará el estudio de Sistema de Gestión de Seguridad de Información

2.3.6. *SGSI – Diseño e Implementación*

SGSI[24]:

- Es la parte del sistema de gestión, que basado en los riesgos del negocio, se centra en establecer, implementar, operar, supervisar, revisar, mantener y mejorar el sistema de seguridad. [IBNORCA, ©2005]

Diseño e implementación:

- Es influenciado por los objetivos y necesidades del negocio, requerimientos de seguridad, los procesos empleados y el tamaño y la estructura de la organización. Es lógico pensar que estos y sus sistemas de soporte cambien continuamente. [IBNORCA, ©2005]

2.3.7. *ISO 17799*

El camino de ISO 17799 es la protección de la **confidencialidad, integridad y disponibilidad** de información escrita, hablada o digitalizada, ISO 17799 es:

- Una estructura metodológica dedicada a la seguridad de información reconocida internacionalmente.
- Un proceso definido para evaluar, implementar, mantener y administrar la seguridad de información.
- Un conjunto integral de controles comprendidos en las mejores prácticas en seguridad de información.
- Desarrollado por la industria para la industria.[25]

ISO 17799 no es:

- Un estándar técnico orientado a un producto o tecnología

[24] SGSI: Sistema de Gestión de Seguridad de Información
[25] Seminario Internacional "Gestión de la Seguridad de la Información: Introducción a la Norma NB-ISO/IEC 17799"

- ❖ Una metodología de evaluación de equipamiento tal como el criterio Común/ISO 15408
    - o Pero puede requerir la utilización de una "Common Criteria Equipment Assurance Level (EAL)"[26]
- ❖ Relacionando con los "Generally Accepted Systemn Security Principles," or GASSP.
    - o Pero puede incorporar los lineamientos de los GASSP
- ❖ Relacionado con las cinco partes de las "Guidelines for the Management of IT Security," o GMITS/ISO TR 13335
    - o Pero puede implemetar conceptos de las GMITS.[27] [IBNORCA, ©2005]

ISO 17799 puede ser utilizada por cualquier tipo de organización o de compañía, privada o pública. Si la organización utiliza sistemas internos y externos que poseen informaciones confidenciales, si depende de estos sistemas para el funcionamiento normal de sus operaciones o si simplemente desea probar su nivel de seguridad de la información conformándose a una norma reconocida, la norma BS 7799 / ISO 17799 es la solución en Gobiernos, Bancos, Servicios de Salud, Industrias de Servicio Privadas, etc. [IBNORCA, ©2005]

ISO 17799 define las mejores prácticas para la administración de la seguridad de información.

Un sistema de gestión debe balancear la **seguridad física**, **técnicas**, **procedimental**, y **personal**. Sin un Sistema de Administración de Seguridad de Información formal, tal como el descrito en la ISO 17799-2, hay un riesgo grande de que existan brechas en la seguridad.

La seguridad de información es un proceso de gestión, no un proceso tecnológico. [IBNORCA, ©2005]

El ISO 17799 se resume en medible, repetible y escalable:

Medible:

- ➢ Solamente un estándar internacional puede ser evaluado por terceros.
- ➢ Incorpora un proceso de escalas de riesgos y de valoración de activos.

[26] Criterio de Equipo de Común Nivel de Convicción.
[27] Referencia: "Information Security Management: Understanding ISO 17799," Ton Carlson, Lucent Technologies Worldwide Services

- Evalúa las amenazas, vulnerabilidades, impactos, tolerancia de riesgos, grado de aseguramiento, probabilidad de la ocurrencia.

Repetible:

- El nivel de formalización del sistema y el poseer procesos estructurados ayudarán a hacer que el sistema sea repetible.
- La inversión en el compromiso de la dirección superior y la educación de los empleados en el tema de seguridad reducirá la probabilidad de las amenazas.

Escalable:

- La infraestructura (sistema de dirección y procesos) puede ser desarrollada en forma centralizada y luego desplegada a escala mundial.
- Si se desea, puede ser agregados controles adicionales al SGSI. [IBNORCA, ©2005]

El ISO 17799 Estándar se divide en:

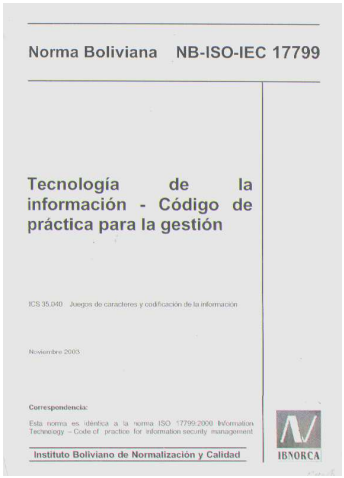
- ISO/IEC 17799:2000

  Código de Prácticas para Administración de Seguridad de Información

- BS 7799-2:1999

  Especificaciones para un Sistema de Administración de Seguridad de Información es el ISO 17799 como se observa en la figura 2.9.

Figura 2. 9: Código Internacional de Mejores Prácticas


Norma Boliviana NB-ISO-IEC 17799

Tecnología de la información - Código de práctica para la gestión

ICS 35.040 Juegos de caracteres y codificación de la información

Noviembre 2003

Correspondencia:

Esta norma es idéntica a la norma ISO 17799:2000 Information Technology – Code of practice for information security management

Instituto Boliviano de Normalización y Calidad

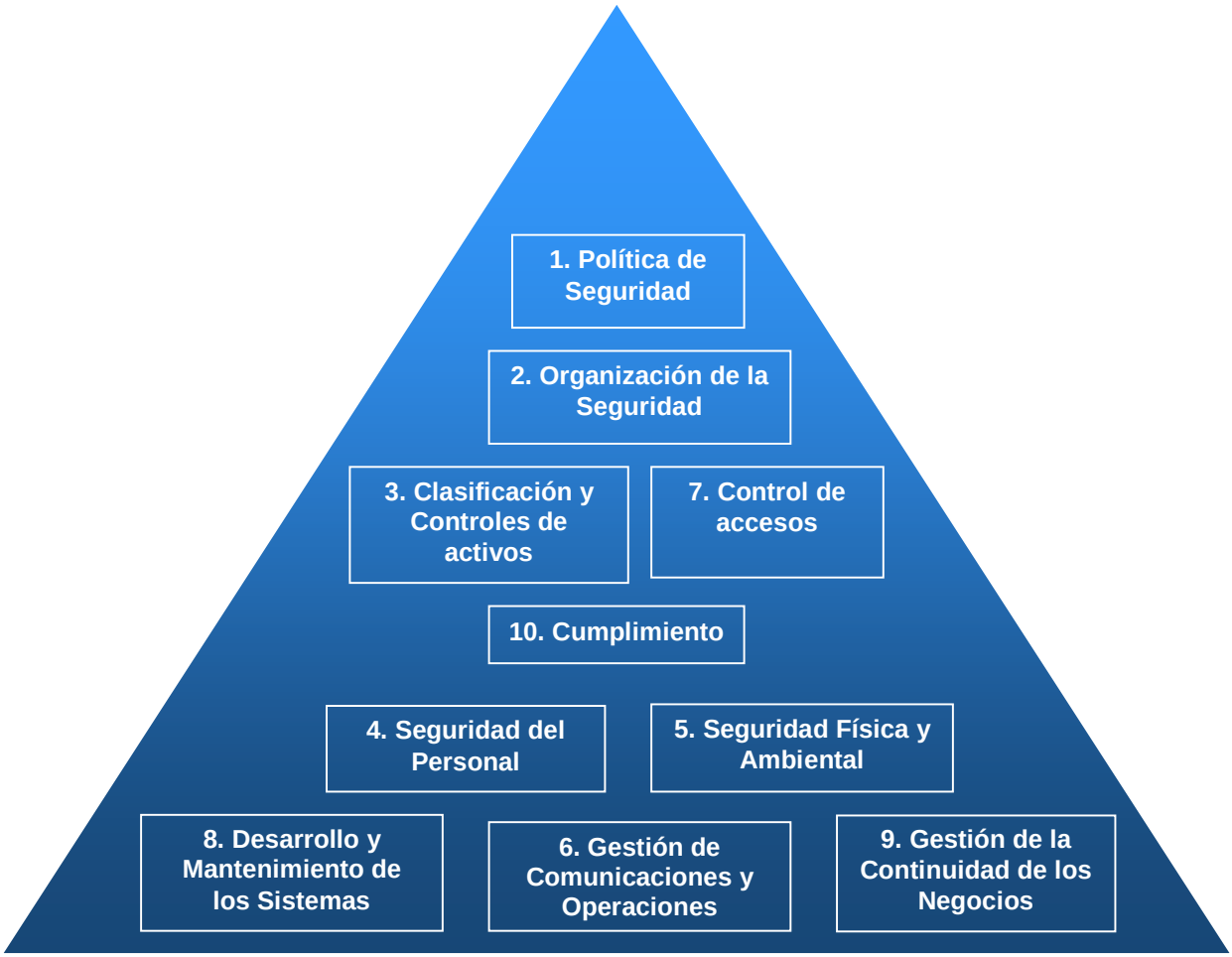
IBNORCA

Fuente: IBNORCA – www.ibnorca.org.bo

El ISO 17799 es un Código Internacional de Mejores Prácticas y es funcional:

- Basado sobre la norma BS 7799-1:1999.
- Preparado para ser utilizado como documento de referencia.
- Provee un conjunto integral de controles de seguridad.
- Basado sobre mejores prácticas de seguridad de la información.
- Su aplicación coadyuva en la aplicación de sistemas de gestión como son los ISO 9000.
- Consiste de 10 secciones de control, 36 objetivos de control y 128 controles (medidas) descritas a continuación en la figura 2.10:

Figura 2.10: Las 10 secciones de ISO 1799



Fuente: Seminario Internacional sobre "Gestión de la Seguridad de la Información en la empresa Norma ISO/IEC 17799"

2.3.8. *Razones para Adoptar ISO 17799*

Las razones principales para que las empresas adopten el ISO 17799 son:

- Aumenta la eficiencia de la seguridad de la información
- Diferenciarse en el mercado y satisfacer requerimientos de clientes
- Único estándar mundialmente reconocido en esta área
- Potenciales disminuciones de costo y primas de seguros
- Focaliza las responsabilidades del personal
- La Norma cubre tanto IT como organización, personal e instalaciones
- Mandatos legales (por el. Habeas Data, Firma Digital, Reforma del Estado, etc.)
- Se complementa a estándares como ser:
    - Productos y sistemas certificados ISO 15408 (CC)
    - Guías para la gestión de la seguridad de la TI ISO 13335 (GMIT5)
- Reduce los problemas por políticas o procedimientos no implementados
- Oportunidad para identificar vulnerabilidades
- La Alta Gerencia se transforma en propietaria de la seguridad de información
- Examen independiente de su Sistema de Gestión de Seguridad de Información
- Provee privacidad a socios comerciales inversionistas y clientes (la certificación demuestra 'due diligence')
- Mejora la conciencia sobre la seguridad
- Combina recursos con otros Sistemas de gestión
- Mecanismo para la medición del éxito del sistema [IBNORCA, ©2005]

Para mayor información de IBNORCA revise el Anexo G.

Conclusiones del Capítulo

Planteadas todas la bases referenciales sobre la Superintendencia de Telecomunicaciones, el Anteproyecto de Firmas y Certificados Digitales, y la Normativa Internacional para la Seguridad de la Informaciones llega a las siguientes conclusiones:

- A diez años de la creación de la Superintendencia de Telecomunicaciones en Bolivia, se tuvo un desarrollo inigualable a anteriores gestiones en el desarrolla de las comunicaciones, sin embargo Bolivia sigue retrasado en la implementación de nuevas tecnologías que ayuden al desarrollo de la Sociedad de la Información, entre las que se encuentran las firmas y certificados digitales.
- El Anteproyecto de ley de "COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS", será la primera ley en Bolivia orientada hacia el área de las Tecnologías y desarrollada por SITTEL, ADSIB y PNUD; con su aprobación Bolivia tendrá una herramienta para gestionar las firmas y certificados digitales.
- Para el desarrollo del presente proyecto de grado se utilizó el Anteproyecto de ley mencionado para el correspondiente sustento jurídico para las firmas y certificados digitales y con probabilidades de ser promulgado el anteproyecto de ley entre finales del 2005 y 2006.
- El Instituto Boliviano de Normalización y Calidad más conocido como IBNORCA, con apoyo de especialistas en el área de la seguridad de la información, conformaron equipos técnicos que trabajaron en la adopción de la Norma Internacional ISO/IEC 17799 a Norma Boliviana; entre los participantes se encuentra el Ing. Guido Rosales (Tutor del presente proyecto de grado).
- La mencionada Norma tiene sus orígenes en la Norma BS 7799 del Reino Unido y nos servirá para identificar los riesgos inherentes a la utilización de Tecnologías de Información y Comunicación en la Superintendencia de Comunicaciones antes y después de la aplicación de Firmas y Certificados Digitales, verificando el grado de riesgo que tiene por problemas de seguridad de la información.

Capítulo 3
Marco Teórico y Metodológico

"… es imposible hablar o pensar sin recurrir a conceptos generales; sin ellos, el conocimiento y el lenguaje resultan imposibles."

Daniel Allahan

Resumen

El presente capítulo expone los fundamentos y bases teóricas sobre criptografía y seguridad de sistemas, ingeniería de software y auditoria de sistemas, ciencias que serán empleadas en el desarrollo del trabajo de grado, también muestra la metodología para el análisis y diseño del sistema de administración para firmas y certificados digitales.

3.1. Criptografía y Seguridad de Sistemas

La utilización cada vez más creciente de Internet y la constante interconexión entre redes de computadoras ha incrementado los riesgos para poder garantizar la seguridad de la información de una empresa.

Las vulnerabilidades y amenazas crecen en forma exponencial. Todos los días se descubren nuevas vulnerabilidades en el software, hardware, los protocolos de comunicación, los procedimientos usualmente aceptados y en usuarios internos, en ocasiones un ex-empleado, un proveedor, un contratista, un consultor cuando se convierten en atacantes.

Los responsables en el área de sistemas cada vez se ven más desbordados por la tecnología. Aspectos tales como: la presión del día a día, los nuevos requerimientos, el mantener los sistemas funcionando, el satisfacer las demandas de los usuarios y otras responsabilidades saturan la agenda del departamento de Sistemas o Tecnologías de Información y Comunicación. Esta carga de trabajo lleva consigo dejar la seguridad en último lugar. [Advance Team, © 2004]

La aplicación de la seguridad de sistemas coadyuva en la mejora de la seguridad institucional.

3.1.1. Seguridad de Sistemas

Según la Organización de Internacional de Estándares la información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y

por consiguiente debe ser debidamente protegida. La seguridad de la información comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades de negocio.

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o utilizando medios electrónicos y otros. Cualquiera sea la forma que adquiera la información, o los medios por los cuales se distribuya o almacena, siempre debe ser protegida en forma adecuada, para lo cual la seguridad de la información deberá cumplir los siguientes requisitos.

a) Confidencialidad: garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

b) Integridad: salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

c) Disponibilidad: garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

La seguridad de la información se logra implementando un conjunto adecuado de controles que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. [NB-ISO-IEC 17799, ©2004]

3.1.2. Políticas de Seguridad

Según Ruiz las políticas de seguridad, son las prácticas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de daño sobre:

- Las computadoras de los sistemas de la organización y los elementos físicos asociados con éstos (edificación, impresoras, discos, cables, dispositivos de interconexión, etc.)
- El software y la información almacenada en los sistemas de la organización.
- Los usuarios que tiene acceso al sistema de la organización. [RUIZ, ©1993]

Según Microsoft el conjunto de medidas preventivas, de detección y corrección destinadas a proteger la integridad, confidencialidad y disponibilidad de los recurso informáticos además de afirmar que la seguridad informática permite compartir los Sistemas de información de la empresa entre sus empleados, e incluso con terceros, pero garantizando su protección a través del Análisis de Gestión y Riesgos aplicados a la seguridad de la información. [NB-ISO-IEC 17799, ©2004]

3.1.3. Análisis de Gestión y Riesgos de Seguridad

Según la Organización Internacional de Estandarización (ISO) define a los riesgos como las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de su ocurrencia, existiendo en cualquier actividad la contingencia implícita asociada al medio de trabajo y las tecnologías exigentes. [ISO 9001, ©2002]

La gestión de riesgos hace procesos de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información. [NB-ISO-IEC 17799, ©2004]

A través de la gestión de riesgos se determinan las vulnerabilidades, amenazas y las posibles contramedidas, los cuales son:

- Vulnerabilidad: Representan las debilidades, aspectos factibles o atacables en el sistema informático.
- Amenaza: Posible peligro del sistema. Puede ser una persona, un programa o un suceso natural o de otra índole. Existen dos tipos de amenazas.
- Y las Contramedidas: Técnica de protección del sistema contra las amenazas, por el cual se determino que más de la mitad de los mismos son ataques intencionados por Hackers.

3.1.4. Técnicas de Hacking

Un hacker es una personas con elevado conocimiento de la computación tanto en hardware como en software, vulneran los servicios más seguros con la finalidad de avisar a la empresa que tiene alguna vulnerabilidad, nunca aprovechan la información obtenida, caso contrario ocurriera lo mencionado es un cracker.

A continuación describimos las principales técnicas de hacking utilizadas:

- Footprinting
- Scanning
- Enumeration
- Gaining Access
- Privilege Escalation
- Interactive Control
- Camouflaging
- Intelligence Gathering
- Island Hopping
- Denial of Service

- Buffer Overflows
- Shovel a Shell
- Social Engineering
- Y otros.

Dichos ataques crean una inseguridad en cualquier institución, razón principal para hacer una determinación de riesgos y encontrar la solución más adecuada para las necesidades de la empresa. [Microsoft, ©2004]

La determinación de riesgos busca contramedidas a estos problemas, para lo cual la existencia de diferente métodos que coadyuvan a solucionar dichos problemas tenemos:

- Establecimiento de una medida de control de accesos
- Definición de una política de instalación y copia de software
- Uso de cortafuegos para proteger los datos y las comunicaciones
- Utilización de herramientas criptográficas de las cuales destacamos.

3.1.5. Criptografía

Criptografía proviene del griego kriptón que significa oculto y pórpelv que significa escritura, y su definición es: “Arte” de escribir con clave secreta o de un modo enigmático.

El término Criptografía emplea habitualmente de Criptoanálisis y Criptosistemas.

El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado; hemos de suponer por el contrario que los algoritmos siempre son conocidos. [www.criptored.upm.es, ©2005]

En general el criptoanálisis se suele llevar a cabo estudiando grandes cantidades de pares mensaje–criptograma generados con la misma clave. El mecanismo que se emplee para obtenerlos es indiferente, y puede ser resultado de escuchar un canal de comunicaciones, o de la posibilidad de que el objeto de nuestro ataque responda con un criptograma cuando le enviemos un mensaje. Obviamente, cuanto mayor sea la cantidad de pares, más probabilidades de éxito tendrá el criptoanálisis. [www.criptored.upm.es, ©2005]

Definiremos un criptosistema como una quíntupla (M, C, K, E, D), donde:

- M representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o plaintext) que pueden ser enviados.

- C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el criptosistema.
- E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave k.
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

Dk(Ek(m)) = m (2.1) es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m. [LUCENA LOPEZ, MANUEL, ©2005]

Existen dos tipos fundamentales de criptosistemas:

Criptosistemas simétricos o de clave privada. Son aquellos que emplean la misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitir la clave de forma segura.

Figura 3. 1: Ejemplo de Criptosistema

Fuente: http://www.htmlweb.net

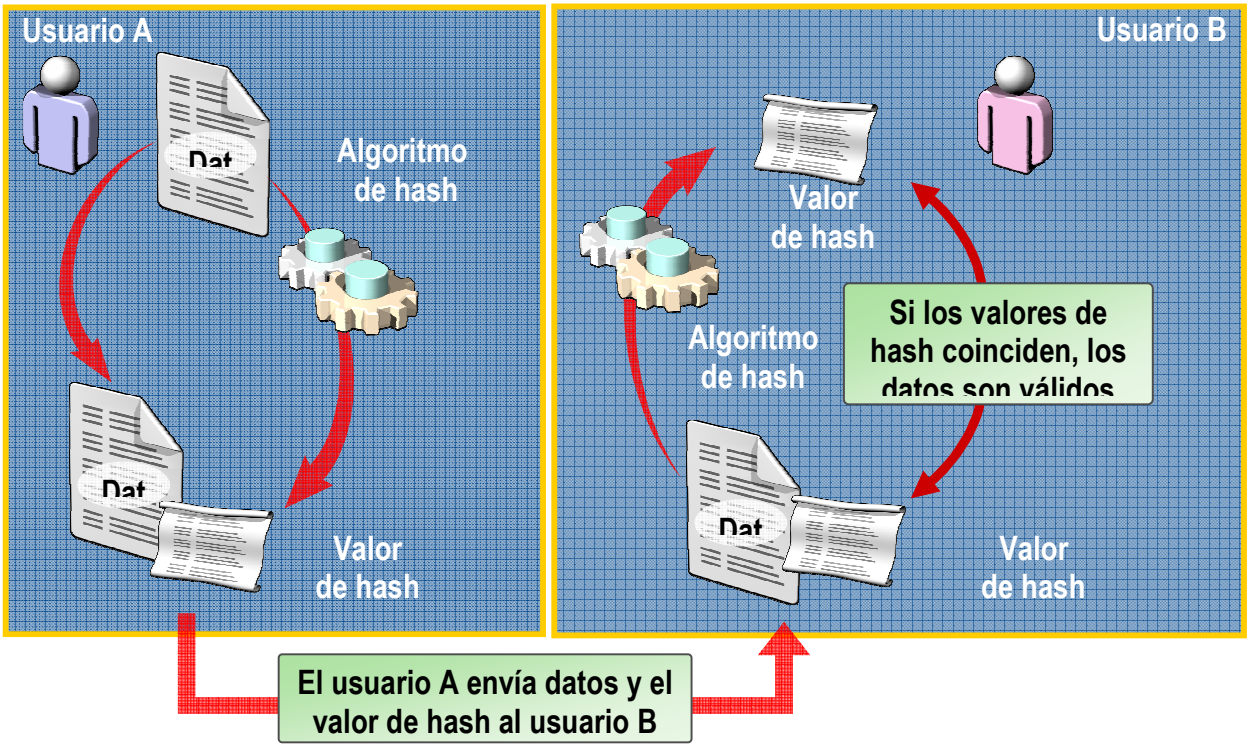
Criptosistemas asimétricos o de llave pública. Que emplean una doble clave (kp, kP). kp se conoce como clave privada y kP se conoce como clave pública (ver la figura 3.1). Una de ellas sirve para la transformación E de cifrado y la otra para la transformación D de

descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros —puesto que únicamente viaja por el canal la clave pública—, o para llevar a cabo autentificaciones. [LUCENA LOPEZ, MANUEL, ©2005]

A continuación hacemos un estudio de los cifrados asimétricos para la aplicación de estos en las firmas y certificados digitales. [LUCENA LOPEZ, MANUEL, ©2005]

3.1.6. Cifrados Asimétricos

Figura 3. 2: Cifrados Asimétricos



Fuente: Microsoft, ©2004

Introducidos por Whitfield Diffie y Martin Hellman a mediados de los años 70 (ver figura 3.2), su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares. Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros; otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, bien sea porque la longitud de la clave es enorme. Se basan en general en plantear al atacante

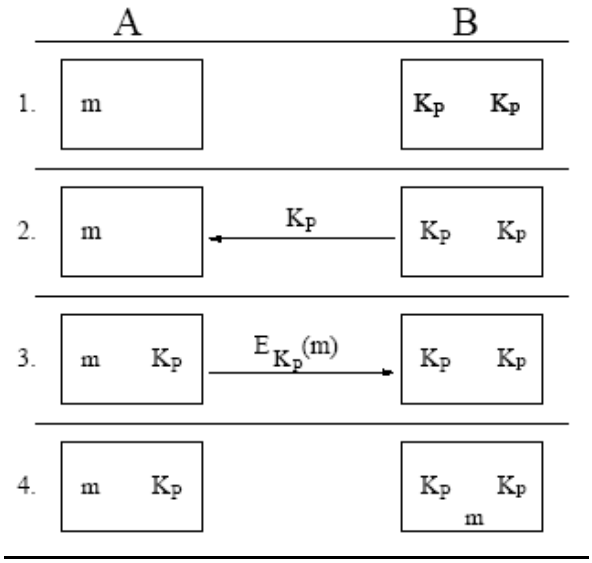
problemas matemáticos difíciles de resolver. En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable. Otros algoritmos son los de ElGamal y Rabin. [LUCENA LOPEZ, MANUEL, ©2005]

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de **128 bits**, para algoritmos asimétricos —si exceptuamos aquellos basados en curvas elípticas— se recomiendan claves de al menos 1024 bits. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado simétricos. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

Los algoritmos asimétricos poseen dos claves diferentes en lugar de una, Kp y KP, denominadas clave privada y clave pública. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra. [LUCENA LOPEZ, MANUEL, ©2005]

3.1.7. Aplicaciones de Cifrados Asimétricos

Figura 3. 3: Transmisión de la Información por Algoritmos Asímétricos



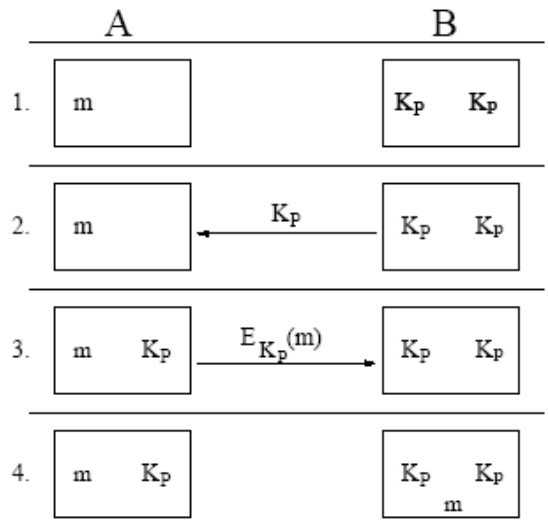
Fuente: Aplicaciones de Algoritmos Asimétricos de Manuel Lucena, ©2005

Una de las aplicaciones inmediatas de los algoritmos asimétricos es el cifrado de la información sin tener que transmitir la clave de decodificación, lo cual permite su uso en canales inseguros (ver figura 3.3). Supongamos que A quiere enviar un mensaje a B. Para ello solicita a B su clave pública KP. A genera entonces el mensaje cifrado EKP (m). Una vez hecho esto únicamente quien posea la clave Kp —en nuestro ejemplo, B— podrá recuperar el mensaje original m. Nótese que para este tipo de aplicación, la llave que se hace pública es aquella que permite codificar los mensajes, mientras que la llave privada es aquella que permite descifrarlos. [LUCENA LOPEZ, MANUEL, ©2005]

Explicación de la Figura 3.3:

1. **A** tiene el mensaje m y quiere envidárselo a **B**; 2. **B** envía a **A** su clave pública, KP; 3. **A** codifica el mensaje m y envía a **B** el criptograma EKP (m); 4. **B** decodifica el criptograma empleando la clave privada Kp.

Figura 3. 4: Autentificación de la Información por Algoritmos Asimétricos



Fuente: Aplicaciones de Algoritmos Asimétricos de Manuel Lucena, ©2005

La segunda aplicación de los algoritmos asimétricos es la autentificación de mensajes, con ayuda de funciones MDC, que nos permiten obtener una firma digital a partir de un mensaje. Dicha firma es mucho más pequeña que el mensaje original, y es muy difícil encontrar otro mensaje que dé lugar a la misma. Supongamos que A recibe un mensaje m de B y quiere comprobar su autenticidad. Para ello B genera un resumen del mensaje r(m) (ver figura 3.4) y lo codifica empleando la clave de cifrado, que en este caso será privada. La clave de descifrado se habría hecho pública previamente, y debe estar en

poder de A. B envía entonces a A el criptograma correspondiente a r(m). A puede ahora generar su propia r0(m) y compararla con el valor r(m) obtenido del criptograma enviado por B. Si coinciden, el mensaje será auténtico, puesto que el único que posee la clave para codificar es precisamente B. [LUCENA LOPEZ, MANUEL, ©2005]

Nótese que en este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.

Explicación de la Figura 3.4:

1. **A**, que posee la clave pública KP de **B**, recibe el mensaje m y quiere autentificarlo; 2. **B** genera el resumen de m envía a **A** el criptograma asociado EKp(r(m)); 3. **A** genera por su cuenta r0(m) y decodifica el criptograma recibido usando la clave KP ; 4. **A** compara r(m) y r0(m) para comprobar la autenticidad del mensaje m. [MANUEL LUCENA, ©2005]

Habiéndose revisado las aplicaciones de los criptosistemas asimétricos, se realiza a continuación el Estado de Arte para comparar las diferencias entre criptosistemas asimétricas en base a lo bueno, malo y las vulnerabilidades que presenta cada uno y elegir el criptosistema más conexo al desarrollo de firmas y certificados digitales del presente proyecto de grado.

3.1.8. Estado de Arte

En muchos de los algoritmos asimétricos ambas claves sirven tanto para cifrar como para descifrar, de manera que si empleamos una para codificar, la otra permitirá decodificar y viceversa. Entre los algoritmos asimétricos más robustos tenemos:

RSA: Debe su nombre a sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman. Tiene las siguientes características:

Lo Bueno:

- Algoritmo asimétrico con mayor facilidad de implementar y utilizarse respecto a otros algoritmos asimétricos.
- Sus claves sirven indistintamente tanto para decodificar como para autentificar.
- Es uno de los algoritmos asimétricos más seguros en el mundo.
- La dificultad de desencriptar se base en la factorización de grandes números, con algoritmos de encriptación que manejen 128 bits o superiores.

Lo Malo:

- Laboratorios RSA tuvo la patente hasta el 20 de septiembre de 2000 y actualmente la tiene el Gobierno de los Estados Unidos.
- Su utilización e implementación tiene costo de patente, por lo tanto no es un algoritmo asimétrico libre.

Vulnerabilidades:

Aunque el algoritmo RSA es bastante seguro conceptualmente, existen algunos puntos débiles en la forma de utilizarlo que pueden ser aprovechados por un atacante. A continuación se señalan las posibles vulnerabilidades:

- Claves o llaves débiles en RSA
- Claves demasiado cortas
- Ataques de Intermediario
- Ataques de Texto en Claro Escogido
- Ataques de Módulo en Común
- Ataques de Exponente Bajo
- **Ataque de Firma y Decodificar:** Con un algoritmo RSA nunca se debe firmar un mensaje después de codificarlo, por lo contrario, debe firmarse primero. Existen ataques que aprovechan mensajes primero codificarlos y luego firmados, aunque se empleen funciones resumen. [RSASECURITY, ©2005]

Algoritmo de Diffie-Hellman: Lleva el nombre de sus creadores. Tiene las siguientes características:

Lo Bueno:

- Basado en el Problema de Diffie-Hellman de transmisión segura de la información.
- No son necesarias llaves públicas en el sentido estricto, sino una información compartida por los dos comunicantes.

Lo Malo.

- Parte del protocolo de comunicación que son el factor X y Y no pueden ser trasmitidos por canales de comunicación públicos.

- Dificultad de ser utilizados para Firmas y Certificados Digitales por su estructura. Para lo cual se debe implementar una estructura de Firmas Digitales de ElGamal. [RSASECURITY, ©2005]

Algoritmo de Rabin: Las características son las siguientes.

Lo Bueno:

- Basado en el problema de calcular raíces cuadradas de módulo de un número compuesto.

Lo Malo:

- Genera cuatro posibles respuestas.
- No existe mecanismos para decidir cuál de las cuatro es la auténtica, por lo cual el mensaje deberá incluir algún tipo de información para que el receptor pueda distinguirlo de los otros. [REDIRIS, ©2005]

Algoritmo DSA: El algoritmo DSA (Digital Signature Algorithm) es parte del estándar DSS (Digital Signature Standard). Este algoritmo propuesto por el NIST data de1991, es una variante del método asimétrico ELGAMAL. Por lo cual tiene los mismos beneficios y problemas que el algoritmo mencionado. [RSASECURITY, ©2005]

PGP: Debe su nombre a sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman. Tiene las siguientes características:

Lo Bueno:

- OPEN SOURCE.
- Soporte para aplicaciones en Internet
- Aplicación de Herramientas Sencillas, Potentes y Gratuitas.
- Convertido en un estándar internacional (RFC 2440)
- Aplicación de codificación automática y transparente sobre TCP/IP (PGPnet)
- Trabajado sobre Estándares del ISO 14888 a ser utilizados en el trabajo de grado.

Vulnerabilidades:

- Escoger contraseñas inadecuadas
- Proteger adecuadamente los archivos sensibles

- Emitir revocaciones de nuestras claves al generarlas
- Creación de agujeros por mala instalación
- Intrínsecas al protocolo

Entre otros algoritmos menos relevantes tenemos el MDC, MD5 y SHA-1. Después de haberse estudiado los algoritmos se determino el uso de PGP. [GNUPGP, ©2005]

3.1.9. PGP

El nombre PGP responde a las siglas pretty good privacy (privacidad bastante buena), y se trata de un proyecto iniciado a principios de los 90 por Phil Zimmermann. La total ausencia por aquel entonces de herramientas sencillas, potentes y baratas que acercaran la criptografía seria al usuario movió a su autor a desarrollar una aplicación que llenara este hueco.

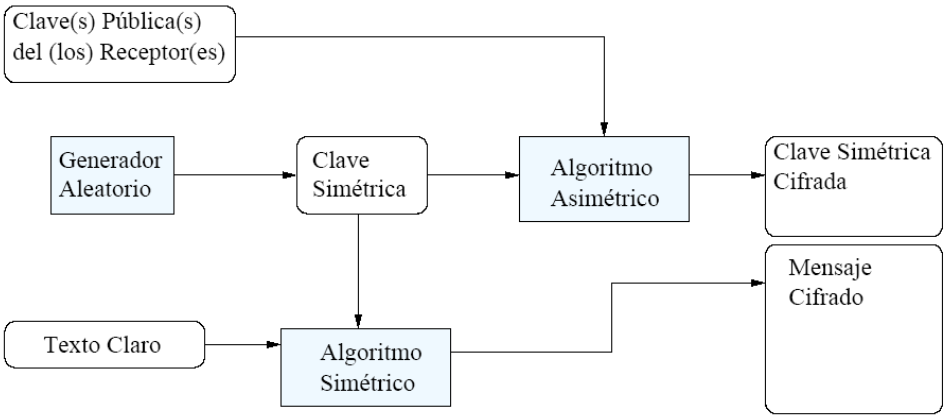
Con el paso de los años, PGP se ha convertido en uno de los mecanismos más populares y fiables para mantener la seguridad y privacidad en las comunicaciones, especialmente a través del correo electrónico, tanto para pequeños usuarios como para grandes empresas.

Actualmente PGP se ha convertido en un estándar internacional (RFC 2440), lo cual está dando lugar a la aparición de múltiples productos PGP, que permiten desde cifrar correo electrónico hasta codificar particiones enteras del disco duro (PGPDisk), pasando por la codificación automática y transparente de todo el tráfico TCP/IP (PGPnet). [PGPI, ©2005]

3.1.10. Estructura de PGP

Los algoritmos simétricos de cifrado son considerablemente más rápidos que los asimétricos. Por esta razón PGP cifra primero el mensaje empleando un algoritmo simétrico (ver figura 3.5) con una clave generada aleatoriamente (clave de sesión) y posteriormente codifica la clave haciendo uso de la llave pública del destinatario. Dicha clave es extraída convenientemente del anillo de claves publicas a partir del identificador suministrado por el usuario, todo ello de forma transparente, por lo que únicamente debemos preocuparnos de indicar el mensaje a codificar y la lista de identificadores de los destinatarios. Nótese que para que el mensaje pueda ser leído por múltiples destinatarios basta con que se incluya en la cabecera la clave de sesión codificada con cada una de las claves publicas correspondientes.

Figura 3. 5: Codificación de un mensaje PGP



Fuente: MANUEL LUCENA, ©2005

Como puede comprenderse, gran parte de la seguridad de PGP reside en la calidad del generador aleatorio que se emplea para calcular las claves de sesión, puesto que si alguien logra predecir la secuencia de claves que estamos usando, podrá descifrar todos nuestros mensajes independientemente de los destinatarios a los que vayan dirigidos. Afortunadamente, PGP utiliza un método de generación de números pseudoaleatorios muy seguro —una secuencia aleatoria pura es imposible de conseguir—, y protege criptográficamente la semilla que necesita[28]. No obstante, consideraremos sensible al fichero que contiene dicha semilla —normalmente RANDSEED.BIN—, y por lo tanto habremos de evitar que quede expuesto. [MANUEL LUCENA, ©2005]

La utilización de proceso de codificación para un mensaje PGP contempla similares características para el proceso de firmado de un documento por la clave privada de un usuario, la misma es desarrollada a continuación.

3.1.11. Firma Digital

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada

[28] Algunas implementaciones de PGP emplean otras fuentes de aleatoriedad, como ocurre con GnuPG, por lo que no necesitan almacenar una semilla aleatoria.

correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras dieron un lugar al concepto.

Pero, sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas, ya sea jurídica o real.

El fin, de la firma digital, es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado; y es por eso que a través de la legislación, se intenta acercarla, exigiéndose ciertos requisitos de validez. [CABRERA FEDERICO, ©2003]

Las firmas digitales son el objetivo del trabajo de grado y su análisis y estudio son necesarios para su utilización.

3.1.11.1. Ventajas de la Firma Digital

Gracias a la firma digital, los ciudadanos podrán realizar transacciones de comercio electrónico seguras y relacionarse con la Administración con la máxima eficacia jurídica, abriéndose por fin las puertas a la posibilidad de obtener documentos como la cédula de identidad, carnet de conducir, pasaporte, certificados de nacimiento, o votar en los próximos comicios cómodamente desde su casa.

El uso de la firma digital en el trabajo de grado va a satisfacer los siguientes aspectos de seguridad:

Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un

usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados. [CABRERA FEDERICO, ©2003]

A continuación se hace énfasis en sus aplicaciones de las firmas para el trabajo de grado.

3.1.12. Aplicaciones de Firmas Digitales

La firma digital se puede aplicar en las siguientes situaciones:

- **Transferencia en sistemas electrónicos**, por ejemplo si se quiere enviar un mensaje para transferir $100,000 de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los $100,000 por 1000,000,con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción
- **En aplicaciones de negocios**, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios
- **En sistemas legislativos**, es a menudo necesario poner un grupo fecha / hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha / hora electrónico se podría poner a los documentos en forma electrónica y entonces firmado usando al

DSA o al RSA. Aplicando cualquiera de los dos algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

- E-mail
- Contratos electrónicos
- Procesos de aplicaciones electrónicos
- Formas de procesamiento automatizado
- Transacciones realizadas desde financieras alejadas [MANUEL LUCENA, ©2005]
- En SITTEL servirá para la autentificación de usuarios en la transferencia de información en la red interna de SITTEL.

Determinado su utilización de la firma digital se hace hincapié en su funcionalidad.

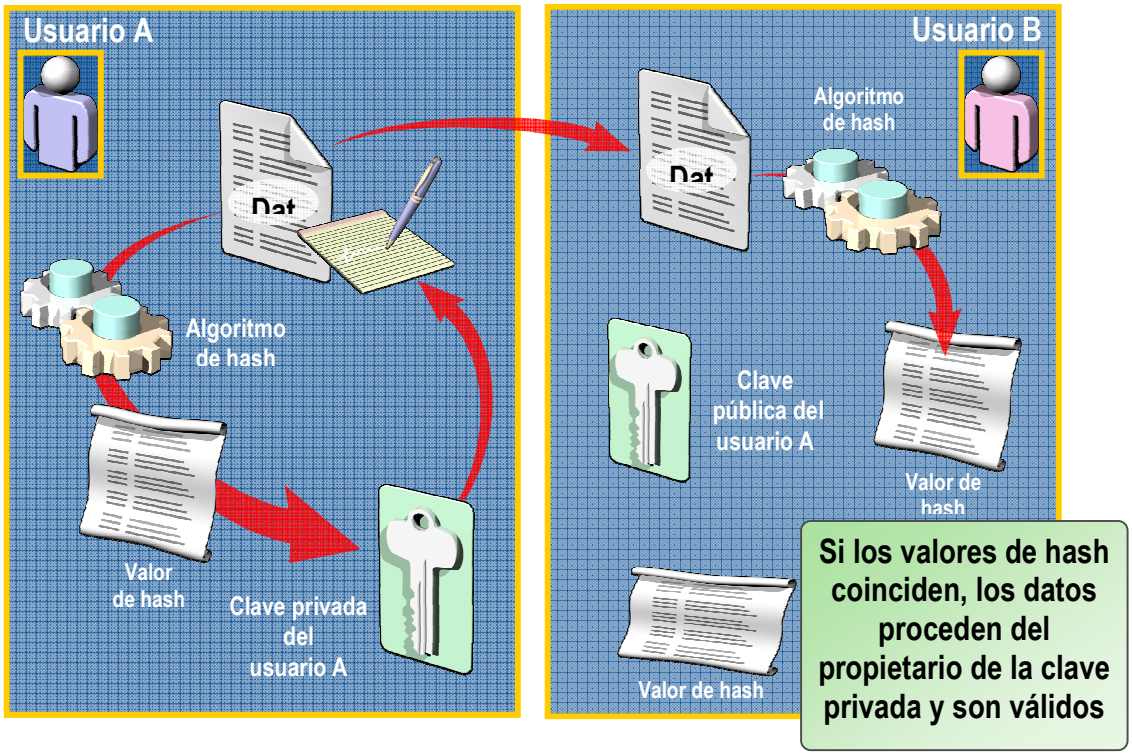
3.1.12.1. Funcionalidad de las Firmas Digitales

La firma digital (ver la figura 3.6) garantiza que los datos proceden de una parte concreta al crear una firma digital que es única de esa parte. Este proceso también utiliza funciones de hash. Por simplificar, las firmas digitales combinan el hash (para la validación de los datos de firma) con el cifrado asimétrico para codificar los datos de esa firma.

Cuando se firman datos con una firma digital ocurre lo siguiente:

1. Se aplica un algoritmo de hash a los datos para crear un valor de hash.
2. Se cifra el valor de hash con la clave privada del usuario A, creando así la firma digital.
3. Se envía al usuario B la firma digital y los datos.
4. Cuando se descifran datos firmados digitalmente ocurre lo siguiente:
5. El usuario B descifra la firma mediante la clave pública del usuario A y después recupera el valor de hash. Si la firma se puede descifrar, el usuario B sabe que los datos proceden del usuario A (o del propietario de la clave privada).
6. Se aplica el algoritmo de hash a los datos para crear un segundo valor de hash.
7. Se comparan los dos valores de hash. Si los valores de hash coinciden, el usuario B sabe que no se han modificado los datos. [MICROSOFT, ©2005]

Figura 3. 6: Funcionamiento de la Firma Digital



Fuente: Microsoft, ©2004

El almacenamiento de las claves utilizadas en la presente subsección, se realiza en dos carpetas denominadas SECRING.SKR para claves privadas y PUBRING.PKR para clavles públicas.

Al finalizar y entender su utilización, a continuación se hace énfasis en la gestión de claves y almacenamiento de las mismas.

Comprendido las características principales de las firmas digitales, se explica las posibles vulnerabilidades de las mismas.

3.1.12.2. Vulnerabilidades de PGP

Según todo lo dicho hasta ahora, parece claro que PGP proporciona un nivel de seguridad que nada tiene que envidiar a cualquier otro sistema criptográfico jamás desarrollado. ¿Qué sentido tiene de hablar de sus vulnerabilidades, si estas parecen no existir? Como cualquier herramienta, PGP proporcionara un gran rendimiento si se emplea correctamente, pero su uso inadecuado podría convertirlo en una protección totalmente inútil. Es por ello que parece interesante llevar a cabo una pequeña recapitulación acerca de las buenas

costumbres que harían de PGP nuestro mejor aliado, las cuales son desarrolladas a continuación:

- **Escoger contraseñas adecuadas**. Todo lo comentado anteriormente es valido para PGP.
- **Proteger adecuadamente los archivos sensibles**. Estos archivos serán, lógicamente, nuestros llaveros (anillos de claves) y el fichero que alberga la semilla aleatoria. Esta protección debe llevarse a cabo tanto frente al acceso de posibles curiosos, como frente a una posible pérdida de los datos (¡recuerde que si pierde el archivo con su clave privada no podrá descifrar jamás ningún mensaje).
- **Emitir revocaciones de nuestras claves al generarlas y guardarlas en lugar seguro**. Serán el único mecanismo valido para revocar una clave en caso de perdida del anillo privado. Afortunadamente, la versión 6 de PGP permite nombrar revocadores para nuestras claves, de forma que estos podrán invalidarla en cualquier momento sin necesidad de nuestra clave privada.
- **Firmar sólo las claves de cuya autenticidad estemos seguros**. Es la única manera de que las redes de confianza puedan funcionar, ya que si todos firmáramos las claves alegremente, podríamos estar certificando claves falsas. Al margen de un uso correcto, que es fundamental, debemos mencionar que ´ últimamente han sido detectados algunos fallos en las diversas implementaciones de PGP. Clasificaremos dichas vulnerabilidades en dos grupos claramente diferenciados.
- **Debidas a la implementación**: Estos agujeros de seguridad son provocados por una implementación defectuosa de PGP, y corresponden a versiones concretas del programa. Por ejemplo, el fallo descubierto en la versión 5.0 de PGP para UNIX, que hacía que las claves de sesión no fueran completamente aleatorias, o el encontrado en todas las versiones para Windows, desde la 5.0 a la 7.0.4, en la que un inadecuado procesamiento de las armaduras ASCII permitía a un atacante introducir ficheros en la computadora de la víctima.
- **Intrínsecas al protocolo**: En este apartado habría que reseñar aquellos agujeros de seguridad que son inherentes a la definición del estándar Open PGP. En este sentido, a principios de 2001 se hizo pública una técnica que permitiría a un atacante falsificar firmas digitales. En cualquier caso, se necesita acceso físico a la computadora de la víctima para manipular su clave privada, por lo que el fallo

carece de interés práctico, aunque suponemos que obligaría a una revisión del protocolo. [PGPI, ©2005]

Las vulnerabilidades descritas son utilizadas en el manual de usuario para evitar problemas con el criptosistema y para mayor seguridad de la autentificación de las firmas digitales se hará uso de las firmas y certificados digitales desarrollados a continuación.

3.1.13. Certificado Digital

Es un documento electrónico que proporciona al usuario un alto grado de confianza con una organización o persona con la que estén tratando. Se pueden utilizar cuatro tipos de certificaciones:

- *Certificaciones de una autoridad de certificación*. Una autoridad de certificación es una organización que proporciona certificados digitales. (ej. Canada Post Corporation y los servicios postales de US)
- *Certificaciones del servidor*. Estas certificaciones contienen datos tales como la clave pública del servidor, el nombre de la organización que posee el servidor y la dirección del servidor en Internet
- *Certificaciones Personales*. Estas son las certificaciones asociadas a un individuo. Contendrán información tal como la dirección del individuo junto con al información relacionada con la computadora como la clave publica y la dirección de correo electrónico de la persona.
- *Certificaciones del Editor de Software*. Estos son certificados que proporcionan confianza en que el software ha sido producido por una compañía de software específica. [ROGER PRESSMAN, ©2003]

En el presente trabajo se desarrollaran únicamente los **certificados personales** entre los certificados mencionados.

Entendido los certificados digitales, se detalla a continuación las aplicaciones de los mismos.

3.1.13.1. Aplicaciones de Certificados Digitales

Entre los usos frecuentes de los certificados se incluyen:

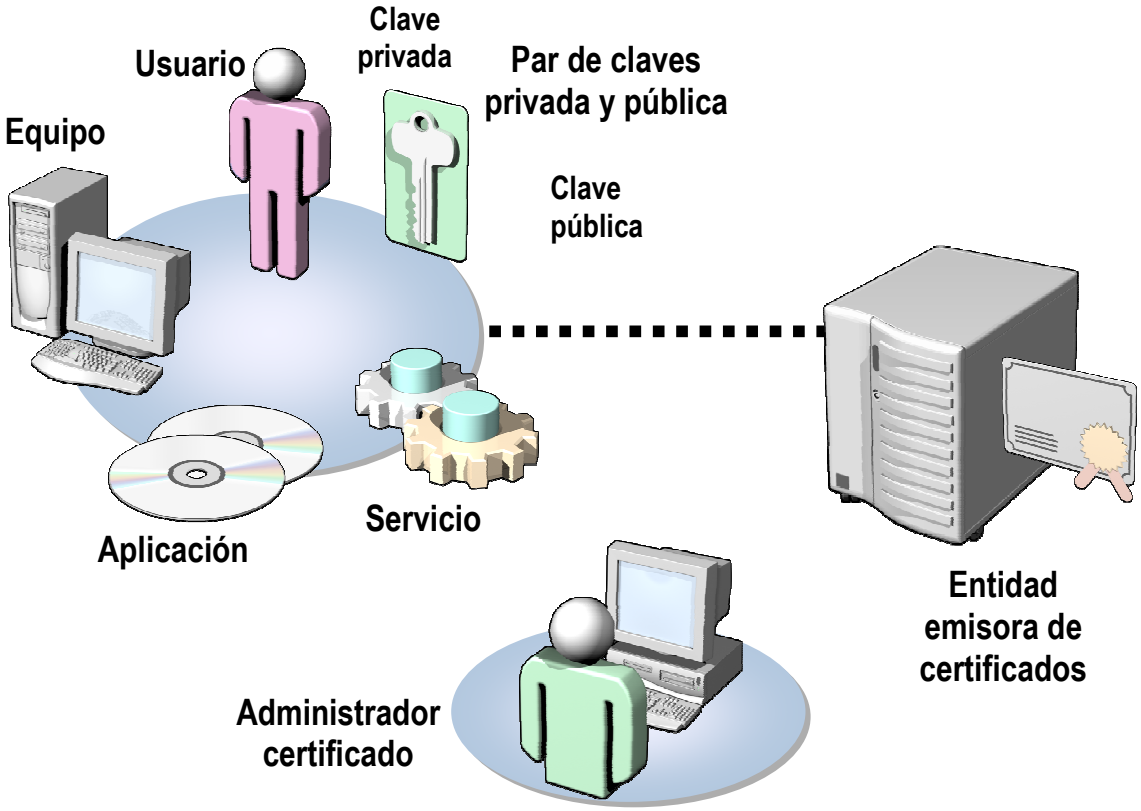
- Comunicación inalámbrica 802.1x
- Sistema de archivos de cifrado (EFS)

- Autenticación de Internet
- Seguridad IP (IPSec)
- Correo electrónico seguro
- Inicio de sesión mediante tarjeta inteligente
- Firma de código por software [MICROSOFT, ©2005]

Con el fin de entender la funcionalidad de los certificados Digitales, y su aplicación en SITTEL se explica a continuación su funcionamiento.

3.1.13.2. Funcionamiento de los Certificados Digitales

Figura 3. 7: Funcionamiento de los Certificados Digitales



Fuente: Microsoft, ©2004

Si bien las firmas digitales aseguran que los datos proceden de una parte que tiene acceso a una clave privada, no garantizan la identidad de dicha parte. Por ejemplo, un atacante podría haber obtenido una clave privada perteneciente a Microsoft. Entonces podría utilizar esa clave junto con un algoritmo de hash estándar para firmar unos datos,

lo que daría a entender que el origen de los datos es Microsoft. Un certificado digital (ver figura 3.7) impide este robo de la identidad electrónica al comprobar que la firma pertenece sin duda alguna al editor. Ahora es posible comprobar los datos y la firma como pertenecientes al editor autorizado porque la entidad emisora de certificados (CA) de confianza ha comprobado que el editor posee tanto la clave pública como la clave privada.

Con los certificados digitales tiene lugar el siguiente proceso:

1. Un usuario, equipo, servicio o aplicación crea el par de claves pública y privada.
2. La clave pública se transmite a la entidad emisora de certificados (**CA**) a través de una conexión de red segura.
3. El administrador certificado examina la solicitud de certificado para comprobar la información.
4. Para la aprobación, el administrador certifica la firma la clave pública con la clave privada de la CA y asegura su autentificación, caso contrario la rechaza y pone en consideración del usuario receptor de la llave que no la utilice. [MICROSOFT, ©2005]

Se determino el uso del estándar internacional **ITU X.509 S - Norma Internacional** para desarrollar de los certificados digitales y por que cumple con el funcionamiento anteriormente descrito.

3.1.13.3. ITU X.509 S

Esta Recomendación o Norma Internacional encargada de la Interconexión de Sistemas Abiertos y Autentificación de los mismos por certificado digital tiene el fin de:

- Indica la forma de la información de autenticación contenida por el directorio.
- Describe cómo puede obtenerse la información de autenticación a partir del directorio
- Enuncia los supuestos formulados en cuanto a la formación y al emplazamiento de esa información de autenticación en el directorio
- Define tres modos en los cuales las aplicaciones pueden usar esa información de autenticación para realizar la autenticación, y describe cómo otros servicios de seguridad pueden ser soportados por autenticación.

Esta Recomendación | Norma Internacional describe dos niveles de autenticación: autenticación simple, mediante el uso de una contraseña como verificación de una identidad pretendida, y autenticación fuerte, que implica credenciales formadas usando técnicas criptográficas. Si bien la autenticación simple ofrece cierta protección limitada contra el acceso no autorizado, sólo la autenticación fuerte debe servir de base para ofrecer servicios seguros. No se pretende con ello establecer un marco general para la autenticación; no obstante, puede ser de uso general para aplicaciones en que estas técnicas se consideran adecuadas.

La autenticación (y otros servicios de seguridad) sólo puede suministrarse dentro del contexto de una política de seguridad definida para una aplicación particular. Incumbe a los usuarios de una aplicación definir su propia política de seguridad, la cual puede verse constreñida por los servicios proporcionados según una norma.

Incumbe a las normas definir las aplicaciones que *usan* el marco de autenticación para especificar los intercambios de protocolo que necesitan ser realizados para lograr la autenticación basada en la información de autenticación del directorio. El protocolo usado por las aplicaciones para obtener la información de autenticación del directorio es el protocolo de acceso al directorio (DAP), especificado en la Rec. X.519 del CCITT | ISO/CEI 9594-5.

El método de autenticación fuerte especificado en esta especificación de directorio se basa en los criptosistemas de claves públicas. Es una gran ventaja de esos sistemas el que los certificados de usuario puedan estar contenidos en el directorio como atributos, y ser comunicados libremente dentro del sistema del directorio y obtenidos por los usuarios del directorio del mismo modo que otra información de directorio. Se supone que los certificados de usuario están formados por medios «fuera de línea», y que son introducidos en el directorio por su creador. La generación certificados de usuario la efectúa cierta autoridad de certificación «fuera de línea» que está completamente separada de los DSA en el directorio. En particular, no se imponen requisitos especiales a los suministradores del directorio para almacenar o comunicar certificados de usuario en una manera segura.

En general, el marco de autenticación no depende del uso de un determinado algoritmo criptográfico, siempre que tenga las propiedades descritas en 7.1. Es probable, en la práctica, que se use cierto número de algoritmos diferentes. Sin embargo, dos usuarios que quieran autenticar tienen que soportar el mismo algoritmo criptográfico para que la autenticación se realice correctamente. Así, dentro del contexto de un conjunto de

aplicaciones conexas, la elección de un algoritmo único servirá para maximizar la comunidad de usuarios capaces de autenticar y comunicar de manera segura.

Análogamente, dos usuarios que deseen autenticar tienen que soportar la misma función hash usada en la formación de credenciales y testigos (tokens) de autenticación)]. Aquí también, en principio, un número de funciones hash alternativas pudieran ser usadas, a expensas de reducir las comunidades de usuarios capaces de autenticar. [UIT. ©1998]

Planteadas las bases teóricas para el desarrollo de las firmas y certificados digitales a través de la criptografía, criptografía asimétrica, PGP, las firmas digitales, certificados digitales y la norma ITU X.509 S, se puede continuar con el desarrollo del Marco Teórico y Metodológico en la subsección de Ingeniería de Software.

3.2. Ingeniería de Software

La ingeniería de software es la aplicación de un enfoque sistemático, disciplinado y cuantificable al desarrollo, operación (funcionamiento) y mantenimiento del software; es decir, la aplicación de ingeniería al software. [Computer Society, ©1993].

3.2.1. Modelo de las 4P's

La gestión eficaz de un proyecto de software se centra en las cuatro P's: personal, producto, proceso y proyecto El orden no es arbitrario. El gestor que se olvida de que el trabajo de ingeniería de software es un esfuerzo humano intenso nunca tendrá éxito en la gestión de proyectos. Un gestor que no fomenta una minuciosa comunicación con el cliente al principio de la evaluación del proyecto arriesga as construir una elegante solución para un problema equivocado. El administrador que presta poca atención al proceso corre el riesgo de arrojar métodos técnicos y herramientas eficaces al vacío. El gestor que emprende un proyecto sin un plan sólido arriesga el éxito del producto.

Con el fin de aplicar al trabajo de grado se realizó un estudio de sus principales áreas que contempla, las cuales son el proyecto, personal producto y proceso desarrollados a continuación:

3.2.2. El Proyecto

Se orienta hacia la dirección del proyecto de software, se realiza la planificación y el control por fases, analizando su complejidad, con el fin de evitar el fracaso del proyecto, además se determina el proceder del gestor para el proyecto de software con los ingenieros de sistemas, con el fin de comprender los factores de éxito crítico que conduce a la gestión

correcta del proyecto y desarrollar un enfoque de sentido común para planificar, supervisar y controlar el proyecto.

3.2.3. El Personal

La necesidad de contar con personal para el desarrollo del software altamente preparado y motivado se viene discutiendo desde los años 60. De hecho el factor humano es tan importante que el instituto de Ingeniería de Software ha desarrollado un modelo de madurez de la capacidad de gestión del personal (MMCGP) “para aumentar la preparación de organizaciones del software para llevar a cabo las cada vez complicadas aplicaciones ayudando a traer, aumentar, motivar, desplegar y retener el talento necesario para mejorar su capacidad de desarrollo de software”

El modelo de madurez de gestión de personal define las siguientes áreas claves prácticas para el personal que desarrolla software: reclutamiento, selección, gestión de rendimiento, entrenamiento, retribución, desarrollo de la carrera, diseño de la organización y del trabajo cultural y de espíritu de equipo.

3.2.4. El producto

El software se ha convertido en el elemento clave de la evaluación de los sistemas y productos informáticos. En los pasados 50 años, el software ha pasado de ser una resolución de problemas especializada y una herramienta de análisis de información, a ser una industria por sí misma. Pero la temprana cultura e historia de la «programación» ha creado un conjunto de problemas que persisten todavía hoy. El software se ha convertido en un factor que limita la evolución de los sistemas informáticos. El se compone de programas, datos y documentos. Cada unos de estos elementos componen una configuración que se crea como parte del proceso de la ingeniería del software. El intento de la ingeniería del software es proporcionar un marco de trabajo para construir software con mayor calidad [PRESSMAN, ©2002].

Se hará uso de la concepción del producto de software en el trabajo de grado con el fin de presentar un software que cumpla los requisitos de la ingeniería de software, a continuación nos referimos al proceso para el desarrollo del producto software.

3.2.5. El proceso

La ingeniería de software es una disciplina que integra procesos, métodos y herramientas para el desarrollo del software de computadora. Se tiene varios modelos de proceso para la

ingeniería de software, cada uno exhibe ventajas e inconvenientes, pero todos tienen una serie de fases genéricas en común.

Entre los procesos de desarrollo de software tenemos:

- El Modelo Lineal Secuencial
- El Modelo de Construcción de Prototipos
- El Modelo DRA
- Modelos Evolutivos de Proceso del Software
    - El Modelo Incremental
    - El Modelo Espiral
    - El Modelo espiral WINWIN (Victoria & Victoria)
    - El Modelo de Desarrollo Concurrente
- Desarrollo Basado en Componentes
- El Modelo de Métodos Formales
- Técnicas de Cuarte Generación [PRESSMAN, ©2002]

Se utilizará el Modelo Lineal Secuencial por su facilidad, rapidez para el desarrollo y alta prestación para el producto software y la experiencia adquirida en el modelo.

3.2.6. El Modelo Lineal Secuencial

Conocido como Ciclo de Vida Clásico, es el método más utilizado por la ingeniería de software por su facilidad y alta prestación en el desarrollo del software.

El Modelo Lineal Secuencial es el conjunto de actividades que los analistas, diseñadores y programadores realizan para desarrollar e implantar un sistema de información, a continuación se especifica las etapas por las cuales esta compuesta el modelo:

A) Investigación preliminar: La solicitud para recibir ayuda de un sistema de información pueden originarse por una persona, cuando se formula la solicitud comienza la primera actividad del sistema. Esta actividad tiene tres partes:

a. Aclaración de la solicitud.

b. Estudio de factibilidad (Factibilidad técnica, Factibilidad económica, Factibilidad operacional)

c. Aprobación de la solicitud.

B) Determinación de los requisitos del sistema: Los analistas, al trabajar con los empleados y administradores, deben estudiar los procesos de una empresa para dar respuesta a ciertas preguntas claves. Para contestar estas preguntas, el analista conversa con varias personas para reunir detalles relacionados con los procesos de la empresa. Cuando no es posible entrevistar, en forma personal a los miembros de grupos grandes dentro de la organización, se emplean cuestionarios para obtener esta información.

C) Diseño del sistema (diseño lógico): El diseño de un sistema de información responde a la forma en la que el sistema cumplirá con los requerimientos identificados durante la fase de análisis. Es común que los diseñadores hagan un esquema del formato o pantalla que esperan que aparezca cuando el sistema esta terminado, se realiza en papel o en la pantalla de una terminal utilizando algunas de las herramientas automatizadas disponibles para el desarrollo de sistemas.

D) Desarrollo de software (diseño físico): Los encargados de desarrollar software pueden instalar software comprado a terceros o escribir programas diseñados a la medida del solicitante. La elección depende del costo de cada alternativa, del tiempo disponible para escribir el software y de la disponibilidad de los programadores. Los programadores son responsables de la documentación de los programas y de explicar su codificación, esta documentación es esencial para probar el programa y hacer el mantenimiento.

E) Prueba de sistemas: Durante esta fase, el sistema se emplea de manera experimental para asegurarse que el software no tenga fallas, es decir, que funciona de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga. Se alimentan como entradas conjuntos de datos de prueba para su procesamiento y después se examinan los resultados. En ocasiones se permite que varios usuarios utilicen el sistema, para que los analistas observen si tratan de emplearlo en formas no previstas, antes de que la organización implante el sistema y dependa de él. En muchas organizaciones, las pruebas son conducidas por personas ajenas al grupo que escribió los programas originales; para asegurarse de que las pruebas sean completas e imparciales y, por otra, que el software sea más confiable.

F) Implantación y evaluación: La implantación es el proceso de verificar e instalar nuevo equipo, entrenar a los usuarios, instalar la aplicación y construir todos los archivos de datos necesarios para utilizarla. Cada estrategia de implantación tiene sus méritos de acuerdo con la situación que se considere dentro de la empresa. Sin importar cuál sea la estrategia utilizada, los encargados de desarrollar el sistema procuran que el uso inicial del sistema se encuentre libre de problemas. Los sistemas de información deben mantenerse siempre al día, la implantación es un proceso de constante evolución [María Carmen Fernández, ©2000].

Consecuente al desarrollo del Modelo Lineal Secuencial que nos servirá para desarrollar el Modelo de la Aplicación para Administrar las Firmas y Certificados Digitales se hará uso de Métricas de Calidad garantizar la funcionalidad del software de acuerdo a los requisitos de SITTEL y mejorar la seguridad del software.

3.2.7. Métricas de Calidad

Las métricas del software proporcionan una manera cuantitativa de valorar la calidad de los atributos internos del producto, permitiendo por tanto al ingeniero valorar la calidad antes de construir el producto. Las métricas proporcionan la visión interna necesaria para crear modelos efectivos de análisis y diseño, un código solidó y pruebas minuciosas.

Para que sea útil en el contexto del mundo real, una métrica de software debe ser simple y calculable, persuasiva, consistente y objetiva. Debería ser independiente del lenguaje de programación y proporcionar una realimentación eficaz para el desarrollo del software.

Las métricas del modelo de análisis se concentran en función, de los datos y el comportamiento. El punto de función y la métrica *bang* proporciona medidas cuantitativas para evaluar el modelo del análisis. Las métricas del diseño consideran aspectos de alto nivel, del nivel de componentes y de diseño de interfaz. Las métricas de diseño de alto nivel consideran los aspectos arquitectónicos y estructuras del modelo de diseño. Las métricas de diseño de nivel de componentes proporcionan una indicación de calidad estableciendo medidas indirectas de la cohesión, acoplamiento y complejidad. Las métricas de diseño de interfaz proporcionan una indicación de la convivencia de la representación de una IGU.

La ciencia de software proporciona una intrigante conjunto de métricas a nivel de código fuente. Usando el número de operadores y operandos presentes en el código, la ciencia del

software proporciona una variedad de métricas que pueden usarse para valorar la calidad del programa.

Se determino el uso de las métricas técnicas para un empleo directo en las pruebas y mantenimiento del software. Sin embargo, se pueden emplear muchas otras métricas-técnicas para guiar el proceso de las pruebas y como mecanismo para valorar la facilidad de mantenimiento de un programa de computadora [www.symantec.com].

Dentro de la elección de métricas de calidad, se determino el uso de los Factores de Calidad de McCall y el ISO 9123 desarrollados a continuación:

3.2.7.1. Factores de Calidad de McCall

Los factores que afectan a la calida del software se pueden categorizar en dos amplios grupos:

(1) factores que se pueden medir directamente -por ejemplo, defectos por punto defunción

(2) factores que se pueden medir sólo indirectamente (por ejemplo, facilidad de uso o de mantenimiento)

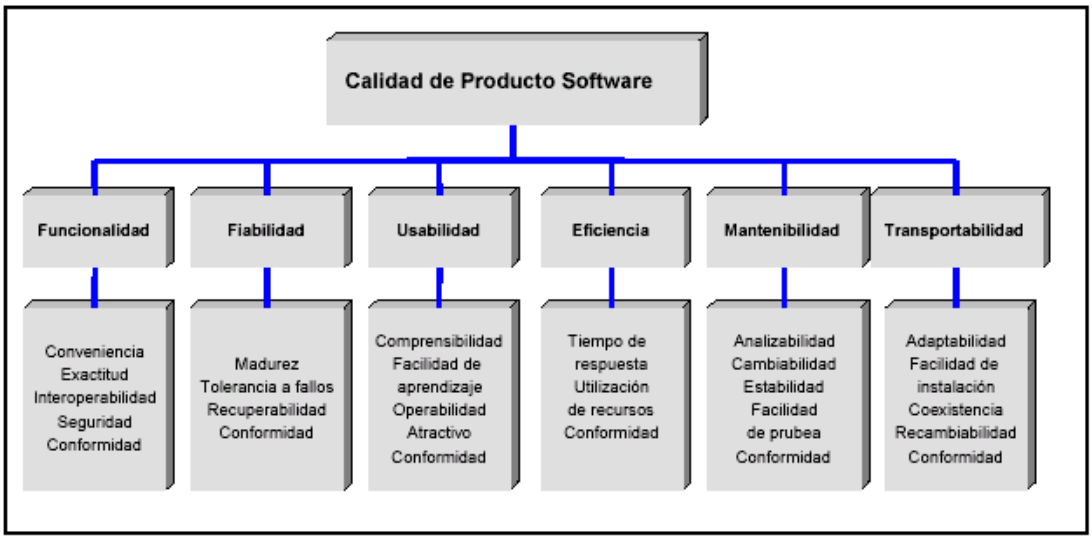
En todos los demás casos debe aparecer la medición. Debemos compara el software (Documentos, programas y datos) con una referencia y llegar a una conclusión sobre la calidad [www.symantec.com].

3.2.7.2. ISO 9126

Con el fin de garantizar la calidad del software se hará uso del estándar ISO 9126 que se define como la totalidad de características relacionadas con su habilidad para satisfacer necesidades o implicadas.

- Los atributos de calidad se clasifican según seis características, las cuales a su vez se subdividen en subcaracterísticas (ver figura 3.8).
- También se describen métricas de calidad del software basadas en atributos internos y en el comportamiento externo del sistema.
- En este estándar se establece que cualquier componente de la calidad del software puede ser descrito en términos de algunos aspectos de una o más de estas seis características. [Guido Rosales, ©2005]

Figura 3. 8: Calidad de un producto software (modelo ISO 9126)



Fuente: ISO 9126

Consecuentemente al uso de métricas para mejorar la calidad del software a ser implantado en SITTEL, se utilizara las herramientas Case para disminuir el tiempo de producción, el cual es desarrollado a continuación.

3.2.8. Herramientas Case

Las herramientas de ingeniería de software asistida por computadora abarcan todas las actividades del proceso del software y también aquellas actividades generales que se aplican a lo largo de todo el proceso. CASE[29] combinado con un conjunto de bloques de construcción que comienzan en el nivel de hardware y del software de sistema operativo y finalizan en las herramientas individuales.

Las categorías de las herramientas CASE abarcan tanto las actividades de gestión como las actividades técnicas, e incluyen la mayor parte de las áreas de aplicaciones del software. Todas las categorías de herramientas se han considerado para el proyecto de firmas y certificados digitales.

El entorno I-CASE combina mecanismos de integración para datos, herramientas e interacción hombre-computadora. La integración de datos se puede conseguir mediante el intercambio directo de información, mediante estructuras de archivos comunes, mediante datos compartidos o interoperatibilidad, o a través de la utilización de un repositorio I-CASE

completo. La integración de herramientas se puede diseñar de forma personalizada por parte de fabricantes que trabajan a la vez, o bien se puede lograr mediante un software de gestión que se proporcione como parte del repositorio.

La integración entre hombre y computadora se logra mediante estándares de interfaz que se están volviendo cada vez más comunes a lo largo y ancho de toda la industria. Para facilitar la integración de los usuarios con herramientas, de las herramientas entre sí, de las herramientas con datos y de los datos con otros datos se diseña una arquitectura de integración.

Se ha aludido al repositorio CASE con el nombre de «bus de software». La información pasa por él, y va circulando de herramienta en herramienta a medida que progresa el proceso del software. Pero el repositorio es mucho más que un «bus». También se trata de un lugar de almacenamiento que combina sofisticados mecanismos para integrar herramientas CASE mejorando consiguientemente el proceso mediante el cual se desarrolla el software. El repositorio es una base de datos relacional u orientada a objetos que es «el centro de acumulación y almacenamiento» de la información de ingeniería de software. [Kendall & Kendall, ©2001]

Descrita la metodología a ser empleada para el desarrollo del producto software (Producto, Proceso, Modelo Lineal Secuencial, Métricas de Calidad, McCall, ISO 9126, Herramientas Case), se pude continuar con el desarrollo del Marco Teórico y Metodológico en la Subsección Tercera de Auditoria de Seguridad de Sistemas desarrollada a continuación.

3.3. Auditoria de Seguridad de Sistemas

Una de las principales preocupaciones de las Entidades Públicas y Privadas que han realizado ingentes esfuerzos en la implementación de tecnologías de información, es la probabilidad de sus inversiones que han realizado no den soluciones inmediatas, tangibles y medibles; y allí donde se veía una oportunidad de mejora, realmente están creando un problema difícil de administrar, controlar y caro de mantener. La Auditoria de Seguridad de Sistemas se constituye en una herramienta que gestiona la tecnología de la información en las entidades, a través de auditorias internas y externas.

El presente trabajo propone una metodología de auditoria informática con la finalidad de medir los riesgos y evaluar los controles en el uso de las tecnologías de información,

[29] Computer Aided Software Engineering, traducido es: “Ingeniería de Software Asistida por Computadora”

haciendo uso de técnicas y estrategias de análisis, que permitan que la auditoria informática se convierta en una real y eficiente herramienta de gestión de tecnologías de información, a disposición de SITTEL.

A continuación se desarrolla la Auditoria de Sistemas y su metodología a través de las herramientas y dominios de la Norma Bolivia ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información aplicados en la Superintendencia de Telecomunicaciones.

3.3.1. Auditoria de Sistemas

Es auditor de sistemas debe tener la capacidad de definir las etapas y las técnicas que serán necesarias para la realización de la auditoria de manera óptima y cumpliendo las Normas de Auditoria de Sistemas y el Código de Ética Profesional.

Razón por la cual será utilizada la metodología de la Norma Boliviana ISO/IEC 17799 para la auditoria en los puntos que tienen relación con las firmas y certificados digitales. [NB-ISO-IEC 17799, ©2004]

Los dominios a ser evaluados en SITTEL para mejorar los niveles de seguridad son los siguientes:

3.3.1.1. Políticas de Seguridad

Objetivo: Verificar en SITTEL si existe dirección y apoyo gerencial para brindar seguridad de la información.

El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.

Se hará la revisión y evaluación a las políticas, procesos y procedimientos en el Departamento de Tecnologías de Información y Comunicación en SITTEL. [NB-ISO-IEC 17799, ©2004]

3.3.1.2. Organización de la Seguridad

Objetivo de la política de seguridad de la información: Se buscará administrar la seguridad de la información dentro de SITTEL.

Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de SITTEL a través de firmas y certificados digitales.

Debe establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de la seguridad de información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información.

Se definirá claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad. [NB-ISO-IEC 17799, ©2004]

3.3.1.3. Clasificación y Control de Activos

Objetivo de la Clasificación de la Información: Garantizar que los recursos de información de SITTEL reciba un apropiado nivel de protección.

La información debe ser clasificada para señalar la necesidad, la prioridad y el grado de protección. La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrán requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento espacial. [NB-ISO-IEC 17799, ©2004]

3.3.1.4. Seguridad del Personal

Punto muy importante en la seguridad del cual se obtiene los siguientes puntos:

1º Punto:

Objetivo de Capacitación del Usuario: Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, están capacitados para respaldar la política de seguridad de SITTEL en el transcurso de sus tareas normales.

Los usuarios deben estar capacitados en relación con los procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad.

2º Punto:

Objetivo de Respuestas a incidentes y anomalías en materia de seguridad: Minimizar el daño producido por incidentes y aprender de los mismos a través de planes de contingencia en SITTEL.

Los incidentes que afectan la seguridad deben ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible.

Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible, además de implementar controles necesarios en SITTEL para el correcto funcionamiento del mismo. [NB-ISO-IEC 17799, ©2004]

3.3.1.5. Control de Accesos

Objetivo de Gestión de Accesos de Usuarios: Impedir el acceso no autorizado a los sistemas de información en SITTEL.

Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.

Los procedimientos en ejecución deberán comprender todas las etapas del ciclo de vida de accesos de usuarios, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieran de acceso a los sistemas y servicios de información. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso privilegiado, que permiten a los usuarios pasar por alto los controles de sistema. [NB-ISO-IEC 17799, ©2004]

3.3.1.6. Desarrollo y Mantenimiento de Sistemas

Punto muy importante en la seguridad del cual se obtiene los siguientes puntos:

1º Punto:

Objetivo de Requerimiento de Seguridad de los Sistemas: Asegurar que la seguridad es incorporada a los sistemas de información en SITTEL.

Este incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas el analista de sistemas. Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados como una parte de la totalidad del caso de negocios de un sistema de información.

2º Punto:

Objetivo de Seguridad en los sistemas de aplicación: Prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación utilizados en SITTEL.

Se deben diseñar en los sistemas de aplicación, incluyendo las aplicaciones realizadas por el usuario. Controles apropiados y pistas de auditoria o registros de actividad. Esto debe incluir la validación de datos de entra, procesamiento interno y salida de datos.

3º Punto:

Objetivo de Controles Criptográficos: Proteger la confidencialidad, autenticidad o integridad de la información.

Deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se consideren en estado de riesgo y para la cual otros controles no suministran una adecuada protección. [NB-ISO-IEC 17799, ©2004]

3.3.1.7. Gestión de la Continuidad de los Negocios

Objetivo Aspectos de la Gestión de la Continuidad de los Negocios: Contrarrestar las interrupciones de las actividades de SITTEL y proteger los procesos críticos de SITTEL y de los efectos de fallas significativas o desastres posibles en la ciudad de La Paz y específicamente en SITTEL.

Se debe implementar un proceso de gestión de continuidad en SITTEL para reducir la interrupción ocasionada por desastres y fallas de seguridad a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio. Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de gestión.

La gestión de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables. [NB-ISO-IEC 17799, ©2004]

Consecuentemente se utilizará el Modelo P.H.V.A. para el desarrollo de la Auditoria de Sistemas por su facilidad de uso, experiencia ganada en los cinco años de estudio y por ser el más adecuado para la NB ISO/IEC 17799 por ser un sistema de gestión de calidad, en este caso de calidad de seguridad.

3.3.2. Modelo P.H.V.A.

El Ciclo PDCA es un concepto ideado originalmente por Shewhart, pero adaptado a lo largo del tiempo por algunos de los más importantes personajes del mundo de la calidad. [ISO 9001, ©2004]

El Ciclo PDCA básico se conoce comúnmente como el Círculo Deming. Consiste en una serie de cuatro elementos que se llevan a cabo consecutivamente:

Se le reconoce como metodología de cuatro fases: "Planificar-Hacer-Verificar-Actuar" (PHVA). No es más que un ciclo de mejora continua. Los primeros intentos por modelarlo quizás se pierdan en el tiempo. PHVA puede describirse en esencia como:

Planificar: establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente (ya sea interno o externo) y las políticas de la organización.

Hacer: implementar los procesos o actividades, considerando la educación y capacitación como requisito para seguir adelante con el ciclo.

Verificar: realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.

Actuar: ejecutar acciones para mejorar continuamente el desempeño de los procesos.

Figura 3. 9: Circulo de Deming – Modelo PHVA

Fuente: Microsoft, ©2004

Si bien, parece una sencillez, cuando se analiza el desempeño de muchas organizaciones, aflora el incumplimiento o la desviación de una, o varias, de las etapas establecidas por el ciclo PHVA. No es posible realizar con calidad actividad, proceso, producto o servicio alguno, si se viola alguno de los pasos del ciclo. Podría decirse que la metodología PHVA no da lugar a fisuras en cuanto su propósito: se define una meta y dejándose llevar por la sabiduría contenida en cada etapa, se llega a cumplirla quitando del camino los obstáculos (no conformidades) que se interpongan, ya sean humanos, materiales o financieros. Si el objetivo es realista y considera las variables del entorno, entonces siguiendo la estrategia del Ciclo de la Calidad, la probabilidad de éxito es mayor. No debe olvidarse que en cada paso habrá que realizar acciones tácticas y operativas para seguir adelante con dominio.

Durante todo este proceso, están presentes los indicadores e índices de gestión de cada área que deben estar alineados con sus respectivas unidades de negocio para lograr la efectividad de los objetivos estratégicos propuestos. [ISO 9001, ©2004]

Planteado las bases teóricas y metodológicas para el desarrollo de la auditoria de Sistemas (Auditoria de Sistemas, Norma Bolivia ISO 17799 para Sistemas de Gestión de Seguridad de Información, Norma P.H.V.A.) se describe a continuación las conclusiones del capítulo.

Conclusiones del Capítulo

Planteada todas las bases teóricas y metodológicas generales para el desarrollo de las firmas y certificados digitales, se concluye que:;

- Las firmas y certificados digitales están basados en la CRIPTOGRAFÍA Y SEGURIDAD de sistemas a ser utilizadas con el algoritmo de encriptación **PGP de 128 bits** o superior por su robustez.
- La ingeniería de software es la ciencia que nos ayudará en el desarrollo del PRODUCTO a través de un PROCESO LINEAL SECUENCIAL más conocido como Ciclo de Vida Clásico, utilizando una GESTIÓN ESTRATIFICADA para garantizar su culminación, ANÁLISIS Y GESTIÓN DEL RIESGO DEL SOFTWARE para evitar problemas probables en el desarrollo y utilizar contramedidas a las mismas, como también MÉTRICAS DE CALIDAD para asegurar la calidad y el cumplimiento del mismo

mediante el ISO 9126 Y MCCALL, para finalizar con la utilización de HERRAMIENTAS CASE para apresurar el desarrollo de las firmas y certificados digitales.

- Para finalizar se hará uso la AUDITORIA DE SEGURIDAD DE SISTEMAS mediante el ISO 17799 y tomando en cuenta los puntos más relevantes que fueron descritos anteriormente, para verificar si la utilización de FIRMAS Y CERTIFICADOS DIGITALES EN SITTEL **coadyuvó en mejorar** la seguridad interna en la transferencia de información.

Todos los conceptos desarrollados en el anterior capítulo se hacen uso a lo largo del capítulo de Ingeniería del Proyecto y el capítulo de Garantía de Calidad de Software, en los cuales son desarrollados el software de Firmas y Certificados Digitales.

Capítulo 4

Factibilidad del Proyecto

Si has construido un castillo en el aire, no has perdido el tiempo, es allí donde debería estar. Ahora debes construir los cimientos debajo de él."

George Bernard Shaw

Resumen

El éxito del proyecto está determinado por el grado de factibilidad que se presenta en cada una de las etapas, la posibilidad de desarrollar el producto se centra en la demostración de factibilidades Operativa, Técnica y Económica. El presente capítulo se centra en el desarrollo de las mismas.

La investigación de factibilidad de un proyecto consiste en descubrir cuales son los objetivos de la organización, luego determinar si el proyecto es útil para la empresa y si están alineados con sus objetivos.

La finalidad de la factibilidad debe contemplar los recursos disponibles o aquellos que la empresa pueda proporcionar, pues si se tomará recursos que la empresa no pudiera brindar el proyecto será irrealizable.

Al respecto SITTEL se cuenta con una serie de características tecnológicas que nos ayudarán a determinar la factibilidad del proyecto, los cuales serán limitadores del mismo. Estos moderadores son:

- Reducción de costos mediante la optimización o eliminación de recursos no necesarios como ser la reutilización de código de software.
- Integración de todas las áreas y subsistemas a través proyecto e-SITTEL.
- Actualización y mejoramiento de los servicios a clientes o usuarios a través de la implementación de sistemas por tecnología Web.
- Reducción en el tiempo de procesamiento y ejecución de tareas generando la reducción de gastos por tiempo y mejorando el tiempo de entrega de resultados.
- SITTEL utiliza plataforma Microsoft en sus diferentes versiones para el desarrollo de software.
- La aplicación esta orientada a ser desarrollada en tecnología Web.
- El software esta orientado a ser utilizado en el ámbito interno de SITTEL.

- SITTEL no cuenta con ningún sistema que le brinda autenticidad e integración en la información, por lo tanto no hay punto de comparación.

En concreto estas características coadyuvan a mejorar el rendimiento de SITTEL y a la vez son limitantes tecnológicas para el desarrollo del presente trabajo, porque en cualquier proyecto de software desarrollado para SITTEL deberá adecuarse a los moderadores descritos anteriormente.

Expuestas las características tecnológicas del objeto bajo estudio, a continuación se desarrolla el análisis de las tres factibilidades mencionadas y se presentan sus resultados:

4.1 Factibilidad Técnica

Se refiere a los recursos necesarios como herramientas, conocimientos, habilidades, experiencia, tecnológica que son necesarios para efectuar las actividades o procesos que requiere el proyecto. Generalmente nos referimos a elementos tangibles (medibles) a fin de que el proyecto considerare si los recursos técnicos actuales son suficientes o están en capacidad de complementarse.

De acuerdo a lo anteriormente expuesto se determinó analizar:

- Herramientas de Software Propietaria y Libre
- Conocimiento y Experiencia del Desarrollo del Software
- Hardware

Los mencionados puntos son desarrollados a continuación con el objetivo de comprobar la factibilidad técnica.

4.1.1 Herramientas de Software Propietario y Libre

Habiéndose revisado el software necesario para el desarrollo del producto se determino el uso del software propietario, con el fin de utilizar similar tecnología que utiliza SITTEL:

Tabla 4. 1: Software Propietario brindado por SITTEL

Nº	Software
1	Microsoft Visual Studio.NET con Licencia
2	Microsoft Visual Studio.NET Enterprice Architecture con Licencia
3	Microsoft Plataform SDK – February 2003 o superior Avaliable on MSDK

	con Licencia
4	Microsoft Incide ASP.NET Web Matrix
5	Microsoft Windows XP Professional con IIS V6
6	Microsoft SQL Server 2000 o Superior
7	Microsoft insede asp.Net Web Matrix
8	Microsoft Office 2003

Fuente: elaboración propia en base al Software Necesario para el Desarrollo del Producto

Con la finalidad de utilizar similar tecnología, se solicito que el Departamento de Tecnologías de Información y Comunicación brindará las licencias de funcionamiento de los siguientes productos detallados en la tabla 4.1, las cuales fueron entregadas por el mismo, para evitar el gasto de la compra de las mismas.

Con referencia a otros paquetes para el desarrollo del producto en la cual SITTEL no tuviera la licencia o fueran libres, se determino la utilización de los siguientes paquetes de software descritos en la tabla 4.2, de los cuales destacamos la utilización de versiones de prueba y utilización de herramientas case libres:

Tabla 4. 2: Software Libre

Nº	**Software**
1	DotNetNuke (Herramienta CASE)
2	DreamWeaver 2004 (Versión de Prueba)

Fuente: elaboración propia en base al Software Necesario para el Desarrollo del Producto

Se llega a la conclusión que **obtenidas las herramientas necesarias** para el desarrollo del proyecto se puede proseguir con el mismo para completar la Factibilidad Técnica.

4.1.2 Conocimiento y Experiencia del Desarrollo del Software

Para determinar el conocimiento adquirido en el software para el desarrollo del producto, se determinó en primera instancia verificar el nivel de complejidad de aprendizaje del producto y el lenguaje de programación a través del Modelo de Medidas por Características-Bases de Ingeniería de Software (**Property-based Software Engineering Measurement**) anexado en el inciso I.

La siguiente tabla 4.3 explica los niveles de complejidad que existe en los diferentes lenguajes de programación para desarrollar la Firma Digital:

Tabla 4. 3: Niveles de Dificultad del Lenguaje de Programación

NIVELES Y CALIFICACIÓN		
	Iniciación	0.20
	Básico	0.40
	Medio	0.60
	Avanzado	0.80
	Profesional/Experto	1.00

Orientación de Software
Aprendizaje

Temática
Programación

Fuente: Francisco Charte, Desarrollo de Aplicaciones en Windows y Linux

Consecuentemente con la anterior tabla se describe a continuación el nivel de dificultad que existe en el aprendizaje y utilización de los siguientes paquetes de software (ver tabla 4.4), obtenidos en PC Magazine:

Tabla 4. 4: Nivel de Dificultad de Aprendizaje y Utilización de los Paquetes de Software

Nº	Software	Dificultad de Aprendizaje
1	Microsoft Visual Studio.NET	Avanzado
2	Microsoft Visual Studio.NET Enterprice Architecture	Medio
3	Microsoft Plataform SDK	Medio
4	Microsoft Internet Information Server 6	Básico
5	Microsoft SQL Server 2000 o Superior	Medio
6	DotNetNuke	Medio
7	DreamWeaver 2004	Avanzado
8	Asp.Net y Microsoft inside asp.Net Web Matrix	Medio

Fuente: elaboración propia

Habiéndose catalogado el software a ser utilizado y su nivel de dificultad de aprendizaje y utilización, determinamos heurísticamente que nivel de aprendizaje y utilización necesitamos para el desarrollo del producto, el cual es descrito en la siguiente tabla 4.5:

Tabla 4. 5: Diferenciación de Conocimientos y Experiencia

Nº	Software	Conocimiento Necesario para el Desarrollo	P1	Conocimiento Adquirido	P2	P1-P2
1	Microsoft Visual Studio.NET	Medio	0.6	Bajo	0.4	0.2
2	Microsoft Visual Studio.NET Enterprice Architecture	Bajo	0.4	Iniciación	0.2	0.2
3	Microsoft Plataform SDK – February 2003 o superior Avaliable on MSDK	Bajo	0.4	Iniciación	0.2	0.2
4	Microsoft Internet Information Server 6	Medio	0.6	Medio	0.6	0.0
5	Microsoft SQL Server 2000 o Superior	Medio	0.6	Bajo	0.4	0.2
6	DotNetNuke	Medio	0.6	Bajo	0.4	0.2
7	DreamWeaver 2004	Avanzado	0.8	Avanzado	0.8	0.0
8	Asp.Net y Microsoft inside asp.Net Web Matrix	Medio	0.6	Bajo	0.4	0.2

Fuente: elaboración propia

De la tabla 4.5 se obtiene los siguientes resultados descritos en la tabla 4.6, en base a los valores de Nivel de Dificultad del Lenguaje de Programación adquiridos en los cinco años de estudio en la Escuela Militar de Ingeniería y el conocimiento necesario para el desarrollo del mismo:

Tabla 4. 6: Riesgo por Falta de Conocimiento y Experiencia

Nº	Software	P3 = P1-P2	Dificultad de Aprendizaje	Valor de Dificultad (VD)	Riesgo por Falta de Conocimiento R = P3 * VD
1	Microsoft Visual Studio.NET	0.2	Avanzado	0.8	0.16
2	Microsoft Visual Studio.NET Enterprice Architecture	0.2	Medio	0.6	0.12
3	Microsoft Plataform SDK	0.2	Medio	0.6	0.12

	– February 2003 o superior Avaliable on MSDK				
5	Microsoft SQL Server 2000 o Superior	0.2	Medio	0.6	0.12
6	DotNetNuke	0.2	Medio	0.6	0.12
8	Asp.Net	0.2	Medio	0.6	0.12

Fuente: elaboración propia en base a la Diferenciación entre el Conocimiento Necesario para el Desarrollo y el Conocimiento Adquirido

- En síntesis la interpretación de los resultados de la tabla 4.6 nos permite describir los procesos críticos por orden de importancia en la etapa del desarrollo del software:
  - Microsoft Visual Studio.NET Enterprice Architecture y Microsoft Plataform SDK – February 2003 o superior Avaliable on MSDK
  - Asp.Net y Microsoft SQL Server 2000 o Superior
  - DotNetNuke
- Establecer que el aprendizaje de Microsoft Visual Studio.NET tendrá que ser paralelo al Enterprice Architecture y al SDK por su importancia.
- Que para salvar cualquier problema con respecto al desarrollo, es aconsejable tomar cursos en Visual Studio.Net con Asp.Net.

Se llega a la **conclusión** que **medido el Nivel de Riesgo por Falta de Conocimiento y Experiencia** en la utilización de los programas para el desarrollo del Software **a través del Modelo de Medidas por Características-Bases de Ingeniería de Software**, y habiéndose asegurado el Riesgo por Falta de Conocimiento y Experiencia en los programas para el desarrollo normal del producto, se puede proseguir con el mismo para completar la Factibilidad Técnica.

4.1.3 Hardware

Comprenden los equipos físicos requeridos para el desarrollo del sistema, de los cuales describimos sus características obtenidos a partir de los requerimientos mínimos del software de desarrollo en la tabla 4.7.

Tabla 4. 7: Tabla de Hardware

Equipo	Descripción de Características	Se Tiene
Tres Computadores	➢ Pentium IV ➢ Procesador Intel 3.00 ➢ Tarjeta Madre Intel Original ➢ Tarjeta de Red 10/100 ➢ Tarjeta de Fax/Modem ➢ Tarjeta de Video Gforce 128 Mb ➢ Memoria RAM 512 ➢ Disco Duro MAXTOR 120 GB ➢ Combo Lector DVD/Quemador LITE-ON ➢ Lector LITE-ON ➢ Disquetera Mitsumi ➢ Combo Case con Mouse y Teclado ➢ Pantalla de 17'' Samsung	Si
Una Impresora	Canon Modelo PIXMA 1000 con una velocidad de 14 ppm y calidad de borrador	Si
Un Scanner	GENIUS de página completa, con resolución de 1200 dpi.	Si
Servidor	Servidor Web con soporte para Asp.Net y SQL Server 2000	Si

Fuente: Elaboración Propia con el Hardware Disponible SITTEL

- Las tres computadoras necesarias para el desarrollo del proyecto se tienen con características necesarias para el soporte al software de desarrollo, al igual que la impresora y scanner.
- El servidor será prestado por SITTEL a través del Dep. de Tecnologías de Información y Comunicación para probar el software en sus instalaciones.

Se llega a la **conclusión** que habiéndose **analizado el hardware necesario para el desarrollo normal del producto** y determinado la posibilidad de obtenerlo, se puede proseguir con el mismo para completar la Factibilidad Técnica.

4.1.4 Conclusión de Factibilidad Técnica

Habiendo analizados las herramientas a ser utilizadas, el conocimiento y la experiencia necesario y el hardware necesario para el desarrollo e implementación en SITTEL, se llega a la conclusión que en los tres casos no existen inconvenientes para llegar a desarrollar el mismo, porque en el caso de las herramientas se tienen al alcance, el conocimiento y la experiencia necesaria se adquirirán en el transcurso del desarrollo del proyecto de grado,

que es el fin de la tesis, adquirir conocimiento y ganar experiencia para enfrentar el mundo laboral.

En concreto es factible técnicamente porque se tienen los recursos necesarios para efectuar el desarrollo del software.

4.2 Factibilidad Operativa

Se refiere a la capacidad de todos aquellos recursos humanos donde interviene algún tipo de actividad (Procesos). Durante esta etapa se identifico todas aquellas actividades que son necesarias para lograr el objetivo, también se evaluó y determino todo lo necesario para llevarla a cabo.

Se identificaron las tres etapas principales en el desarrollo del proyecto de grado descritas a continuación:

- Auditoria de Sistemas
- Desarrollo del Producto
- Verificación de la Calidad del Producto

Los mencionados puntos son desarrollados a continuación con el objetivo de comprobar la factibilidad operativa.

4.2.1 Auditoria de Sistemas

El desarrollo de la Auditoria de Sistemas de Seguridad en SITTEL a través de la Norma Boliviana ISO 17799 nos ayudará a establecer la política y los objetivos de seguridad de la información de SITTEL, para el cual se necesito de un Auditor de Sistemas con práctica en el ISO 17799, el cual fue contratado y concluyo con la mencionada auditoria.

Se llega a la **conclusión** que **habiéndose contratado al auditor de sistemas con especialidad en la NB-ISO 17799 para la realización de la Auditoria de Sistemas en SITTEL** y finalizado la auditoria de sistemas, se puede proseguir con el mismo para completar la Factibilidad Operativa.

4.2.2 Desarrollo del Producto

Para el desarrollo del producto de Administración de Firmas y Certificados Digitales, se identificaron los siguientes módulos:

- Registro de Nuevos Usuarios
- Recuperación de Firma Digital

- Aplicación de Firma Digital a un archivo
- Obtención de Llaves Públicas
- Verificación de Certificado Digital
- Autentificación e Integridad de la Información

Para el cual se determino la contratación de tres personas con experiencia en programación asp.Net y diseño gráfico Web para el desarrollo del producto, respecto a la utilización de otros recursos se determino un lapso de cinco meses en que el equipo desarrollo el software.

Se llega a la **conclusión** que **habiéndose contratado a tres personas con experiencia en programación asp.Net y diseño gráfico Web** para el desarrollo del producto, se puede proseguir con el mismo para completar la Factibilidad Operativa.

4.2.3 Verificación de la Calidad del Producto

Para la verificación de la calidad del producto nos sirve para el desarrollo eficiente de software de calidad, y reduce el riesgo de incertidumbre del desarrollo de software (aplicada en la etapa de prueba y mantenimiento), de los cuales se identificaron los siguientes módulos para la aplicación de la verificación de la calidad del producto:

- Factores de Calidad de McCall y factores de Calidad ISO 9126
- Métricas de Calidad del Código Fuente

La verificación de la calidad del producto necesitó del equipo de tres personas con experiencia en Factores de McCall y Factores de Calidad del ISO 9126 solicitados en el desarrollo del trabajo de grado.

Se llega a la **conclusión** que **habiéndose contratado a tres personas con Experiencia en Factores de McCall y Factores de Calidad del ISO 9123 para la verificación de calidad del producto software**, se comprueba la factibilidad operativa del mismo respecto a la verificación de la calidad del producto.

4.2.4 Conclusión de Factibilidad Operativa

Habiendo realizado las factibilidades operativas en las tres etapas (Auditoria de Sistemas, Desarrollo del Producto y Verificación de la Calidad del Software) descritas anteriormente y haber probado la factibilidad operativa de las mismas, se llega a la conclusión que en tres casos no existen inconvenientes para llegar a desarrollar el mismo, por lo cual esta probado la factibilidad operativa.

Respecto a la organización y a los futuros usuarios existe un apoyo debido a que el sistema planteado protegerá su información de manera automatizada y rápida, el compromiso por la seguridad del programa a SITTEL.

4.3 Factibilidad Económica

Se refiere a los recursos económicos y financieros necesarios para desarrollar o llevar a cabo las actividades o procesos en SITTEL y/o para obtener los recursos básicos. Al respecto deben considerarse los costos del tiempo aplicado al proyecto, el costo de la realización y el costo de adquirir nuevos recursos.

Generalmente la factibilidad económica es el elemento mas importante ya que a través de el se solventan las demás carencias de otros recursos, es lo mas difícil de conseguir y requiere de actividades adicionales cuando no se posee.

Por otra parte nos muestra los costos asociados con el desarrollo del prototipo, de manera que si estos son elevados no se acepta el sistema propuesto, pero viendo desde el punto que la pérdida de información en los sistemas informáticos puede ocasionar gastos de recuperación de información que pueden ser prevenidos con el software de seguridad. La pérdida de la información en SITTEL se compararía con la pérdida de muchos años de trabajo y duplicación de esfuerzos por recuperarla o volver a generarla.

Sobre los mencionados puntos se trabajara en pos de probarlos y asegurar la factibilidad económica a través del siguiente Análisis de Costos.

4.3.1 Análisis de Costos

Para determinar el costo del desarrollo del proyecto en SITTEL se analizarán los siguientes puntos:

- Costo de Recopilación de Información
- Costo del Hardware
- Costo de las Licencias de Software
- Costo del Desarrollo del Producto
- Costo de la Capacitación y Soporte Técnico
- Costos de Auditoria de Sistemas

Los mencionados puntos son desarrollados a continuación con el objetivo de comprobar la factibilidad económica.

4.3.1.1 Costo de Recopilación de Información

La realización de la recopilación de información nos ayudo a hacer el análisis de factibilidad del proyecto en SITTEL tomando en cuenta:

- **Visitas a SITTEL:** Realización de 30 visitas aproximadamente a SITTEL para obtención de información necesaria para la realización del proyecto, con el valor de Bs. 6.00 por ida y vuelta.
- **Información por Internet en 8 meses de realización de la Tesis:** La utilización de Internet para la realización de la investigación correspondiente en el proyecto.
- **Suscripción a Seminarios y Cursos:** Participación en diferente cursos y seminarios para actualizarse en temas afines al proyecto de grado.

Con lo expuesto se realizo el análisis de costos descrito en la siguiente tabla 4.10.

Tabla 4. 8: Costos de Recopilación de Información

Detalle	Precio/Unidad	Cantidad	Costo en US$	Costo en Bs.
Visitas a SITTEL	6.00	30	22.25	180.00
Información por Internet (ADSL)	153.90	8	152.19	1231.20
Suscripción a Seminarios y Cursos	70.00	10	86.52	700.00
		TOTAL	**260.96**	**2111.20**

Fuente: Elaboración Propia

En su equivalente es US$. 260.96 a cambio de Bs. 8.09/US$ 1.00.

Se llega a la **conclusión** que **habiéndose analizado el costo de la recopilación de información y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.1.2 Costo del Hardware

La realización del análisis de costos del hardware ayuda a determinar el requerimiento necesario para el desarrollo y puesta en marcha del proyecto a partir de un sondeo de mercado (ver anexo I) respecto a los equipos descritos en la tabla 4.3. Comprenden equipos físicos los cuales fueron obtenidos a partir de los requerimientos mínimos de los diferentes software's utilizados para el desarrollo del producto (ver tabla 4.3).

Tabla 4. 9: Tabla de Costos Hardware

Equipo	Descripción de Características	Costo US$
Tres Computadores	➢ Pentium IV Procesador Intel 3.00 ➢ Tarjeta Madre Intel Original ➢ Tarjeta de Red 10/100 ➢ Tarjeta de Video Gforce 128 Mb ➢ Memoria RAM 512 ➢ Disco Duro MAXTOR 120 GB ➢ Combo Lector DVD/Quemador LITE-ON ➢ Lector LITE-ON ➢ Disquetera Mitsumi ➢ Combo Case con Mouse y Teclado ➢ Pantalla de 17'' Samsung	**Precio Unitario:** 850.00 **Total:** 2550.00
Una Impresora	Canon Modelo PIXMA 1000 con una velocidad de 14 ppm y calidad de borrador	50.00
Un Scanner	GENIUS de página completa, con resolución de 1200 dpi.	70.00
Servidor	Servidor Web con soporte para Asp.Net y SQL Server 2000	0.00
TOTAL		**2670.00**

Fuente: Elaboración Propia

En su equivalente es Bs. 21600.30 a cambio de Bs. 8.09/US$ 1.00.

Se llega a la **conclusión** que **habiéndose analizado el costo del hardware necesario para el desarrollo del producto software y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.1.3 Costo de Licencias del Software

La realización del análisis de costos de las licencias coadyuva a determinar la factibilidad de utilizar diferentes productos para el desarrollo del software. Con la finalidad de apoyar en el desarrollo del software por parte de SITTEL, el Departamento de Tecnologías de Información y Comunicación brindo las mismas, excluyendo del costo de las mismas.

En relación al producto Macromedia DreamWeaver se utilizó la versión de distribución libre.

Con el fin de reducir los costos se hace uso de programas de **Distribución Libre**, los cuales son descritos en la tabla 4.10:

Tabla 4. 10: Costos de Licencia de Software

Software	Descripción	Costo US$.
Microsoft Visual Studio.NET con Licencia	Software de desarrollo tecnología .NET, licencia entregada por SITTEL	Licencia entregada por SITTEL **0.00**
Microsoft Visual Studio.NET Enterprice Architecture con Distribución Libre	Software de desarrollo tecnología .NET	Distribución Libre **0.00**
Microsoft Plataform SDK – February 2003 o superior Avaliable on MSDK con Distribución Gratuita	Software de desarrollo tecnología .NET	Distribución Libre **0.00**
Microsoft Internet Information Server 6 con Licencia, incluida en Windows XP o superior	Software de desarrollo tecnología .NET que incluye Windows XP Professional, licencia entregada por SITTEL	0.00
Microsoft Office 2003	Word, Excel, PowerPoint	0.00
Microsoft SQL Server 2000 o Superior con Licencia	Base de Datos con soporte para asp.NET, licencia entregada por SITTEL	0.00
DotNetNuke con Distribución Libre	Manejador de Contenidos para Página Web, Herramienta CASE	Distribución Libre **0.00**
DreamWeaver 2004 con Distribución Libre	Herramienta de Diseño de Páginas Web con Soporte para asp.NET y SQL Server 2000, se bajo la distribución Triad	Distribución Libre **0.00**
	TOTAL	**0.00**

Fuente: Elaboración Propia

En su equivalente es Bs. 0.00 a cambio de Bs. 8.09/US$ 1.00.

Se llega a la **conclusión** que **habiéndose analizado el costo de las licencias para el desarrollo de software y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.1.4 Costo de Desarrollo de Software

La realización del análisis de costos del desarrollo de software coadyuva a determinar la posibilidad de desarrollar el producto, este se realizó a través del Modelo COCOMO que es un modelo empírico más completo para la estimación del software desarrollado por B. W. Boehm a finales de los 70[30]. COCOMO es una jerarquía de modelos de estimación de costes software que incluye submodelos básicos, intermedios y detallado (ver anexo J).

Para la estimación de este costo se utilizó:

- La ecuación de Putman, la misma que se usa para la estimación de las líneas de código (ver Anexo K).

$$L = C_K * K^{\frac{1}{3}} * td^{\frac{4}{3}} \qquad \textbf{Ecuación 4.1}$$

- COCOMO II en el modo Semi-Acoplado por la complejidad media del software y el tiempo de desarrollo como se explica en el anexo I.

Donde:

- C_K es una constante (2000, 8000, 11000), en el caso del sistema la constante es igual a **8000** para tener un buen entorno de desarrollo, contar con una documentación adecuada y un modo de ejecución interactivo.
- *K* es el esfuerzo, considerando un rango de 1 a 3, el esfuerzo es igual a 2 puesto que se tienen otras materias y paralelamente se termino la documentación del producto.
- *td* es el tiempo de desarrollo en años del sistema, de acuerdo al calendario académico de la Escuela Militar de Ingeniería, el tiempo aproximado del desarrollo del sistema son de 4 meses.

4 meses = 0.333 años

[30] Prentice-Hall, 1981

En primer lugar se obtiene la estimación de líneas de código del producto software, y para esto se hace uso de la Ecuación de Putnam que es la siguiente:

$$L = C_K * K^{\frac{1}{3}} * td^{\frac{4}{3}} \qquad \textbf{Ecuación 4.1}$$

Aplicando la ecuación 4.1 con los datos representados anteriormente se tiene lo siguiente:

$$L = 8000 * 2^{\frac{1}{3}} * 0.333^{\frac{4}{3}}$$
$$L = 2326.44 \cong 2326\, LCD$$

El sistema tiene un total aproximado de 2326 LCD (Líneas de Código).

A continuación se hace uso del Modelo COCMO II para conocer el tiempo total de Programación.

Las ecuaciones del COCOMO II son las siguientes:

$$\mathrm{E} = \mathrm{a_b} * (\mathrm{KLDC}) \exp(\mathrm{b_b}) \qquad \textbf{Ecuación 4.2}$$

$$\mathrm{D} = \mathrm{c_b} * (\mathrm{E}) \exp(\mathrm{d_b}) \qquad \textbf{Ecuación 4.3}$$

$$\text{Costo de desarrollo de Software} = \mathrm{E} * \text{Costo Relativo} \qquad \textbf{Ecuación 4.4}$$

Donde: E = El esfuerzo aplicado en personas/mes

KLDC = Es el número de líneas de código dividido entre 1000

D = Es el tiempo de desarrollo en meses

En primer lugar para el uso del Modelo COCOMO II, es necesario establecer el tipo de modo (orgánico, semiacoplado y empotrado - Ver Anexo I), de acuerdo a las características del Software este pertenece a un modo orgánico, ya que por el corto plazo para la conclusión del desarrollo del sistema, se espera que este sea un proyecto pequeño con un conjunto proa rígido de requisitos.

Como el sistema esta dentro del modo semiacoplado del COMO II, se tiene los siguiente datos constante (ver Anexo I).

$$aa = 2.4 \qquad bb = 1.05$$
$$cc = 2.5 \qquad dd = 0.38$$

Otro dato necesario para el desarrollo del Modelo es el resultado del número de líneas estimadas de Putnam (Ecuación 6.1) y se le expresa en miles de líneas de código:

KDLC = 2326 = 2.326 miles de líneas

Reemplazando en la ecuación 4.2 con los datos descritos anteriormente se tiene:

$$E = aa * (KLDC) \exp bb$$
$$E = 2.4 * (2.3626) \exp 1.05$$
$$E = 5.823 \cong 6\, programadores / mes$$

E = 6 prog/mes es el esfuerzo del Programador por mes

- Se reducirá a 3 prog/mes a través de la utilización de herramientas CASE:
  - Un Ingeniero de Sistemas
  - Un programador orientado a aplicaciones asp.Net
  - Un Programador orientado al diseño de aplicaciones Web incluyendo Diseño Gráfico.

Y haciendo uso de la ecuación 4.3 con datos del esfuerzo obtenido y las constantes de modo orgánico se tiene:

$$D = cc * (E) \exp\ dd$$
$$D = 2.5 * (6) \exp\ 0.38$$
$$D = 4.939 \cong 5\,(\text{Meses})$$

D = 5 meses es el lapso aproximado de duración del trabajo.

El costo de un programador con especialidad en asp.NET y SQL Server 2000 comprende funciones detalladas en la siguiente tabla (ver tabla 4.11) con sus costos respectivos:

Tabla 4. 11: Costos de Programador de Firmas y Certificados Digitales

Nº	Función	Costo US$.
1	Incorporación de PGP y obtención de las llaves públicas y privadas	10.00
2	Interfaz entre PGP y SQL Server 2000 para almacenar las llaves	8.00
3	Desarrollo del programa Hashing para las firmas Digitales	8.00
4	Desarrollo de la aplicación Firma Digital	11.00
5	Desarrollo del módulo de recuperación de Firmas Digitales	8.00
6	Desarrollo de la aplicación Certificado	7.00

	Digital	
7	Obtención de Llaves Públicas de Otros Usuarios	7.00
8	Verificación de la Autenticidad e Integridad de la Información	7.00
9	Acoplamiento de los módulos	7.00
10	Desarrollo de Interfaz Web y subir la página	7.00
	TOTAL	80.00

Fuente: Elaboración Propia

El costo promedio del programador por hora es de US$. 80/10 horas = US$. 8.00/Hora, equivalente en Bs. 64.72 a cada programador

Por lo tanto aplicando la **ecuación 4.4** se tiene el costo del programador, y las horas de trabajo por mes especificando en el siguiente párrafo.

Costo del Analista-Programador = US$.8.00/Hora

Horas de Trabajo Mes = 160 Hrs.

3 Meses * 160 Horas/Mes * 8.00 US$/Hora = US$ 3840.00/Analista-Progr.

Entonces el costo de desarrollar el software es:

E* US$. 3840.00= 3 Prog./Mes * US$.11520.00/prog. = US$.

Costo de Desarrollar el Software = US$. 11520.00

Se realizó también el cálculo sobre las etapas de Análisis, Diseño, Desarrollo del prototipo, tomando como base los supuestos anteriormente mencionados.

Etapa de análisis, investigación preliminar y recopilación de información:+

160 Hrs/mes * 0.5 Mes * 8.00 US$/Hora = **US$ 640.00**

Etapa de Diseño:

160 Hrs/mes * 0.5 Mes * 8.00 US$/Hora = **US$ 640.00**

Etapa de Prueba:

160 Hrs/mes * 1.0 Mes * 8.00 US$/Hora = **US$ 1280.00**

Los costos del desarrollo del software estimados se presentan en forma resumida en la tabla 4.12.

Tabla 4. 12: Costos de Desarrollo de Software

Etapa del Desarrollo	Duración (Meses)	Costos en US$
Investigación Preliminar y Análisis de Requerimientos	0.50	640.00
Diseño y obtención de Software de Desarrollo	0.50	640.00
Desarrollo del Prototipo	3.00	11520.00
Prueba y Mantenimiento	1.00	1280.00
Tiempo y Costo Total Personal	**5.00**	**14080.00**

Fuente: Elaboración Propia

En su equivalente es Bs. 113907.20 a cambio de Bs. 8.09/US$ 1.00.

Se llega a la **conclusión** que **habiéndose analizado el costo del desarrollo del producto software y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.1.5 Costo de la Capacitación y Soporte Técnico

La realización del análisis de costos de la Capacitación y Soporte Técnico vienen a significar uno de los problemas al desarrollar software, la dificultad se presenta cuando el software tiene que responder al tiempo y las evoluciones del software (sistemas operativos, entornos y tecnologías) tanto como el hardware.

Para lograr la factibilidad del proyecto se realizó en primera instancia el análisis del costo de la capacitación del personal de SITTEL respecto al software, con el resultado que la capacitación tendrá un costo de Bs. 0.00, a causa que el costo del desarrollo y soporte técnico cubrirán el mismo.

Referencia al soporte técnico, la actualización del software se ajusta al modo Semiacoplado del Modelo COCOMO II, como se aprecia en el Anexo I por ser un proyecto de complejidad mediana.

Para aplicar las ecuaciones del modelo COCOMO II, se ha considerado en función del prototipo:

- El prototipo se estima que tendrá 2326 líneas de código a través de la Ecuación 4.1.

- Se utilizará los valores del modelo semiacoplado.

$$aa = 2.4 \qquad bb = 1.05$$
$$cc = 2.5 \qquad dd = 0.38$$

Para la ecuación 4.2 se tiene:

$$E = aa * (KLDC) \exp bb$$
$$E = 2.4 * (200/1000) \exp 1.05$$
$$E = 0.44 \cong 1 prog/mes$$

E = 0.44 prog/mes es el esfuerzo del Programador, es decir que un programador puede desarrollar el soporte técnico en la mitad de tiempo.

Para la ecuación 2 reemplazando los valores se tiene:

$$D = cc * (E) \exp\ dd$$
$$D = 2.5 * (0.44) \exp\ 0.38$$
$$D = 1.83$$

D = 1.83 es el lapso aproximado de duración del trabajo en meses con un prog.

Por lo tanto aplicando la ecuación 3 se tiene el costo del programador, y las horas de trabajo por mes especificando en el siguiente párrafo.

Costo del Analista-Programador = US$. 8.00/Hora

Horas de Trabajo Mes = 160 Hrs.

1.83 Meses * 160 Horas/Mes * 8.00 US$/Hora * 0.44 Prog/Mes = US$ 1030.65 Progr.

Costo del Soporte Técnico del Software = US$. 1030.65 = Bs. 23742.72

En su equivalente es Bs. 8337.95 a cambio de Bs. 8.09/US$ 1.00.

Se llega a la **conclusión** que **habiéndose analizado el costo de la capacitación y soporte técnico y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.1.6 Otros Costos

El desarrollo de la Auditoria de Sistemas de Seguridad en SITTEL necesitó de un Auditor de Sistemas con práctica en el ISO 17799, el cual fue contratado y concluyo con la mencionada auditoria.

Se determino el costo de desarrollo de la Auditoria de Sistemas:

Tabla 4. 13: Costo de la Auditoria de Sistemas

Costo del Proyecto de Auditoria de Sistemas	US$.	Bs.
Material	12.36	100.00
Norma ISO 17799	20.89	169.00
Costo por 10 Horas de Trabajo en la Auditoria de Sistemas	52.00	420.68
TOTAL	**85.25**	**689.68**

Fuente: Elaboración Propia

Se llega a la **conclusión** que **habiéndose analizado el costo de la auditoria de sistemas y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.2 Costos Totales

Obteniendo la suma de los costos totales de hardware, licencias de software y mano de obra, se tiene la suma de inversión requerida para le desarrollo de la aplicación propuesta.

Tabla 4. 14: Costos Totales

Tipo	US$.
Costo de Recopilación de Información	260.96
Costo de Hardware	2670.00
Costo de Licencias de Software	0.00[31]
Costo de Desarrollo de Software	14080.00
Costo de Capacitación y Soporte Técnico	1030.65
Otros Costos	85.25
TOTAL	**18123.86**

Fuente: Elaboración Propia

[31] El costo de las licencias de software es de 0.00 por utilización de software libre y entrega de licencias por la Superintendencia de Telecomunicaciones.

Equivalente en Bs. 146622.03 al cambio de Bs. 8.09/US$. 1.00.

Se llega a la **conclusión** que **habiéndose realizado el análisis de costos y determinado que el mismo no representa un factor de complicación económica para el proyecto a través del análisis de mantenimiento anual de las firmas digitales** descrita en la Sección 4.3.2 de Comprobación de Factibilidad Económica, con lo expuesto se puede proseguir para completar la factibilidad económica.

4.3.3 Comprobación de Factibilidad Económica

El valor de la aplicación de Firmas y Certificados Digitales se desarrolla con el fin de obtener las firmas digitales a un valor menor del que se puede comprar.

Se estimo en el capítulo de generalidades que el costo anual de una firma digital es US$. 35.00, si se compraría 100 firmas digitales para SITTEL[32] el costo rebajaría a US$. 10.50 por firma digital.

100 Firmas Digitales * 10.50 US$./Firma Digital = US$. 1050.00

Para mantener anualmente el costo de las firmas digitales se tendría que tener un capital al 5% anual de:

$$\frac{US\$.1050.00}{0.05} = US\$.21000 \qquad \text{Ecuación 4.5}$$

El costo de mantener las firmas digitales infinitamente es de US$. 21.000, mucho mayor a lo estimado de **US$.18123.86 que es el costo del desarrollo del software**.

Otro de los beneficio de la aplicación son mantener la integridad de la información, autenticidad del origen del mensaje y apoyar en el desarrollo interno de SITTEL en el área de la seguridad de la información.

Se llega a la **conclusión** que **realizado la factibilidad económica** y **obtención de los costos totales** se demostró la misma.

Conclusiones del Capítulo

Comprobada la factibilidad técnica, operativa y económica, se determina que el proyecto es factible y en consecuencia puede ser desarrollado en el siguiente capítulo.

[32] Número estimado de personal trabajando en SITTEL

Capítulo 5

Ingeniería del Proyecto

"Todos los hombres son capaces de ver las tácticas por las cuales conquisto, pero nadie puede observar la estrategia a partir de la cual evoluciona la victoria."

Anónimo

Resumen

En el presente capítulo se desarrolla el producto como tal, las firmas y certificados digitales; para justificar su desarrollo se realizo una auditoria a SITTEL a través de la técnica que utiliza la ISO17799 “Tecnología de la Información: Seguridad de la Información”, consecuentemente desarrollamos el producto utilizando el Modelo Lineal Secuencial o más conocido como Modelo Clásico.

5.1. Auditoria a la Gestión de Seguridad de las Tecnologías de Información

Dado el concepto de Auditoria de Sistemas de Seguridad en la tercera sección del Capitulo de Marco Teórico y Metodológico, coadyuvado por la utilización de la herramienta ISO 17799 para la Gestión de la Seguridad de la Información descrita en la Sección 2.3 se concreta a continuación la utilización de las mencionadas herramientas en la determinación de la Evaluación de Riesgos y Contra riesgos en SITTEL.

Habiéndose aplicado los procedimientos de auditoria de sistemas en la Superintendencia de Telecomunicaciones a través del modelo PHVA (Planificar-Hacer-Verificar-Actuar) expuesto en el Marco Teórico y Metodológico y la Norma Internacional ISO/IEC 17799 con el objetivo de lograr la realización de la revisión de la organización del área de la Información y el cumplimiento del estándar de seguridad de información alineadas a la Norma Internacional ISO/IEC 17799 sobre Seguridad de las Tecnologías de Información, el cual fue cumplido y detallado a continuación.

Como resultado de los procedimientos aplicados en SITTEL se concluye que:

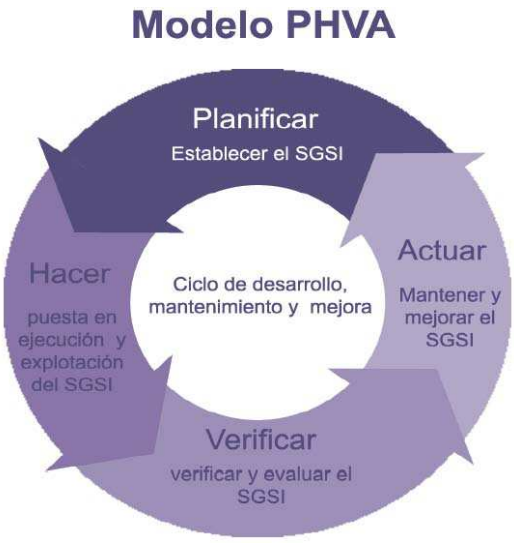
- Las políticas y normas para la Gestión Informática, Operaciones Informáticas, Seguridad Informática, Administración de Comunicaciones, Contratos con Proveedores y usuarios, no fueron definidas, formalizados ni implementadas.

- Por otro lado se ha evidenciado que no existen adecuadas herramientas para el control y monitoreo gerencial sobre las actividades del área de TI, así como la inexistencia de métricas de rendimiento y evaluaciones de satisfacción. Adicionalmente, no se tiene una planificación consensuada sobre las actividades de TI que reflejen las necesidades de las áreas usuarios.
- Además de no contarse con la definición e implementación de políticas y normas relacionadas al cumplimiento de la Norma Internacional ISO/IEC 17799.

Para facilitar la lectura del presente documento se detalla el resumen ejecutivo, el mismo ha sido estructurado de la siguiente manera a partir del modelo de Auditoria P.H.V.A. (ver figura 5.1):

Resumen Ejecutivo: Antecedentes y Planificación (Objetivo y Alcances) Hacer (Consideraciones Generales), Verificación (Conclusión General), Actuar (Conclusiones Específicas, Resumen de Recomendaciones), modelo el cual es utilizado para el desarrollado de la sección de Auditoria de Sistemas.

Figura 5.1: Estructura del Modelo PHVA



Fuente: Microsoft Corporation

Descrito la Estructura del Modelo P.H.V.A., se puede proseguir con el Resumen Ejecutivo.

5.1.1. Antecedentes

El presente trabajo ha sido enmarcado dentro del alcance señalado en las necesidades del desarrollo de las firmas y certificados digitales en SITTEL.

SITTEL cuenta con un personal permanente de aproximadamente 100 personas las cuales se dividen en las áreas de Dirección Jurídica, Intendencia Regulatoria (Dirección de Fiscalización y Defensor del Consumidor, Dirección de Regulación Económica, Dirección de Regulación Técnica y Derechos) y Intendencia de Planificación y Control de Gestión (Director de Administración y Finanzas, Director de Planificación y Desarrollo (Dirección de Acceso y Servicio Universal, Dpto. de Normas Políticas y Dpto. de Tecnologías de Información y Comunicación) y Responsable de Correspondencia y Registro). La máxima autoridad ejecutiva es el Superintendente, quien depende del Superintendente General establecido por el Gobierno Nacional de Bolivia.

El Departamento de Tecnologías de Información y Comunicación cuenta con la estructura organizacional conformada por el Jefe de Tecnología de Información y Comunicación, Analista de Redes y Comunicación, Administrador de Base de Datos y Analista de Información quienes tienen asignadas sus funciones y distribuyen tareas de apoyo a producción.

SITTEL cuenta con un plan de Negocios que abarca un año y se asemeja a un Plan Operativo, el mismo que ha influido en que no se cuente con los objetivos claramente definidos sobre el apoyo que debe brindar la tecnología al negocio.

El sistema principal de SITTEL es e-SITTEL, desarrollado por el Dpto. de TIC de SITTEL con el fin de converger las telecomunicaciones e informática bajo una sola plataforma tecnológica, a fin de lograr trasformaciones en los procesos productivos y de gestión de las organizaciones.

- La **visión** de e-SITTEL es lograr desarrollar hasta el año 2005 los instrumentos tecnológicos necesarios para mejorar los procesos involucrados en la regulación del sector de telecomunicaciones.
- Su **misión** de e-SITTEL es prestar servicios de regulación a los ciudadanos, las empresas y el gobierno.

El soporte técnico y mantenimiento del Sistema se encuentra a cargo del Dpto. de TIC.

Asimismo, es importante mencionar que el área de TIC cuenta con Políticas, normas y procedimientos internar aprobados por su personal.

Con lo cual se concluye que habiéndose determinado la misión y visión de e-SITTEL, principal sistema de la Superintendencia de Telecomunicaciones, se puede proseguir con la planificación de la Auditoria de Sistemas.

5.1.2. Planificación

El fin de la planificación fue establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos de SITTEL (ya sea interno o externo) y las políticas de la organización respecto a la seguridad de la información.

Objetivos

Realizar una auditoria de sistemas a la SITTEL con la NB-ISO-IEC 17799 con el fin de obtener los niveles de seguridad de información actuales y después de haber implementado el software.

Efectuar un análisis de los sistemas de información de SITTEL, trabajo que estuvo enfocado a la evaluación de los aspectos detallados alcance (ver el siguiente punto), identificando aspectos susceptibles de mejora y generando recomendaciones para que SITTEL subsanar los aspectos identificados.

Alcances

Alcances Geográficos

El trabajo fue realizado en la Superintendencia de Telecomunicaciones ubicada en la ciudad de La Paz, en la Calle 13 N° 8280 y 8260 en la Zona de Calacoto.

Alcance Técnico

Como parte de la Auditoria, se realizaron las siguientes tareas:

A) Revisión de Controles Generales sobre la Seguridad de la Información

Política de Seguridad

- Evaluación de las políticas de seguridad de la información definidas para la administración de la seguridad de SITTEL.

Organización y Administración de la Seguridad:

- Evaluación de la Organización, administración y política de seguridad.
- Evaluación de Normas para el Desarrollo y Mantenimiento de Sist. Y evaluación de Normas para la seguridad del personal.

Clasificación y Control de Activos

- Evaluación de la clasificación de la Información.

Seguridad Personal

- Evaluación a la capacitación a los usuarios
- Evaluación a respuestas a incidentes y anomalías en Materia de Seguridad.

Seguridad Física - Estrategia de Seguridad Física

- Evaluación de normas de seguridad física y ambiental.

Gestión de Comunicaciones y Operaciones

- Evaluación a la protección contra software malicioso.

Control de Accesos

- Evaluación de la administración de accesos a usuarios.

Desarrollo y Mantenimiento de Sistemas

- Evaluación de los Controles Criptográficos

Plan de Contingencia o Plan de Continuidad del negocio (PCN)

- Desarrollo, Prueba del PCN, conocimiento, entrenamiento del personal en el PCN y mantenimiento y actualización del PCN.

Cumplimiento

- Evaluación para la implantación de la NB ISO/IEC 17799.

B) Evaluación del Grado de Cumplimiento de la Normativa Internacional ISO/IEC 17799 sobre la Gestión de la Seguridad de la Información en Función de la Aplicación de Firmas y Certificados Digitales

Se llega a la **conclusión** que **planificado la auditoria de sistemas en base a la NB ISO/IEC 17799**, se logro los objetivos y alcances necesarios para proseguir y completar la Auditoria de Sistemas en su fase de Hacer.

5.1.3. Hacer

Se realizo la implantación de los procesos y actividades, considerando la educación y capacitación del plantel de SITTEL, requisito para seguir adelante con el ciclo a través de las siguientes Consideraciones Generales y el Enfoque del P.H.V.A. del estado actual del

Sistema de Gestión de la Seguridad de Información en SITTEL, obteniéndose las siguientes consideraciones:

Consideraciones Generales

Las medidas que permitirán alinearse en mayor medida a la Normativa Internacional ISO/IEC 17799 sin perder la percepción de la realidad y las necesidades propias, dichas medidas se basan en los hallazgos surgidos de la ejecución del presente trabajo. De este modo, SITTEL obtendrá una visión clara de su problemática, comprendiendo las relaciones causa-efecto existentes entre los hallazgos obtenidos, por lo cual es imprescindible que SITTEL alinea sus políticas a la Norma Boliviana ISO/IEC 17799.

Enfoque del P.H.V.A.

Como mencionamos, la adaptación y monitoreo del proceso de planeación ayuda al uso del modelo P.H.V.A. (Planear, Hacer, Verificar y Actuar), siempre y cuando se constituyan en un proceso cíclico, es decir, que se planee, se toma una acción, se verifique si los resultados eran los esperados y se actúe sobre dichos resultados para reiniciar el proceso.

El P.H.V.A. dinamiza la relación entre el hombre y los procesos y busca su control con base a su establecimiento, mantenimiento y mejora de estándares.

El control se define como todas las actividades necesarias para alcanzar eficiente y económicamente todos los objetivos a largo plazo y como se puede observar la planificación estratégica de sistemas es un factor crítico de éxito para la adecuada administración de los recursos tecnológicos y de la información dentro de una organización.

Se llega a la **conclusión** que **habiéndose desarrollado las Consideraciones Generales y el Enfoque del P.H.V.A.** para la aplicación de la Norma Boliviana ISO/IEC 17799, se puede proseguir con la fase de Verificación del Modelo P.H.V.A. para completar la Auditoria de Sistemas en la Superintendencia de Telecomunicaciones.

5.1.4. Verificar

La verificación fue la realización del seguimiento y la medición de los procesos y los productos respecto a las políticas de seguridad y los requisitos para mejorar los procesos de certificación de la seguridad de la información, e información sobre los resultados, de los cuales fueron acoplados el siguiente informe respecto a al obtención de los Dominios de

Riesgos en SITTEL, obtenidos a través de la implantación del Sistema de Gestión de la Información en SITTEL a través de la Norma Internacional ISO/IEC 17799:

A continuación se desarrolla la aplicación de la Norma Bolivia ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información de la Superintendencia de Telecomunicaciones:

5.1.5. Aplicación de la Norma Boliviana ISO 17799

La Norma Internacional ISO/IEC 17799 tiene por objetivo "proporcionar una base común para la elaboración de las normas de seguridad de las organizaciones, un método de gestión de la seguridad y establecer informes de confianza en las transacciones y las relaciones entre empresas". [CALLIO, ©2004].

La utilización de la Norma está dirigida a cualquier tipo de empresas, pero su aplicación se encuentra determinada por el tamaño de la empresa, ver tabla 5.1:

Tabla 5. 1: Dirección del ISO 17799

Tipo de Empresa	Tamaño	Objetivo Principal	Utilización de la Norma
Pequeña Empresa	Inferior a 200 empleados	Sensibilizar a la dirección general de la seguridad de la información	La norma ISO 17799 contiene los temas de seguridad que deben tratarse como base de gestión
Empresa Mediana	Inferior a 1000 empleados	Crear una cultura de seguridad global compatible	La Norma contiene las prácticas necesarias para constituir una política de seguridad de información
Empresa Grande	Superior a 1000 empleados	Obtener una certificación de seguridad	Utilización de la BS7799-2 para crear un documento referencial de seguridad interno

Fuente: CALLIO, ©2004

Consiguientemente se desarrolla el Sistema de Gestión de Seguridad de la Información (SGSI) para el tipo de Pequeña Empresa porque SITTEL cuenta con no mas de 150 empleados, de los cuales aproximadamente 100 empleados tienen interacción con el Sistema e-SITTEL.

Para su aplicación de la Norma se determino los siguientes pasos:

A) **Evaluación de Riesgos en SITTEL:** Diagnosticar el nivel de conformidad de la Norma Internacional sobre “Gestión de la Seguridad de la Información ISO/IEC 17799”. Hacer un inventario y evaluar los activos que deben protegerse y evaluar las amenazas y vulnerabilidades.

B) **Administración de Riesgos de la Organización:** Conocer cómo la selección y la implantación de los controles permitan reducir los riesgos a un nivel aceptable para la organización.

C) **Formalización y Sensibilización:** Los empleados pueden ser un eslabón débil en la cadena de seguridad de una organización. Aprender a crear un verdadero programa de sensibilización de la seguridad de la información.

D) **Preparación para la Auditoria:** Como validar de gestión y que hacer antes de la llegada de un auditor externo para la certificación NB ISO 17799.

Los mencionados puntos son desarrollados a continuación con el objetivo de realizar la Auditoria de Sistemas de Seguridad.

A) EVALUACIÓN DE RIESGOS EN SITTEL

La tabla 5.2 muestra los dominios desarrollados por los expertos del ISO/IEC 17799 que sirve para clasificar e identificar los riesgos con mayor posibilidad de ocurrencia en el objeto bajo estudio, en nuestro caso el objeto de estudio es la Superintendencia de Telecomunicaciones.

En las columnas de Recursos de TI (Tecnología de Información) se analizan los recursos tecnológicos más importantes en las organizaciones y en las columnas de Criterios de Información se analizan la pertinencia respecto a la disponibilidad de información en cualquier instante, integridad de la información en la transferencia y almacenamiento de la misma, y confidencialidad de la información ante diferentes problemas que pueden existir.

- En las columnas de criterios de información se tomaron en cuenta dos de los tres puntos: Integridad y Disponibilidad.
- En las columnas de recursos de TI se tomó en cuenta a los Datos como principal recurso en peligro.
- Haciendo un análisis de cada dominio (fila por fila) con los anteriores puntos, se coloco una x en donde estos coadyuvan a mejorar la seguridad en SITTEL.

Tabla 5. 2: Obtención de Dominios a Auditar

			Criterios Infor			Recursos de TI				
			Confid.	Integridad	Dispon.	RRHH	Sist. Apl.	Tecno.	Instal.	Datos
Dominio	**CODIGO**	**Proceso**								
Políticas de Seguridad	**PS1**	**Politicas de la seguridad de la información**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Organización de la Seguridad	**OS1**	**Infraestructura de la Seguridad de la Información**			x	x			x	
	OS2	Seguridad frente al acceso por parte de terceros	x							
	OS3	Tercerización	x							
Clasificación y Control de Activos	**CCA1**	Responsabilidad por rendición de cuentas de los activos	x							
	CCA2	**Clasificación de la Información**	x		x					
Seguridad del Personal	**SP1**	Seguridad en la definición de puestos de trabajo y la asignación de recursos								
	SP2	**Capacitación al usuario**	x	x	x					
	SP3	**Respuesta a incidentes y anomalías en materia de seguridad**	x	x	x		x			
Seguridad Física y Ambiental	**SFA1**	Areas seguras			x					
	SFA2	Seguridad del equipamiento								x
	SFA3	**Controles Generales**		x			x			
Gestión de Comunicaciones y Operaciones	**GCO1**	Procedimientos y responsabilidades operativas			x					
	GCO2	Planificación y aprobación de sistamas			x					
	GCO3	**Protección contra el software malicioso**	x	x			x			
	GCO4	Mantenimiento			x		x			
	GCO5	Gestión de la red	x	x	x					
	GCO6	**Gestión y seguridad de los medios de almacenamiento**	x	x						x
	GCO7	**Intercambios de información y software**		x	x		x			
Control de Acceso	**CA1**	Requerimientos de negocio para el control de accesos	x		x					
	CA2	Gestión de accesos de usuarios			x		x			
	CA3	**Responsabilidades del usuario**		x			x			
	CA4	Control de acceso a la red	x							
	CA5	Control de acceso al sistema operativo	x		x					
	CA6	**Control de acceso a las aplicaciones**	x				x			
	CA7	Monitoreo del acceso y uso de los sistemas	x							
	CA8	Computación móvil y trabajo remoto	x		x					
Desarrollo y Mantenimiento	**DMS1**	**Requerimientos de seguridad de los sistemas**		x			x			
	DMS2	Seguridad en los sistemas de aplicación	x		x		x			
	DMS3	**Controles Criptográficos**	x	x	x					x
	DMS4	**Seguridad de los archivos del sistema**	x	x	x					x
	DMS5	Seguridad de los procesos de desarrollo y soporte		x	x		x			x
Gestión de la Continuidad de los Negocios	**GCN**	**Aspectos de la gestión de la continuidad de los negocios**	x	x	x		x			x
Cumplimiento	**C1**	Cumplimiento de requisitos legales	x							
	C2	Revisiones de la política de seguridad y la compatibilidad técnica	x	x						
	C3	**Consideraciones de auditoria de sistemas**	x	x	x		x			x

Fuente: Guido Rosales Uriona, ©2005

- Para finalizar un dominio se habilita para ser auditado si obtiene una x en las columnas de Recursos TI y en las columnas de Criterios de Información.

Con lo cual se llega a la conclusión que **habiéndose realizado la evolución de los Riesgos en SITTEL e identificado los mismos en la Tabla 5.2**, se diagnosticó que el nivel de conformidad respecto al ISO/IEC 17799 es bajo por tener muchos dominios de presumible inconformidad e identificamos las amenazas y vulnerabilidades en SITTEL a través del Modelo de Evaluación de Riesgos, con lo cual se puede proseguir con la Administración de Riesgos en la Organización para completar con la Auditoria de Sistemas en la Superintendencia de Telecomunicaciones.

B) ADMINISTRACIÓN DE RIESGOS DE LA ORGANIZACIÓN

A través de la tabla del ISO 17799 (ver tabla 5.2), se obtuvo los dominios a ser analizados, evaluados y auditados en SITTEL los cuales son:

a) POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - PS1

CONTROL: El nivel gerencial deberá establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una Política de la seguridad de la información en SITTEL.

b) INFRAESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN - OS1

CONTROL: Se deberá establecer un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de SITTEL.

c) CLASIFICACIÓN DE LA INFORMACIÓN - CCA2

CONTROL: La información deberá ser clasificada para señalar la necesidad, la prioridad y su grado de protección.

d) CAPACITACIÓN DEL USUARIO - SP2

CONTROL: Los usuarios deberán estar capacitados en relación con los procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad.

e) RESPUESTA A INCIDENTES Y ANOMALÍAS EN MATERIA DE SEGURIDAD - SP3

CONTROL: Los incidentes que afectan la seguridad deberán ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible.

f) CONTROLES GENERALES - SFA3

CONTROL: Las instalaciones de procesamiento de información y la información deberá ser protegida contra la divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños.

g) PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO - GCO3

CONTROL: Se tomara precauciones para prevenir y detectar la introducción de software malicioso.

h) GESTIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO - CGO6

CONTROL: Los medios de almacenamiento deberán ser controlados y protegidos físicamente.

i) INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE - CGO7

CONTROL: Los intercambios de información y software entre SITTEL y organizaciones deberán ser controlados, y deberá ser consecuente con la legislación.

j) RESPONSABILIDADES DE USUARIO - CA3

CONTROL: La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad. Se deberá concienciar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

k) CONTROL DE ACCESO A LAS APLICACIONES - CA6

CONTROL: Las herramientas de seguridad deberán ser utilizadas para limitar el acceso dentro de los sistemas de aplicación. El acceso lógico al software y a la información deberá estar limitado a los usuarios autorizados.

l) REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS - DMS1

CONTROL: Incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por el usuario.

m) CONTROLES CRIPTOGRÁFICOS - DMS3

CONTROL: Perdida de confidencialidad, autenticidad o integridad de la información.

n) SEGURIDAD DE LOS ARCHIVOS DE SISTEMA - DMS4

CONTROL: Se debe controlara el acceso a los archivos del sistema.

o) ASPECTOS DE LA CONTINUIDAD DE LOS NEGOCIOS - GCN1

CONTROL: Se deberá implementar un proceso de gestión de la continuidad de los negocios para reducir la interrupción ocasionada por desastres y fallas de seguridad a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

p) CONSIDERACIONES DE AUDITORIA DE SISTEMAS - C3

CONTROL: Deberán existir controles que protejan los sistemas de operaciones y las herramientas de auditoria en el transcurso de las auditorias de sistemas.

Con lo cual se llega a la **conclusión** que **habiéndose dado a conocer la selección de riesgos en contra de la seguridad de la información y su correspondiente control para reducir el nivel de impacto en SITTEL**, se prosigue con la formalización y sensibilización del riesgo en la fase de verificación.

C) FORMALIZACIÓN Y SENSIBILIZACIÓN

Se realizó dos actividades relevantes en SITTEL con el fin de determinar el nivel de riesgo de seguridad de la información, la primera es la revisión de la documentación para la seguridad de la información y la segunda es el cuestionario obtenido en base a la administración de riesgos en SITTEL:

i. Revisión de documentación respecto a los dominios auditados de los cuales se determino que SITTEL tiene:
    a. Plan de contingencias
    b. Distribución de cargos para diferentes actividades relacionadas a la seguridad de la información.
    c. Manuales y Normas para el ingreso y salida de ordenadores.

ii. Cuestionario al Jefe del Departamento de Tecnologías de Información y Comunicación en SITTEL para identificar otras debilidades (ver tabla 5.3).

El cuestionario se obtuvo a partir de los dominios obtuvimos en la tabla 5.2 del ISO/IEC 17799 para los Sistemas de la Gestión de la Seguridad de la Información y se determinó que el cuestionario será de preguntas abiertas. Se calificó positivo si se acerca al resultado, caso contrario será negativo, además

a. Las preguntas están basadas en las recomendaciones de los dominios.
b. La calificación de cada pregunta esta en base a la cantidad de preguntas correspondientes al dominio.

A continuación se observa en la tabla 5.3 el cuestionario[33] llenado por el Jefe del Dpto. de Tecnologías de Información y Comunicación de la Superintendencia de Telecomunicaciones:

Lea y responda las preguntas

Tabla 5. 3: Cuestionario Realizado a SITTEL

COD	Pregunta	Respuesta
1	¿SITTEL tiene un plan de contingencias?	Si
2	¿Quién es el encargado de actualizar el plan de contingencia?	La jefatura JTI
3	¿Cada cuanto se brinda a los empleados un curso de seguridad o actualización de la misma?	Cada cambio
4	¿Su documentación de Seguridad de Sistemas prohíbe la utilización de software malicioso y virus?	Si
5	¿Tienen un responsable en Seguridad de la Información?	No
6	¿Quién es el responsable en Seguridad de la Información?	La jefatura JTI
7	¿Tuvo incidentes en seguridad de la Información en SITTEL?	NO
8	¿Puede mencionar algún incidente reciente?	No aplica
9	¿Quién aprueba las principales iniciativas para incrementar la seguridad de la información?	Jefe TIC
10	¿Se clasifico la información por prioridades, necesidades y el grado de protección?	SI

[33] El cuestionario con las respuestas correctas se encuentra en el Anexo P, el mismo indica de donde se obtiene las preguntas a través del código en la columna izquierda (dominio de la Norma Bolivia ISO/IEC 17799), y en la columna derecha se encuentra la respuesta correcta con la cual es comparada el presente cuestionario llenado por SITTEL para su valoración.

11	¿Si la respuesta 10 es positiva, donde esta descrita la clasificación?	En el análisis de riesgos.
12	¿Quién es el responsable de publicar información por medios escritos y por su página Web?	Responsables o dueños de la información
13	¿Se tiene procedimientos para el manejo adecuado de la información?	Si
14	¿Qué procedimiento se maneja para el envió de información por correo electrónico?	NO se tiene
15	Los empleados de SITTEL reciben alguna capacitación respecto a las amenazas e incumbencias en materia de seguridad de la información.	Si
16	¿Qué responsabilidades legales se enseñan a los empleados?	Normas internas informáticas
17	En caso de incidentes con la seguridad de la información, cual es el procedimiento formal de comunicación	Incluido en Plan de Contingencias
18	¿Existe procedimientos de feedback para garantizar la notificación de los resultados en incidentes con los empleados?	Si
19	¿Se registran los incidentes en algún documento?	Si
20	¿Se tiene políticas de escritorios y pantallas limpias?	No se tiene
21	¿Existe procedimientos para el manejo de información sensible o confidencial?	Si
22	¿Las terminales (PC, impresoras y otros) son controladas por cerraduras de seguridad cuando no están en uso?	No
23	¿Existe procedimientos para el ingreso y salida de equipos?	Si
24	¿Dónde se encuentran los procedimientos de retiro de bienes para empleados de SITTEL?	Es un formulario
25	¿Se tiene documentación sobre tipo de cuentas de usuario y cuentas de usuarios de los empleados de SITTEL?	Si
26	¿Quién esta encargado de instalar y desinstalar software en las máquinas de SITTEL?	El Analista de Redes y Comunicaciones
27	¿Se tienen cerrados los puertos de transferencia de archivos con redes externas?	Si
28	¿Qué medios de almacenamiento masivo son utilizados en SITTEL?	Discos duros, CDs, Cintas
29	¿Quién es el encargado de manejar los medios de	El Analista de Redes y

	almacenamiento masivo en SITTEL?	Comunicaciones
30	¿Existe procedimientos de eliminación de medios informáticos?	No
31	¿El ambiente donde es almacenado los medios de información concuerda con las especificaciones de los fabricantes o proveedores?	No se tiene
32	¿Se utiliza log's de auditoria en SITTEL?	Si
33	¿La información que es transmitida por que sistema de encriptación es protegida?	No se tiene
34	¿Qué nivel de confianza recíproca recibe el usuario y SITTEL con respecto a la identidad alegada por cada uno de ellos?	No se tiene
35	¿Existe control de acceso de usuarios remotos a las cuentas de correo electrónico?	Si
36	¿Se hace uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos?	No
37	¿Cuándo se crea un nuevo usuario, se notifica al usuario que debe mantener su contraseña en secreto?	si
38	¿Cada cuanto tiempo el sistema pide actualizar la contraseña?	3 meses
40	¿Qué características tiene la contraseña de ingreso a una computadora personal en SITTEL?	Mas de 6 caracteres – alfanumérica
41	¿En caso de máquinas o bases de datos compartidas, que precauciones se toman?	Se asignan permisos de accesos a los usuarios
42	¿SITTEL que medios de seguridad física tiene en sus instalaciones?	Guardias, rejas, etc.
43	¿Existe documentación respecto a la sensibilidad de los sistemas de aplicación?	Si
44	¿Cuándo una aplicación sensible a ejecutarse en un ambiente compartido, que procedimiento de seguridad se aplica?	Permisos de usuario
45	¿Quién otorga privilegios a los usuarios para el acceso a las bases de datos compartidas en SITTEL?	El Analista de Tecnologías de Información
46	¿Existe procedimientos para el diseño y desarrollo de Sistemas?	Si
47	¿Qué sistemas de validación de datos de entrada se manejan en SITTEL?	No se tiene
48	¿Qué sistemas y técnicas criptográficas son utilizados para proteger la información que se	Ninguna

	considera en estado de riesgo y para la cual otros sistemas no suministran una adecuada protección?	
49	¿Existe políticas sobre el uso de controles criptográficos para la protección de la información de SITTEL?	No
50	¿Cómo determino usted el nivel apropiado de protección criptográfico?	No aplica
51	¿Qué normas de seguridad implemento para el proceso del negocio de SITTEL?	Plan de contingencia
52	¿Qué sistemas utiliza para asegurar la autenticidad e integridad de la información?	Ninguno
53	¿Qué recaudos se toman para proteger las claves de los usuarios en SITTEL?	Certificados de 6 meses de duración.
54	¿Existe en SITTEL políticas de No Repudio?	No
55	¿Qué procedimiento de control de acceso a los sistemas de aplicación en operación se tiene?	Procedimiento de Control de accesos a Sistemas de Información
55	¿Existe procedimientos para la instalación de un servidor de datos en SITTEL?	Si
56	¿Se tiene un plan de Gestión de Continuidad de Negocios?	No
57	¿Quién es el encargado de actualizar el plan de Continuidad de Negocios?	No aplica
58	¿Se tiene estimado la perdida económica por una interrupción por fallas de equipos, inundaciones e incendios en SITTEL?	Si
59	¿Se probo los planes de Continuidad de Negocios?	No
60	¿Se hicieron auditorias de sistemas?	1 vez
61	¿SITTEL tiene un auditor interno?	Si
62	¿Quién es el auditor de sistemas en el Dpto. de TIC?	No se tiene

Fuente: Elaboración Propia

Con el fin de calificar el cuestionario respondido por la Lic. Amparo Subieta en la tabla 5.3 se compara con un cuestionario con las respuestas correctas en el Anexo P y haciendo una breve revisión de las respuestas a continuación se determinó cual es la probabilidad que un riesgo que se produzca con lo cual se arma la siguiente tabla (5.4) de Respuestas Correctas.

Tabla 5. 4: Tabla de Respuestas Correctas

CODIGO	Nº PREGUNTAS	Preguntas Positivas	%	Preguntas Negativas	%	Probabilidad del Riesgo
SP	4	3	75.00	1	25.00	2
OS	**5**	**3**	**60.00**	**2**	**40.00**	**3**
CCA	5	4	80.00	1	20.00	2
SP	**5**	**2**	**60.00**	**3**	**40.00**	**3**
SFA	**5**	**3**	**60.00**	**2**	**40.00**	**3**
GCO	3	2	66.67	1	33.33	2
CGO	**9**	**4**	**44.44**	**5**	**55.56**	**3**
CA	**8**	**5**	**62.50**	**3**	**37.50**	**2**
DMS	**11**	**2**	**18.18**	**9**	**81.82**	**5**
CGN	4	3	75.00	1	25.00	2
C	3	3	100.00	0	0.00	0

Fuente: Elaboración Propia

La puntación de la probabilidad es determinada a través de la siguiente medida:

- Preguntas Negativas en porcentaje de 0% = 0 de Prob. De Riesgo.
- Preguntas Negativas en porcentaje de 1%-19% = 1 de Prob. De Riesgo.
- Preguntas Negativas en porcentaje de 20%-39% = 2 de Prob. De Riesgo.
- Preguntas Negativas en porcentaje de 40%-59% = 3 de Prob. De Riesgo.
- Preguntas Negativas en porcentaje de 60%-79% = 4 de Prob. De Riesgo.
- Preguntas Negativas en porcentaje de 80%-100% = 5 de Prob. De Riesgo.

El significado de la Probabilidad de Riesgo debe ser entendida como se describe a continuación:

5 Inexistente: Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.

4 Inicial. Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos informales que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.

3 Repetible. Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay

capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

2 Definida. Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

1 Administrada. Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.

0 Optimizada. Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. La Tecnología de la Información se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

Con las respuestas se determino la siguiente tabla (ver tabla 5.5), donde se observa la probabilidad de Riesgo obtenida en la anterior tabla 5.4 e incumplimiento de objetivos obtenidos del ISO/IEC 17799 a través del impacto determinado en SITTEL:

Tabla 5. 5: Tabla de Riesgos

						1-5	1-5	
N	**CR**	**Objetivo**	**Debilidad**	**Recomd.**	**Acción**	**Probabilidad de Riesgo (PR)**	**Impacto en SITTEL (IS)**	**R=PR*IS**
1	4	PS1	PS1	PS1	-	2	2	**4**
2	3	OS1	OS1	OS1	-	3	4	**12**
3	5	CCA2	CCA2	CCA2	-	2	2	**4**
4	**2**	**SP2**	**SP2**	**SP2**	**A3**	**3**	**5**	**15**
5	3	SP3	SP3	SP3	-	3	3	**9**
6	5	SFA3	SFA3	SFA3	-	3	2	**6**
7	4	CGO3	CGO3	CGO3	-	2	3	**6**
8	5	CGO6	CGO6	CGO6	-	2	2	**4**
9	5	CGO7	CGO7	CGO7	-	2	2	**4**
10	3	CA3	CA3	CA3	-	2	4	**8**
11	4	CA6	CA6	CA6	-	2	2	**4**
12	**1**	**DMS1**	**DMS1**	**DMS1**	**A1**	**5**	**4**	**20**
13	**1**	**DMS3**	**DMS3**	**DMS3**	**A2**	**5**	**5**	**25**
14	3	DMS4	DMS4	DMS4	-	5	3	**15**

15	4	GCN1	GCN1	GCN1	-	2	3	**6**
16	4	C3	C3	C3	-	0	3	**0**

Fuente: Guido Rosales, ©2005

Tabla 5. 6: Valoración de Riesgos

Evaluación de Riesgo en SITTEL	**1**	**Muy Bajo**
	2	**Bajo**
	3	**Medio**
	4	**Alto**
	5	**Muy Alto**

Fuente: Elaboración Propia

En la anterior tabla 5.5 se realiza una multiplicación de la Probabilidad del Riesgo del dominio determinado con el anterior cuestionario y el Impacto que tendría en SITTEL cuando el riesgo se materialice, además se adjunto una tabla con la valoración del Riesgo (**R**) descrito en la tabla 5.6.

Con los resultados obtenidos se analizo la probabilidad de ocurrencia y el cumplimiento de objetivos, llegando a las siguientes conclusiones en la tabla 5.7 donde describimos los posibles problemas, se determino por colores siendo el rojo el de **Mayor Riesgo** y el Verde Claro el de **Menor Riesgo**.

Tabla 5. 7: Tabla de Riesgos

		Riesgos				
		5	**4**	**3**	**2**	**1**
IMPACTO	**5**	**DMS3**		**SP2**		
	4	**DMS1**		**OS1**	**SGO3-CA3**	
	3	**DMS4**		**SP3**	**GCN1**	
	2			**SFA3**	**PS1-CCA2-SGO6 SGO7-CA6**	
	1					**C3**

Fuente: Elaboración Propia

En la tabla 5.8 se describen de manera esquemática los problemas con Mayor Riesgo de probabilidad de Ocurrencia e Impacto en SITTEL, quienes describen la necesidad de implementar una herramienta que coadyuve a la transferencia segura de información en SITTEL.

Tabla 5. 8: Tabla de Objetivos

C	Importancia	Nivel	CR
Muy Alto	De 20 a 25	Muy Alto	DMS3
Alto	De 16 a 20	Alto	DMS1-SP2-DMS4
Medio	De 11 a 15	Medio	SP3-SGO3-CA3

Bajo	De 06 a 10	Bajo	SFA3-PS1-CCA2-SGO6-SGO7-CA6
Muy Bajo	De 01 a 05	Muy Bajo	C3

Fuente: Elaboración Propia

El riesgo en la seguridad de la información y con mayor probabilidad de ocurrencia fue:

- DMS3 – Controles criptográficos

Con la cual se determino que SITTEL necesita la implantación de Controles Criptográficos.

Se llega a la **conclusión** que **habiéndose sensibilizado los riesgos a ser auditados para el cumplimiento del objetivo del proyecto**, se puede proseguir con la preparación de la Auditoria de Sistemas en la fase de verificación.

D) Preparación para la Auditoria de Sistemas

A fin de desarrollar con mayor facilidad la auditoria, se realizarán acciones frente a los riesgos presentados en la sección anterior, los cuales son descritos a continuación:

A1. Acción frente al Riesgo de la Seguridad de la Información en los Requerimientos de Seguridad de los Sistemas

- **Política de utilización de controles criptográficos.**

  Las comunicaciones de requerimientos comerciales para nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de controles. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Se deben aplicar consideraciones similares al evaluar paquetes de software para aplicaciones comerciales. Si se considera adecuado, la administración puede querer utilizar productos certificados y evaluados en forma independiente.

  Los requerimientos de seguridad y los controles deben reflejar el valor comercial de los recursos de información involucrados y el potencial daño al negocio que pudiere resultar por una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo.

  Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Se llego a la conclusión que dichos controles fueron revisados a la terminación del producto o software, determinándose el contra riesgo ante la perdida de seguridad en la sección 6.3 de la prueba de hipótesis, con el cual se puede proseguir con la preparación de la Auditoria de Sistemas.

A2. Acción frente al Riesgo de la Seguridad de la Información en los Controles Criptográfico.

- **Firma digital**

  Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Por ejemplo, puede utilizarse en comercio electrónico donde existe la necesidad de verificar quien firma un documento electrónico y comprobar si el contenido del documento firmado ha sido modificado.

  Las firmas digitales pueden aplicarse a cualquier tipo de documento que se procese electrónicamente, por ej., pueden utilizarse para firmar pagos, transferencias de fondos, contratos y convenios electrónicos. Pueden implementarse utilizando una técnica criptográfica sobre la base de un par de claves relacionadas de manera única, donde una clave se utiliza para crear una firma (la clave privada) y la otra, para verificarla (la clave pública).

  Se den tomar recaudos para proteger la confidencialidad de la clave privada, esta clave debe mantenerse en secreto dado que una persona que tenga acceso a esta clave puede firmar documentos, por ej.: pagos y contratos, falsificando así la firma del propietario de la clave.

  Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

  Es necesario considerar el tipo y la calidad del algoritmo de firma utilizado (en el caso del proyecto de grado se hará uso del algoritmo PGP) y la longitud de las claves a utilizar (128 bits). Las claves criptográficas aplicadas a firmas digitales deben ser distintas de las que se utilizan para el cifrado.

  Al utilizar firmas digitales, se debe considerar la legislación pertinente que describa las condiciones bajo las cuales una firma digital es legalmente vinculante. Por ejemplo, en el caso del comercio electrónico es importante conocer la situación jurídica de las firmas digitales. Podría ser necesario establecer contratos de

cumplimiento obligatorio u otros acuerdos para respaldar el uso de las mismas, cuando el marco legal es inadecuado. Se debe obtener asesoramiento legal con respecto a las leyes y normas que podrían aplicarse al uso de firmas digitales que pretende realizar la organización.

- **Administración de Claves y Certificado Digital**

  Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que tipo de control debe aplicarse y con que propósito, y los procesos de la empresa.

  Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, y para evitar un uso inadecuado o incorrecto).

  Se llego a la conclusión que los controles por Firmas Digitales y Administración de Claves y Certificados Digitales fueron revisados a la terminación del producto o software, determinándose el contra riesgo ante la pérdida de seguridad en la sección 6.3 de la prueba de hipótesis.

Se llega a la **conclusión** que **habiéndose realizado la revisión de controles y determinado su contra riesgo**, se puede proseguir con la Auditoria de Sistemas del Modelo P.H.V.A. en la fase de Actuar.

5.1.6. Actuar

Se ejecuto acciones para mejorar continuamente el desempeño de los procesos en SITTEL respecto a la Seguridad de la Información a través de la aplicación de la Norma Internacional ISO/IEC 17799 descritas en las Conclusiones Generales, Conclusiones Específicas y Recomendaciones.

Conclusiones Generales

Como resultado del trabajo realizado se observo que existen aspectos importantes que debilitan la estructura de control interno del ambiente tecnológico, los cuales podrían afectar a la confiabilidad, confidencialidad e integridad de la información.

Por el motivo anteriormente mencionado, es importante que SITTEL realice esfuerzos enfocados a la solución de los principales problemas del área. Los aspectos más importantes a considerar son:

- Planificación estratégica, la cual debería estar alineada a la estrategia del negocio y ser definida como un conjunto de elementos empleados de SITTEL. Lo cual implica una planificación anual de sistemas alineada a la estrategia del negocio que contribuya al logro exitoso de los objetivos de la organización brindando un soporte adecuado tecnológico.

- Gestión del área de sistemas, se debería realizar esfuerzos enfocados a mejorar los mecanismos de gestión existentes, lo cual permitirá una medición cuantitativa del rendimiento del área, la definición y seguimiento de los objetivos establecidos.

  Para lograr este objetivo es importante la formalización e implementación de procedimientos operativos y de control.

- Gestión de la Seguridad Informática, se debería enfocar la gestión de la seguridad de la tecnología de la información en función a un análisis de riesgos que permita la clasificación de la información, definiendo así la criticidad de los datos almacenados en los sistemas. Esto permitirá priorizar las actividades relacionadas con la seguridad según las necesidades de SITTEL.

Con lo cual se determina que **habiéndose realizado las Conclusiones Generales** de la Auditoria de Sistemas en la Superintendencia de Telecomunicaciones, se determino que SITTEL no cumple con la Norma Boliviana ISO/IEC 17799, con lo cual se puede proseguir con las Conclusiones Específicas.

Conclusiones Específicas

Revisión de Controles Generales sobre la Seguridad de la Información

En relación a la revisión de controles generales sobre la seguridad de la información, se observo que si bien las políticas y normas sobre seguridad de la información han sido redefinidas y aprobadas en el plan de contingencias de SITTEL, aún no se ha desarrollado un plan de implementación de dichas políticas, el cual incluya la capacitación tanto del personal de sistemas como de los usuarios finales.

Asimismo, se observo que si bien existe un plan para el traslado y reestructuración de la seguridad del Centro de Procesamiento de Datos, este plan no fue implementado y no se encuentra actualizado, por lo que actualmente existen deficiencias en relación a la seguridad física del Centro de Procesamiento de Datos.

En relación a los procedimientos de recuperación en caso de desastre, se observo que se cuenta con un Plan de Contingencias formalmente documentado, el cual fue probado durante la gestión 2003. Sin embargo, no se realizó pruebas piloto al mencionado plan, debido a que el mismo no considera importante probarlo y disminuir el riesgo que es primordial en el Plan de Contingencias.

Evaluación del Grado de Cumplimiento de la Normativa Internacional ISO/IEC 17799 sobre la Gestión de la Seguridad de la Información en Función de la Aplicación de Firmas y Certificados Digitales

En relación a la revisión de la Norma Internacional ISO/IEC 17799 se determino que SITTEL no cumple con los requisitos establecidos e indispensables para el aseguramiento de la protección de la información, los cuales son:

- Inseguridad en la documentación de la política de seguridad de la información, por desactualización del Plan de Contingencias y falta de pruebas (ver NB ISO/IEC 17799 – 3.1.1).
- Inseguridad por falta de instrucción y entrenamiento en materia de seguridad de la información a los usuarios frente a riesgos no previstos en el plan de contingencias (ver NB ISO/IEC 17799 – 6.2.1).
- No se tiene una base de datos de incidentes relativos a la seguridad ni una comunicación interna respecto a estos con los involucrados (ver NB ISO/IEC 17799 – 6.3.1).
- Inseguridad por falta de controles criptográficos y pérdida de protección en la confidencialidad, autenticidad e integridad de la información (ver NB ISO/IEC 17799 – 10.3)
- Inseguridad en la administración de la continuidad de la empresa (ver NB ISO/IEC 17799 – 11.1)

Con lo cual se determina que **habiéndose realizado las Conclusiones Específicas** de la Auditoria de Sistemas en la Superintendencia de Telecomunicaciones, se determino que SITTEL no cumple con la Norma Bolivia ISO/IEC 17799, con lo cual se puede proseguir con el punto de Recomendaciones de la fase de Actuar del Modelo P.H.V.A.

Recomendaciones

A continuación presentamos un resumen de las recomendaciones que surgieron como resultado del trabajo realizado, para facilitar su lectura y entendimiento las mismas han sido estructuradas en función a las áreas de evaluación que se mencionan en el alcance del presente informe.

Para facilitar en entendimiento de la tabla con el resumen de recomendaciones a continuación presentamos la definición de algunos de los elementos que serán utilizados para la clasificación de los hallazgos.

Nivel de Riesgo, se refiere al efecto que puede tener sobre la información y/o los recursos tecnológicos y consecuentemente el nivel de resguardo que la organización debe asumir para reducir el riesgo, en este sentido los niveles de riesgos definidos son:

Alto (A): Este nivel de riesgo puede tener alto impacto en la Entidad y puede ser cubierto a través de procedimientos y mecanismos muy específicos y detallados, los cuales deben ser implementados a través de adecuadas medidas preventivas. Normalmente este tipo de incidentes causan daños económicos o pueden afectar a la imagen de SITTEL

Medio (M): Son aquellos incidentes cuyo impacto puede ser controlado a través de adecuados mecanismos de salvaguarda, con lo cual es posible reducir el impacto a niveles poco significativos.

Bajo (B): Este tipo de incidentes son mitigados y controlados a través de mecanismos de control de bajo costo y fácil implementación.

Adicionalmente, se incluye en la columna “Área de Impacto”, en la que se detalla las áreas de evaluación involucradas con la observación descrita. Las áreas de evaluación son las siguientes:

a. Evaluación de los controles para la gestión de la tecnología de información

b. Revisión de controles generales sobre la seguridad de la información

c. Evaluación de la seguridad sobre las plataformas de información y dispositivos de comunicación

d. Evaluación sobre la seguridad del DBMS y perfiles de los usuarios

e. Evaluación del grado de cumplimiento de la Normativa Internacional ISO/IEC 17799.

f. Determinación de evaluación de la Aplicación de Administración de Firmas y Certificados Digitales en SITTEL.

Tabla 5. 9. Tabla de Recomendaciones

	Observación	Nivel de riesgo	Area de Impacto
A.	**Revisión de controles generales sobre la seguridad de la información**		**a b c d e f**
1.	La norma sobre contraseñas no se encuentra actualizada ni ha sido implementada.	A	☐ ☑ ☑ ☐ ☑ ☐
2.	No se cuenta con una norma para el tratamiento de reportes de información sensitiva y divulgación a terceros.	A	☐ ☑ ☐ ☐ ☐ ☑
3.	Existen deficiencias en cuanto a la seguridad física del centro de procesamiento de datos (CPD).	A	☑ ☑ ☐ ☐ ☑ ☐
4.	El Plan de Contingencias no fue actualizado.	M	☑ ☑ ☐ ☐ ☑ ☐
B.	**Evaluación del grado de cumplimiento**		**a b c d e f**
5.	Inseguridad en la documentación de la política de seguridad de la información, por desactualización del Plan de Contingencias y falta de pruebas	A	☑ ☑ ☐ ☑ ☑ ☑
6.	Inseguridad por falta de instrucción y entrenamiento en materia de seguridad de la información a los usuarios frente a riesgos no previstos en el plan de contingencias	M	☑ ☐ ☐ ☐ ☑ ☐
7.	No se tiene una base de datos de incidentes relativos a la seguridad ni una comunicación interna respecto a estos con los involucrados	M	☑ ☐ ☐ ☑ ☑ ☑
8.	No se garantiza que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y no están capacitados para respaldar la política de la seguridad de la organización en el transcurso de sus tareas normales.	A	☑ ☐ ☐ ☐ ☑ ☐
9.	Inseguridad por falta de controles criptográficos y perdida de protección en la confidencialidad, autenticidad e integridad de la información	A	☐ ☑ ☑ ☑ ☑ ☑
10.	Incumplimiento en los requerimientos de Seguridad de los sistemas.	B	☑ ☐ ☐ ☐ ☑ ☑
11.	Incumplimiento en la Seguridad de los archivos de los sistemas, perdida de garantía en los proyectos y actividades de soporte técnico de TI que se deberían de llevar a cabo de manera segura.	M	☑ ☐ ☑ ☑ ☑ ☐

Fuente: Elaboración Propia

Se llega a la conclusión que **realizado las recomendaciones y analizado el impacto del incumplimiento de la Norma Boliviana ISO/IEC 17799** se determinó que SITTEL deberá solucionar los riesgos contra su seguridad por el orden de impacto, con lo cual se puede proseguir con las Limitaciones del presente Documento.

5.1.7. Limitaciones del Informe

a. La Gerencia de SITTEL es responsable por el uso de este informe.

b. Es responsabilidad de SITTEL, determinar la implementación de las recomendaciones, no se acepta ninguna responsabilidad sobre las decisiones tomadas por SITTEL.

c. El presente informe se realizó de acuerdo al alcance descrito en el punto 5.1.2 de Planificación de la Auditoria de Sistemas, el cual restringe a la NB ISO/IEC 17799 y al Proyecto de Grado de Firmas y Certificados Digitales.

Se llega a la **conclusión** que **habiéndose realizado las Limitaciones del Informe y habiéndose determinado los puntos de Riesgo para la aplicación de los controles explicados en las recomendaciones**, se determina que SITTEL tiene problemas principalmente en el área de Controles Criptográficos, para lo cual se utilizara su contra riesgo a través del desarrollo del Sistema de Administración de Firmas y Certificados Digitales en la sección 5.2 del capítulo de Ingeniería del Proyecto.

5.2 Desarrollo del proyecto de Software de Firma y Certificado Digital

Dado el concepto de Firmas y Certificados Digitales en la tercera sección del Capítulo de Marco Teórico y Metodológico, coadyuvado por la utilización del criptosistema PGP descrito en la Sección 3.3 se concreta a continuación el desarrollo del software para la Administración de Firmas y Certificados Digitales para la Superintendencia de Telecomunicaciones realizado en PGP y Asp.Net.

La sección del Desarrollo del proyecto de Software se caracteriza por la Administración de la gestión del proyecto de software, la misma cuenta con las siguientes fases a ser desarrolladas a continuación:

- **Proyecto:** Debe organizarse de una manera que permita al equipo de software tener éxito.
- **Personal:** Organización de equipos eficaces, motivados para hacer un software de alta calidad y coordinados para alcanzar una comunicación efectiva.
- **Producto:** Los requisitos del producto deben comunicarse desde el cliente al desarrollador, dividirse (descomponerse) en las partes que lo constituyen y distribuirse para que trabaje el equipo de software.
- **Proceso:** Su fin es adaptarse al personal y al problema. Se selecciona una estructura común de proceso, se aplica un paradigma apropiado de ingeniería del software y se elige un conjunto de tareas para completar el trabajo.

5.2.1 Proyecto

Se analizó a gestión del proyecto de software para garantizar el éxito del desarrollo del mismo, porque mediante el mismo se evitará posibles fallos no determinados en anteriores secciones, para su aplicación se analizó el M**étodo de Jhon** Reel, el cual define diez señales que indican que un proyecto de sistemas se encuentra en peligro:

1. La gente de software no comprende las necesidades de los clientes.

   Se realizo un análisis exhaustivo para determinar las necesidades del cliente poniendo los siguiente limitantes en el desarrollo del mismo, el cual el cliente tiene conocimiento de las mismas:

   a) *El producto autentificara mensajes de ida y vuelta, pero no será un correo electrónico o un sistema de intercambio de paquetes P2P*

   b) *No se realizará un encriptador de paquetes, ni un compresor, solo se adhiere una firma digital al paquete que tendrá que ser transaccionado por sus sistemas de correo electrónico.*

   c) *Se determino que el sistema solo brindará certificados digitales personales y no otros realizará la certificación de otros entes como servidores, páginas web, etc.*

2. El ámbito del producto está definido pobremente.

   El ámbito del producto de software esta definido en el punto 5.2.3.1 con características de Contexto, Objetivo de Información, Funcionamiento y

Rendimiento, lo cual determina las datos cuantitativos necesarios para la realización del producto software.

3. Los cambios están mal realizados en el desarrollo del software.

   Se realizaron cambios en diseño de las pantallas, siendo las mismas que no afectan en gran medida al desarrollo del software y mejoran su funcionamiento e interactibilidad del mismo.

   El cambio de pantallas no afecta al fin del desarrollo del software que son las firmas y certificados digitales.

4. La tecnología elegida cambia.

   La tecnología en el lenguaje de Programación, Asp.Net, el criptosistema PGP y la base de datos SQL Server mejora, pero no cambia, la cual es utilizada por SITTEL.

5. Las necesidades del negocio cambian [o nunca se obtuvieron adecuadamente].

   Las necesidades de SITTEL no cambian, por que su estructura organizativa y su función regulatoria fue determinada por SIRESE, el cual fue decretado en la actual Ley de Telecomunicaciones.

6. Las fechas de entrega no son realistas.

   Las fechas de entrega son realistas al fin del desarrollo del producto, el cual fue analizado por la Comisión Académica de la Escuela Militar de Ingeniería.

7. Los usuarios se resisten.

   Se charlo con los empleados del Departamento de Tecnología de Información y Comunicación (Lic. Amparo Subieta, Ing. Giovanni Gismonti, Ing. Marcelo Lorente, Ing. Roberto Baya, Arq. Claudio Arce) quienes están de acuerdo con el desarrollo del programa y no existe una resistencia por parte de los mismos a causa que no existe una herramienta similar que haya sido utilizado anteriormente.

8. Se pierde los patrocinadores [o nunca se obtuvieron adecuadamente].

SITTEL es el patrocinador del desarrollo del Sistema de Administración de Firmas y Certificados Digitales, la participación de SITTEL fue constante y de apoyo en lo necesario.

9. El equipo del proyecto carece del personal de las habilidades apropiadas.

   El personal tiene las habilidades apropiadas para el desarrollo del producto.

10. Los gestores [y los desarrolladores] evitan buenas prácticas y sabias lecciones.

    Los gestores y desarrolladores no pueden evitar las buenas prácticas y sabias lecciones porque están en constante control por parte del Tutor Colectivo y Tutor del Proyecto de Grado.

Por lo expuesto se llega a la **conclusión** que habiéndose analizado el Modelo Jhon Reel para evitar diez problemas comunes en el desarrollo del software y luego de haber cumplido con cada uno de ellos, se completa el análisis de la Gestión del Proyecto y se puede proseguir con el Análisis del Personal en la sección del Desarrollo del Proyecto de Software de Firmas y Certificados Digitales.

5.2.2 Personal

En el presente punto se examinó a los participantes que colaboraron en el proceso del desarrollo del software y la manera en que se organizó para realizar la ingeniería del software eficaz.

Para facilitar la comprensión de la subsección se dividió de la siguiente manera:

- Los participantes
- El Equipo de Software
- Aspectos sobre La Coordinación y La Comunicación

Los cuales se desarrollan a continuación:

5.2.2.1 Los Participantes

El análisis de los participantes para el Proceso del Software nos ayuda a clasificar los Componentes de Participación dentro del desarrollo del producto con el fin de estudiar al factor más importante dentro del desarrollo del Producto Software, el Recurso Humano y poder interactuar con la mayor facilidad en el Proceso del Software.

Para el mismo se clasificó los componentes de Participación en:

a) ***Gestores Superiores:*** Los aspectos de Negocios en SITTEL es Supervisado por la Lic. Amparo Subieta.

b) ***Gestores (técnicos) del Proyecto:*** Las personas que planifican, motivan, organizan y controlan el Proceso del Software son: Lic. Fernando Yánez (Tutor Colectivo) y Ing. Guido Rosales (Tutor del Proyecto).

c) ***Profesionales:*** Quién proporciona la capacidad técnica necesaria para la ingeniería del producto "Administración de Firmas y Certificados Digitales" es el Alumno Marcelo Palma.

d) ***Clientes:*** Quien especifico los requisitos para la Ingeniería de Software y otros elementos que tuvieron menor influencia en el resultado (Auditoria de Sistemas de Seguridad) es el Ing. Giovanni Gismonti (Revisor de la Parte Técnica en SITTEL).

e) ***Usuarios Finales:*** Son los profesionales del Departamento de Tecnologías de Información y Comunicación quienes interactúan con el Software.

Se llega a la **conclusión** que habiendo determinado los participantes y clasificados los mismos por su participación, se puede proseguir para completar la Gestión del Personal.

5.2.2.2 El Equipo de Software

Las consecuencias prácticas y políticas de un cambio de organización generalmente no están dentro del alcance de las responsabilidades del gestor de un proyecto de software. Sin embargo, la organización del personal directamente involucrado en un nuevo proyecto de software esta dentro del gestor del proyecto. Por tanto su influencia puede ser para bien o mal del Proyecto de Software.

Entre las estructuras organizativas para el Proyecto de "Administración de Firmas y Certificados Digitales" analizamos las siguientes:

- **Descentralizado Democrático (DD):** Las decisiones sobre problemas y los enfoques se hacen en consenso del grupo. La comunicación entre los miembros del equipo es horizontal.
- **Descentralizado Controlado (DC):** La resolución de problemas sigue siendo una actividad de grupo, pero la implementación de soluciones se reparten entre subgrupos por el jefe del equipo. La comunicación entre subgrupos e individuos es horizontal. También hay comunicación vertical a lo largo de la jerarquía de control.

- **Centralizado Controlado (CC):** El jefe del equipo se encarga de la resolución de problemas de alto nivel y la coordinación interna del equipo. La comunicación entre el jefe y los miembros del equipo es vertical.

Debido a que una estructura centralizada realiza las tareas más rápidamente, es la más adecuada para manejar problemas sencillos.

Se llega a la **conclusión** que habiendo determinado la estructura organizativa del equipo de software (Estructura Centralizada Controlada), se puede proseguir para completar la Gestión del Personal.

5.2.2.3 Aspectos Sobre la Comunicación y la Coordinación:

Hay muchos motivos por los que los proyectos de software pueden tener problemas. La ***escala*** (tamaño) de muchos esfuerzos de desarrollo es grande, conduciendo a complejidades, confusión y dificultades significativas para coordinar entre los participantes del Software. La ***incertidumbre*** es corriente, dando como resultado un continuo flujo de cambios que impactan a los participantes del proyecto. La ***interoperabilidad*** se ha convertido en una característica clave de muchos sistemas.

Estas características del software moderno – escala, incertidumbre e interoperabilidad – son aspectos de la vida. Para enfrentar a las mencionadas características eficazmente, el conjunto de participantes del proyectote ingeniería del software de Firmas y Certificados Digitales establecieron métodos efectivos para coordinar la realización del trabajo en grupo detallado a continuación.

Para lograr se estableció mecanismos de comunicaciones formales e informales entre los miembros del equipo, para lo cual se determinó los siguientes medios de de comunicación:

- Comunicación Formal:
    - Por escrito como Informes utilizadas en la entrega de Avances en el Trabajo de Grado.
    - Reuniones organizadas utilizadas en la defensa del Trabajo de Grado.
- Comunicación Informal:
    - Conferencias Telefónicas para coordinar reuniones y entrega de avances.
    - Correo Electrónico para enviar los avances del material.

- Chat para intercambiar opiniones respecto a la metodología y su aplicación dentro del marco práctica y entrega del software para su revisión en el marco práctico.

Además se analizó las diferentes técnicas de coordinación de proyectos que se categoriza de la siguiente manera:

- **Formal, enfoque impersonal.** Incluye documentos de ingeniería de software y entregas (incluyendo el código fuente), memorandos técnicos, hitos del proyecto, planificaciones, planificaciones del programa y herramientas de control del proyecto, peticiones de cambios y documentación relativa, informes de seguimiento de errores e información almacenada.
- **Formal, procedimientos interpersonales.** Se centra en las actividades de garantía de calidad aplicada a productos de ingeniería del software. Esto incluye reuniones de revisión de estado e inspecciones de diseño de código.
- **Informal, procedimientos interpersonales.** Incluye reuniones de grupo para la divulgación de información y resolución de problemas así como “identificación de requisitos y del personal de desarrollo”.
- **Comunicación Electrónica.** Comprende correo electrónico, boletines de noticias electrónicas y, por extensión, sistemas de videoconferencia.
- **Red interpersonal.** Discusiones informales con los miembros del equipo y con personas que no están en el proyecto pero que pueden tener experiencia o una profunda visión que puede ayudar a los miembros del equipo.

Después de haber analizado el material que administramos y generamos por las firmas y Certificados Digitales se determino el uso de la **Técnica de Coordinación Formal, enfoque impersonal** por que nos ayuda en la comunicación y coordinación de la documentación para la Ingeniería de Software.

Por lo expuesto se llega a la **conclusión** que habiéndose analizado los aspectos sobre la comunicación y la coordinación para evitar problemas respecto a las nuevas características del software moderno (escala, incertidumbre e interoperabilidad), se puede proseguir con la sección de Desarrollo del Producto Software de Firmas y Certificados Digitales en la fase de Producto.

5.2.3 Producto

El análisis detallado de los requisitos del software o del producto proporcionaría la información necesaria para las estimaciones cuantitativas y un plan organizado en función de información sólida.

Por tanto, debemos examinar el producto y el problema a resolver justo al inicio del proyecto, para el cual se analizó los siguientes puntos:

- Ámbito del software
- Descomposición del Problema

Los cuales se desarrollan a continuación:

5.2.3.1 Ámbito del Software

El ámbito de software son las características del medio del desarrollo (empresa) que coadyuvan al proyecto a obtener ciertas métricas que ayuden a determinar el avance del software en el tiempo en que desarrollamos.

A continuación se desarrolla el ámbito del software respondiendo a las siguientes cuestiones de Contexto, Objetivos de Información, Funciones y Rendimiento, y Cliente:

a) Contexto

¿Cómo encaja el software a construir en un sistema, producto o contexto de negocio mayor y que limitaciones se imponen como resultado del contexto?

El software se encuentra orientado a ser desarrollado a medida para el Departamento de Tecnologías de Información y comunicación en SITTEL, respecto a las limitaciones del contexto se encuentra la utilización de Tecnología Microsoft (software propietario) y el presupuesto reducido para el desarrollo del producto.

b) Objetivos de Información.

¿Qué objetivo de datos visibles al cliente se obtiene del software?

Se obtiene la firma digital el cual esta adjunto al mensaje a ser autentificado mediante el proceso de firmado digital con PGP y autentificación de la firma digital, el formato es el siguiente:

9E2B 9D14 CBCE FE12 16A8 C103 48B2 5161 69AB 5784

El código es generado para cada mensaje, y es único porque las características del mensaje.

¿Qué objetos de datos son requeridos de entrada?

Son requeridos los siguientes datos para:

a) *Suscripción al sistema para adquirir sus Firmas Digitales:*
   i. *Nombres*
   ii. *Apellidos*
   iii. *Dirección de E-mail en SITTEL*
   iv. *Departamento de SITTEL*
   v. *Usuario*
   vi. *Contraseña*
   vii. *Pregunta de Seguridad*
   viii. *Respuesta de Pregunta de Seguridad*

b) *Recuperación y Modificación de Contraseña de la Firma Digital:*
   i. *Respuesta de Pregunta de Seguridad*
   ii. *Departamento de SITTEL*

c) *Proceso de Firmado Digital*
   i. *Llave Privada*
   ii. *Usuario*
   iii. *Contraseña*
   iv. *Archivo*

d) *Proceso de Autentificación de la Firma Digital por Certificado Digital*
   i. *Llave pública del Emisor del Mensaje*
   ii. *Archivo*

e) *Gestión de Claves Públicas o Anillos Públicos*
   i. *Usuario*
   ii. *Contraseña*

f) *Gestión de Claves Públicas o Anillos Privados*

i. Usuario

ii. Contraseña

g) Eliminar el servicio de Firmas y Certificados Digitales

i. Usuario

ii. Contraseña

c) Funciones y rendimiento.

¿Qué función realiza el software para transformar la información de entrada en una salida?

Se realiza las siguientes funciones en los siguientes procesos:

a) Suscripción al sistema para adquirir sus Firmas Digitales:

i. Ingresar al sistema y después a la opción de Adquirir Firma Digital.

ii. Al obtener los datos necesarios para garantizar la información necesaria del usuario perteneciente a la Red de SITTEL, se pasa al siguiente paso.

iii. En el segundo paso genera las dos llaves para el Firmado Digital con el criptosistema PGP y la contraseña obtenida.

iv. Consecuentemente el usuario deberá exportar las llaves generadas (llave pública y privada) para el funcionamiento del criptosistema.

v. El sistema crea una copia de las llaves al anillo, para realizar la certificación del usuario por el Sistema de Administración de Firmas y Certificados Digitales.

b) Recuperación y Modificación de Contraseña de la Firma Digital:

i. Ingresar a la opción de recuperación de contraseña.

ii. Ingresar los datos solicitados, y aceptar, enviara tu contraseña a tu E-mail y la opción de cambiarlo

c) Proceso de Firmado Digital

i. Ingrese a la opción de Firmar documento

ii. Ingrese su usuario, contraseña y llave privada.

iii. Selecciones el archivo a ser firmado

iv. *Generara el archivo firmado por el criptosistema PGP.*

d) *Proceso de Autentificación de la Firma Digital por Clave Pública*

i. *Ingresar a la opción de Autentificación por Clave Pública*

ii. *Ingresar el archivo firmado y la llave pública del emisor.*

iii. *Se procede a verificar por el método PGP*

iv. *Se determina el resultado si pertenece o no.*

e) *Gestión de Claves Públicas o Anillos Públicos*

i. *Se ingresa a la opción de Claves Públicas*

ii. *Se ingresa el usuario y contraseña*

iii. *Se solicita la llave de un determinado usuario*

iv. *Si existe el usuario le permitirá descargar, caso contrario saldrá un mensaje de Clave Pública inexistente.*

f) *Gestión de Claves Públicas o Anillos Privados*

i. *Se ingresa a la opción de Claves Privada*

ii. *Se ingresa el usuario, contraseña*

iii. *Se solicita la llave privada del usuario.*

iv. *Si existe el usuario enviara una respuesta al Correo Electrónico del mismo con una dirección para bajar la llave y un aviso al administrador del programa..*

v. *Caso contrario le indicara que sus datos son incorrectos o el usuario es desconocido.*

g) *Eliminar el servicio de Firmas y Certificados Digitales*

i. *Se ingresa a la opción de eliminar usuario*

ii. *Se ingresa usuario y contraseña y se elimina el registro.*

iii. *Se envía un e-mail a su correo de confirmación de perdida de usuario.*

¿Hay características de rendimiento especiales que abordar?

No se abordará las características de rendimiento porque el criptosistema PGP ya se encuentra desarrollado y es muy liviano, mientras que otras características para el lenguaje de programación fue subsanado por los potentes servidores de SITTEL.

¿Cuál será el beneficio económico de una buena solución?

La solución al ser orientada hacia una tesis y la seguridad informática de SITTEL, no se encuentra orientada hacia el factor económico, aunque en la factibilidad económica prueba que el desarrollo del producto es posible y con muchos beneficios.

¿Hay otro camino para la solución?

La construcción de un PKI[34] *constituye el marco de referencia que le permite desplegar servicios de seguridad que se basan en cifrado. PKI le permite crear las entidades y la confianza que se necesita para los procesos de identificación y autentificación, y para administrar el cifrado de clave pública que ofrece una solución infinitamente más escalable que las infraestructura de cifrado simétrico y seguridad. El problema es su complejidad, tiempo y costo.*

d) Cliente

¿Qué es lo que espera el cliente del producto?

- *El cliente caracteriza un resultado aceptable el cual cumpla las siguientes función: La firma digital garantice que los datos proceden de una parte concreta al crear una firma digital que es única de esa parte. El certificado digital será EL RESPALDO VIRTUAL Y EL TESTIMONIO de que la firma digital pertenece a un determinado usuario.*

¿Cuáles son las pantallas básicas que esta compuesto el programa?

- *El entorno de trabajo esta compuesto por ocho pantallas básicas:*
  - *Pantalla de Ingreso y selección de opciones*
  - *Pantalla para inscripción y obtención de Claves Asimétricas*
  - *Pantalla de Recuperación y Modificación de Datos de Contraseña de la Firma Digital*
  - *Pantalla para el Proceso de Firmado Digital*
  - *Pantalla del Proceso de Autentificación de un mensaje por Firma Digital*

[34] Public Key Interface – Infraestructura de Llave Pública

- *Pantalla para la Gestión de Claves Públicas y Anillos Públicos*
- *Pantalla para la Gestión de Usuarios*
- *Pantalla para la Autentificación de Firma Digital por Certificado Digital*
- *Pantalla para eliminar el servicio de Firmas y Certificados Digitales*

¿Cuáles son las limitaciones que observa dentro de la institución?

Las limitaciones fueron sus aplicaciones propietarias que utilizan por desconocimiento de las mismas y el lenguaje de programación: asp.Net como la Base de Datos SQL Server a ser empleadas, las mismas que fueron subsanadas.

Se llega a la **conclusión** que habiéndose determinado el ámbito del software mediante el resultado de las anteriores preguntas se determino diferentes métricas para el desarrollo de la Descomposición del Problema, con el objetivo de completar la Gestión del Producto.

5.2.3.2 Descomposición del Problema

La descomposición del problema, denominado a veces particionado o elaboración del problema, es una actividad que se asienta en el núcleo del análisis de requisitos de software (desarrollado en el modelo de secuencia lineal para la firma y el certificado digital) con el fin de facilitar el desarrollo del mismo a través de la estrategia “divide y vencerás” cuando nos enfrentamos a problemas complejos en el Desarrollo del Sistema de Administración de Firmas y Certificados Digitales.

La descomposición se aplica en dos áreas principales:

- La funcionalidad que debe entregarse
- El proceso que se empleara para entregarlo

Los cuales son desarrollados a continuación:

a) La funcionalidad que debe entregarse

Se considero un proyecto que generará firmas digitales y su correspondiente certificado digital para autentificación de mensajes. Entre las características peculiares del producto están:

i. Firmado del Documento; característica extremadamente sofisticada por aplicación del modelo de encriptación PGP.

ii. Autentificación del mensaje; proceso inverso y además paralelo para la autentificación del mensaje.

iii. Acoplamiento del modelo de Certificado Digital a la Firma Digital, dificultad acoplada al modelo de Firma Digital.

b) El proceso que se empleara para entregarlo

A medida que evoluciona la exposición del ámbito, un primer nivel de partición ocurre de forma natural.

❖ Se hablo con el Departamento de Tecnologías de Información y Comunicación de SITTEL respecto a la funcionalidad del sistema.

i. El sistema utilizara el Criptosistema desarrollado por la Empresa PGP Corporation para encriptar y se acoplara al software mediante el sistema OLE de asp.Net.

ii. Se determino que la autentificación del mensaje se realice con el mismo software PGP y para facilitar su uso se acoplara una pantalla amigable.

iii. El certificado digital funcionará de la siguiente manera:

1. Se generara automáticamente en el software un certificado digital al crear la firma digital del usuario, el cual estará acoplado a los anillo de las llaves públicas.

2. Para su verificación deberá ingresar el usuario o su llave pública y mostrará el certificado digital.

Cada una de las características mencionadas anteriormente representa una subfunción para ser desarrollado en la subsección de análisis del sistema dentro del punto del Proceso para el desarrollo de las firmas y certificados digitales.

Con lo expuesto se llega a la **conclusión** que habiéndose determinado el ámbito del software y realizado la descomposición del problema, se logro obtener un análisis inicial para el desarrollo de la Fase de Análisis de Requerimientos del Modelo Lineal Secuencial.

Habiendo completado el Análisis del Producto la sección de Desarrollo del Producto Software de Firmas y Certificados Digitales en la fase de Proceso.

5.2.4 Proceso

Dado el concepto de Proceso descrita en la Sección 3.2.2 se concreta a continuación la utilización de la herramienta seleccionada (Modelo Lineal Secuencial) para el desarrollo de software a través de los procesos, métodos y herramientas a considerarse por el modelo.

Modelo Lineal Secuencial

Conocido como Ciclo de Vida Clásico de Software, se utiliza en el desarrollo del sistema por su facilidad y alta prestación en el desarrollo del software. El Modelo Lineal Secuencial es el conjunto de actividades que los analistas y programadores realizan para desarrollar e implementar un sistema de información y consta de los siguientes pasos:

- Investigación Preliminar
- Análisis sobre los Requerimientos del Sistema
- Diseño del Sistema (Diseño Lógico)
- Desarrollo de Software (Diseño Físico)
- Implantación y evaluación
- Prueba y Mantenimiento

Para su mayor comprensión se aplicó el Modelo Lineal Secuencial a las Firmas Digitales y a los Certificados Digitales para separado bajo el funcionamiento del Criptosistema PGP explicado en la sección 3.1 del Marco Teórico y Metodológico; sin embargo los puntos de prueba y mantenimiento fueron realizados en la sección 5.3 para la verificación de la Métricas de Calidad de Software.

A continuación desarrollamos el **Modelo Lineal Secuencial** para las **Firmas Digitales en Primer y los Certificados Digitales**.

5.3 Modelo Lineal Secuencial para la Firma y Certificado Digital

Dado los conceptos de Firma Digital y Certificado Digital fueron descritos en la primera sección del Capitulo de Marco Teórico y Metodológico, coadyuvado por la utilización de la herramienta y Cripsistema PGP se concreta a continuación el análisis del Modelo Lineal Secuencial para el Desarrollo de la Firma Digital en SITTEL.

5.3.1 Investigación Preliminar

Con el fin de verificar la factibilidad del proyecto y el análisis de los diferentes modelos, métodos y procesos para su desarrollo normal antes de la realización del análisis de las Firmas y Certificados Digitales, se realizó la investigación preliminar que fue desarrollada en el Tercer Capítulo de Marco Teórico y Metodológico, en el Cuarto Capítulo de Factibilidad del Proyecto y en la Subsección 5.2.1 al 5.2.3 de Gestión del Proyecto, Gestión del Personal y Gestión del Producto.

Por lo expuesto se llega a la **conclusión** que habiéndose realizado la correspondiente Investigación Preliminar y determinado la factibilidad del proyecto, se puede proseguir para completar el Desarrollo del Modelo Lineal Secuencial para las Firmas Digitales y Certificados Digitales.

5.3.2 Análisis sobre los Requerimientos del Sistema

El análisis de los requisitos del sistema permite al ingeniero de sistemas especificar las características operacionales del software (función, datos y rendimientos), indica la interfaz del software con otros elementos del sistema y establece las restricciones que debe cumplir el software para su funcionamiento correcto antes del Diseño de las Firmas Digitales.

Antes que los requisitos puedan ser analizados, modelados o especificados, deber ser recogidos a través de un proceso de obtención, su fin es identificar los requisitos mínimos del software e iniciar el proceso de recolección, para lo cual se utiliza la Técnica de Gauge y Weinberg, y el Modelo de Casos de Uso desarrollados a continuación:

5.3.2.1 La Técnica de Gauge y Weinberg

La técnica de obtención de requisitos más usada y que fue utilizada para inicializar el proceso del análisis es llevar a cabo una reunión o entrevista preliminar. El modelo sugiere que el Ingeniero de Software empiece preguntando cuestiones de contexto libre y fue utilizado en el **Analista de Sistemas** en fecha 09 de Marzo del 2005.

El primer conjunto de cuestiones de contexto libre se enfoca sobre el cliente, los objetivos generales y los beneficios esperados desarrollados a continuación:

- ¿Quién está a cargo de la solicitud de este trabajo (Quienes son los responsables del Proyecto por parte de SITTEL)?

El responsable principal es la Lic. Amparo Subieta, Jefa del Departamento de Tecnología de Información y Comunicación de SITTEL, seguido del Ing. Giovanni Gismonti, Analista de Sistemas del Departamento de SITTEL.

- ¿Quién utilizará la solución?

  Se desearía implementar la solución para todo el personal de SITTEL y para la autentificación de usuarios por la Intranet y Extranet de SITTEL, pero en su primera instancia se determino que el uso de la misma será solo para el Personal del Departamento de Tecnologías de Información y Comunicación de SITTEL.

- ¿Cuál será el beneficio económico del éxito de la solución (en SITTEL)?

  La generación ilimitada de firmas digitales sin costo adicional a la construcción del Sistema de Administración de Firmas y Certificados Digitales.

- ¿Hay alguna otra alternativa para la solución que necesita (Hay algún producto sustituto de las Firmas Digitales que se encuentran bajo desarrollo)?

  La compara Firmas Digitales a la empresa VeriSign con el costo de US$. 10.50 por cada una, con una caducado del software anual y un costo de reinscripción de US$. 10.50, con una tasa de mantenimiento de US$. 210.00 con un interés del 5% anual.

Las anteriores preguntas ayudan a identificar todos los participantes que tiene una relación importante con el proceso de desarrollo y utilización del software a construirse. Además, las preguntas identificarán los beneficios medibles en una implementación correcta de posibles alternativas para un desarrollo normal del software.

El siguiente conjunto de preguntas permite al analista obtener un mejor rendimiento del problema y al cliente comentar sus opiniones sobre la solución:

- ¿Cómo caracterizaría una <<buena>> salida (resultado) generada para una buena solución (Cual es su expectativa sobre la utilización de las Firmas Digitales)?

  El Ing. Giovanni Gismonti espera obtener con el software una firma digital que acoplado (en su posibilidad) a un servidor E-mail o un programa de envió y recepción de mensajes, obtener las dos claves o llaves, enviar un mensaje firmado por la llave privada y autentificarlo con su llave pública si le pertenece el mensaje.

- ¿Puede mostrarme (o describirme) el entorno en que se utilizará la solución?

  La solución utilizará un entorno Web para facilitar la utilización del software por el personal del Departamento de Sistemas a través del Modelo Cliente Servidor y utilizará Programación Web y Diseño Gráfico Web para su utilización, se determino que el software tenga la siguiente forma (ver figura 5.2):

Figura 5.2: Modelo de Pantalla del Sistema de Administración de Firmas y Certificados Digitales

Fuente: Elaboración Propia

- ¿Hay aspectos o restricciones especiales del rendimiento que afectan a la manera de enfocar la solución?

  Ninguno en especial, solo restricciones con relación a las tecnologías de información, se puede utilizar los siguientes lenguajes de Programación:

  - *Visual Basic.Net*
  - *Asp o asp.Net*
  - *C.Net*

  Respecto al hardware se cuentan con servidores de gran capacidad que soportan plataformas completas.

El último conjunto de preguntas se concentra en la eficacia de la reunión, **Gauge y Weinberg** las denominan **"meta-preguntas"** y son desarrolladas a continuación:

- ¿Es usted la persona adecuada para responder a estas preguntas? ¿Sus respuestas son <<oficiales>>?

  Si, el Analista de Sistemas esta a cargo del desarrollo y mantenimiento del software utilizado por SITTEL.

- ¿Estoy preguntado demasiado?

  La pregunta determino que el Analista de Sistemas indicó que no tiene un conocimiento extenso en el área de Criptosistemas y Entorno PKI.

- ¿Hay alguien más que pueda proporcionar información adicional?

  El tutor del presente trabajo de grado y el Jefe del Departamento de Tecnología de Información y Comunicación de SITTEL.

- ¿Hay algo más que debería preguntarle?

  El Analista de Sistemas pregunto ¿Para cuando estará el software?, se respondió para mediados de Septiembre en su versión Beta.

Estas preguntas (y otras) ayudaron a iniciar la comunicación tan esencial para el éxito del análisis.

Por lo expuesto anteriormente se llega a la **conclusión** que habiéndose analizado los requisitos de **Gauge y Weinberg** para el desarrollo del Sistema de Administración de Firmas y Certificados Digitales, se logro él análisis para el desarrollo de las Firmas y Certificados Digitales, con lo cual se puede proseguir con el proceso de **Casos de Uso** para completar el análisis de requerimiento del Modelo Lineal Secuencial.

5.3.2.2 Casos de Uso

Una vez recopilado los requisitos para el análisis, se genero un conjunto de escenarios que identifican una línea de utilización para el sistema que va a ser construido. Los escenarios llamados **casos de uso** facilitan una descripción de cómo el sistema se funcionará.

Para generar los **Casos de Usos** se realizó un análisis de los diferentes tipos de personas que utilizan el sistema o el producto (ver Figura 5.3), es importante indicar que

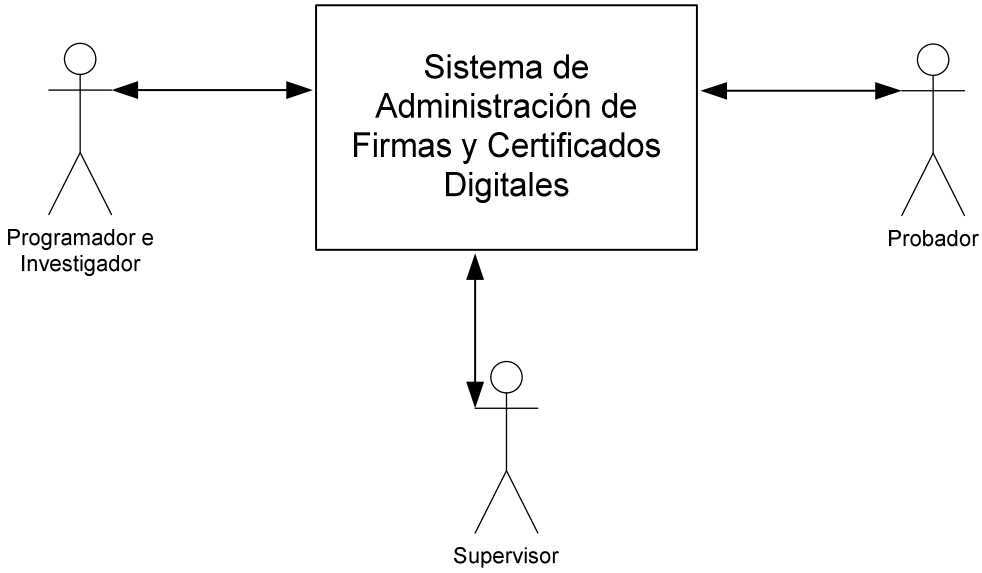
un actor y un usuario no son la misma cosa, y pueden clasificarse en las siguientes funciones: Programador, probador, supervisor e investigador.

Programador e Investigador: Alumno Marcelo Palma

Probador: Ing. Giovanni Gismonti

Supervisor: Lic. Fernando Yánez, Ing. Guido Rosales y Lic. Jesús Rocha

Figura 5.3: Actores que interactúan con el Sistema



Fuente: Elaboración Propia

Identificado los actores en el anterior punto, se desarrolla los casos de uso para el siguiente conjunto de situaciones analizados para el desarrollo del Sistema de Administración de Firmas y Certificados Digitales:

a. *Ingreso al Sistemas y selección de opciones*
b. *Inscripción y obtención de Claves Asimétricas*
c. *Recuperación y Modificación de Datos de Contraseña de la Firma Digital*
d. *Proceso de Firmado Digital*
e. *Proceso de Autentificación de un mensaje por Firma Digital*
f. *Gestión de Claves Públicas y Anillos Públicos*
g. *Gestión de Usuarios*

h. Autentificación de Firma Digital por Certificado Digital

i. Eliminar el servicio de Firmas y Certificados Digitales

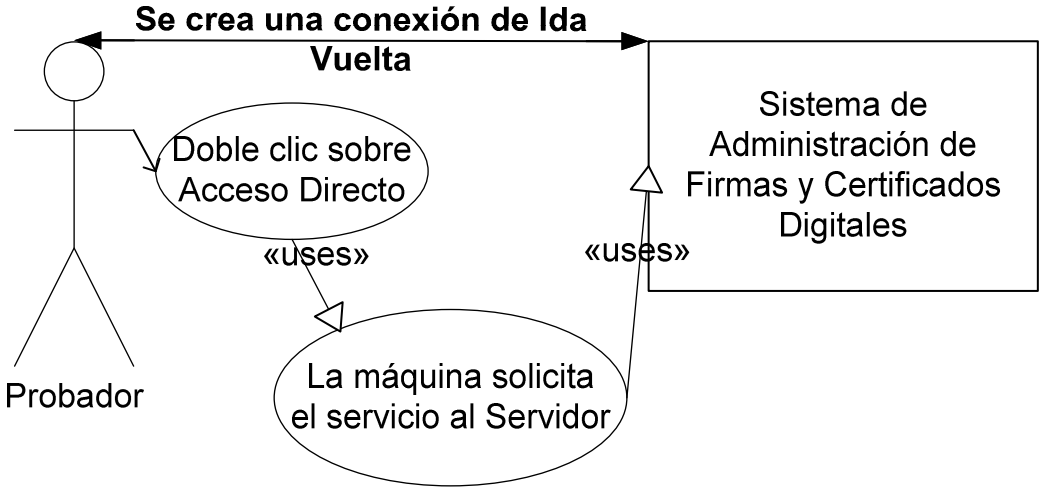
Se utilizó las siguientes preguntas en cada caso de uso para su mejor construcción en la fase de diseño posteriormente:

- ¿Cuáles son las principales tareas o funciones que serán realizadas por el actor?
- ¿Cuál es el sistema de información que el actor adquiere, produce o cambia?

A continuación se desarrollan los casos de usos identificados en el presente punto:

a. Ingreso al Sistemas y selección de opciones

Figura 5.4: Caso de uso para el ingreso al sistema y selección de opciones



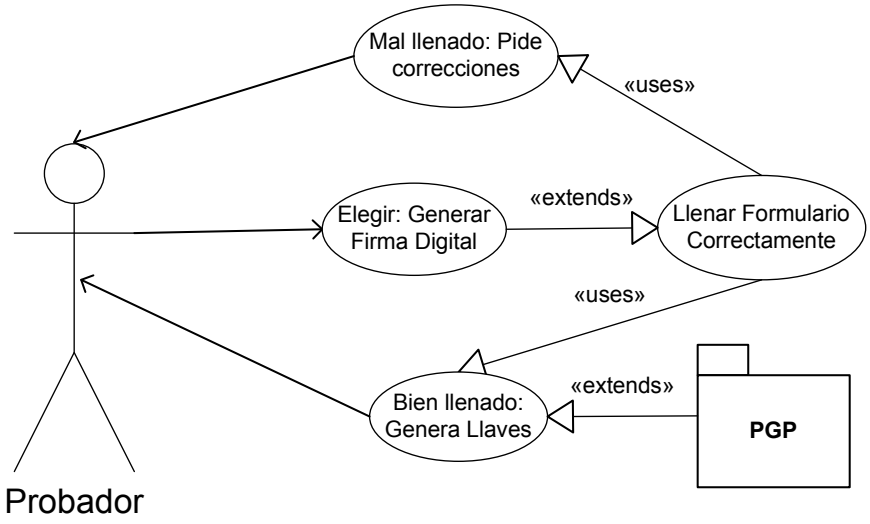
Fuente: Elaboración Propia

- Las principales tareas realizadas por el usuario (como se observa en la figura 5.4) será ingresar al sistema y elegir alguna de las opciones mencionadas en el inciso b.
    - Ingresa al sistema haciendo doble clic sobre el incono de acceso directo.
    - Se abre el programa y muestra las ocho opciones que tiene el usuario para elegir.
    - Se crea una comunicación de Ida y vuelta mediante la tecnología Cliente – Servidor.

- El usuario podrá elegir las ocho opciones básicas del sistema, las cuales son inscribirse y obtener sus claves asimétricas, recuperar y modificar su contraseña de firma digital, realizar el firmado digital, autentificación de un mensaje por firma digital, gestión de llaves públicas y anillos públicos, gestión de claves privadas y anillos privados.

b. Inscripción y obtención de Claves Asimétricas

Figura 5.5: Caso de uso para la inscripción y obtención de Claves Asimétricas



Fuente: Elaboración Propia

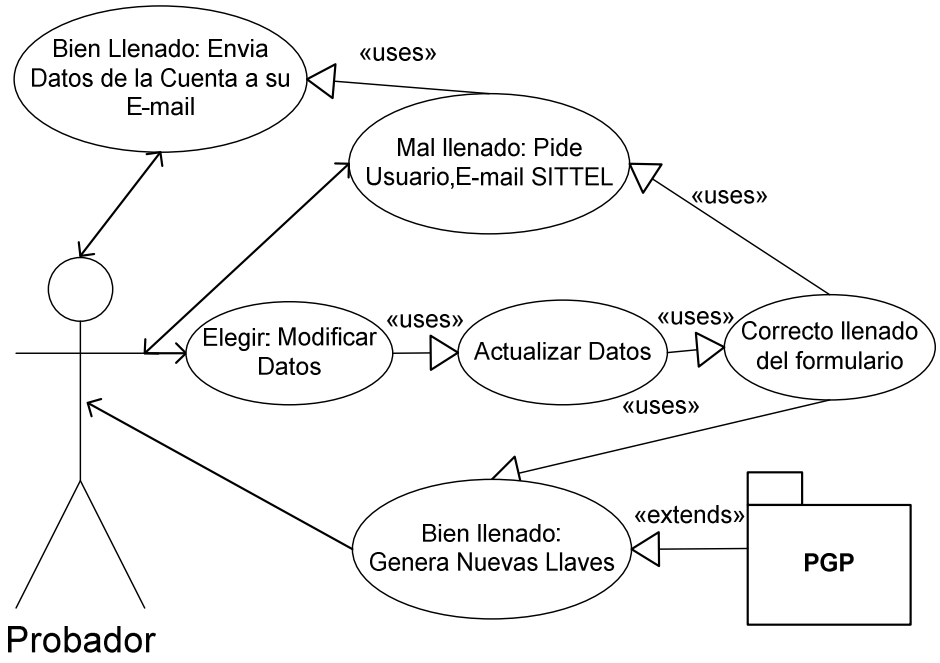
- La principal función que realiza el usuario (como se observa en la figura 5.5) en el presente caso de uso es elegir la opción de Generar Firma Digital, después ingresa a un formulario.
- Al llenar los datos correctamente ingresará a otra pantalla donde podrá descargar sus llaves (privada y pública).

c. Recuperación y Modificación de Datos de Contraseña de la Firma Digital

- La principal función que realiza el usuario (como se observa en la figura 5.6) en el presente caso de uso es elegir la opción de Modificar Datos.
- Después ingresará a un formulario el cual pedirá llenar su usuario y contraseña antigua, en cuanto ingrese correctamente sus datos le solicitará actualizar sus datos, inmediatamente se generara una nueva firma digital.

- Si en caso que no recordará su contraseña, el sistema le pedirá ingresar su usuario y Correo Electrónico de SITTEL, en cuanto ingrese correctamente los datos se enviará un correo electrónico con sus datos.

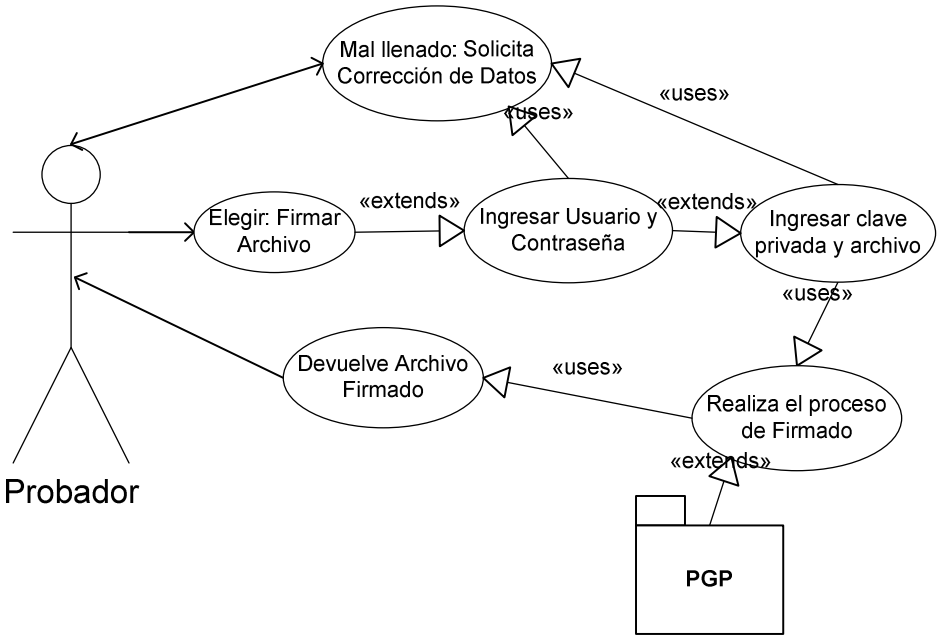
Figura 5.6: Caso de Uso para recuperar y modificar datos de la contraseña de la firma digital



Fuente: Elaboración Propia

d. Proceso de Firmado Digital

Figura 5.7: Caso de uso de Firmado Digital de un archivo

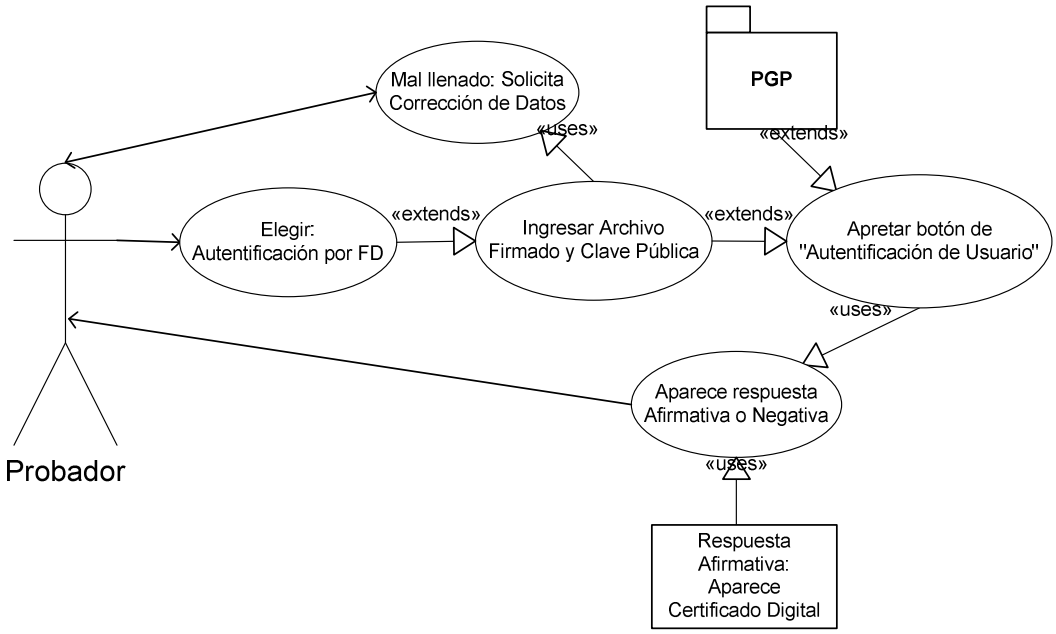


Fuente: Elaboración Propia

- La principal función que realiza el usuario (como se observa en la figura 5.7) en el presente caso de uso es elegir la opción de Firmar Archivo.
- En cuanto ingrese a la opción de “Firmar Archivo” aparecerá una pantalla solicitando su usuario y contraseña, a continuación se pedirá su clave privada y el archivo para firmarlo, después aparecerá una página para descargar el archivo firmado y listo para ser enviado.
- En caso que se introdujera datos incorrectos en la autentificación del usuario, no ingresará y seguirá pidiendo los datos correctos.

e. Proceso de Autentificación de un mensaje por Firma Digital

Figura 5.8: Caso de uso de Autentificación del origen del mensaje



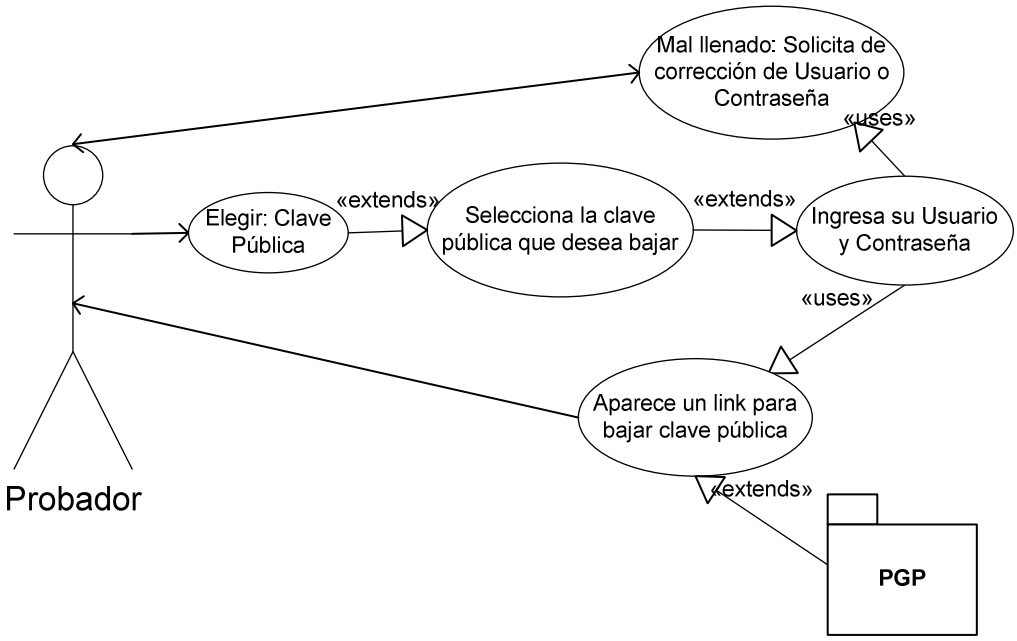
Fuente: Elaboración Propia

- La principal función que realiza el usuario (como se observa en la figura 5.8) en el presente caso de uso es elegir la opción de Autentificación por Firma Digital.
- En cuanto tenga el archivo firmado y la clave pública del emisor para su autentificación, ingresará a la opción de autentificación del usuario, deberá adjuntar el archivo y la clave pública, apretar el botón de ”autentificación de Usuario”, consecuentemente aparecerá una pantalla con la respuesta afirmativa o negativo.
- Si la respuesta es correcta mostrará en la misma pantalla el certificado digital de la clave pública.

a. En caso que se introdujera archivos incorrectos en la autentificación del usuario, no verificará la autenticidad y seguirá pidiendo los datos correctos.

f. Gestión de Claves Públicas y Anillos Públicos

Figura 5.9: Caso de uso de Claves Públicas

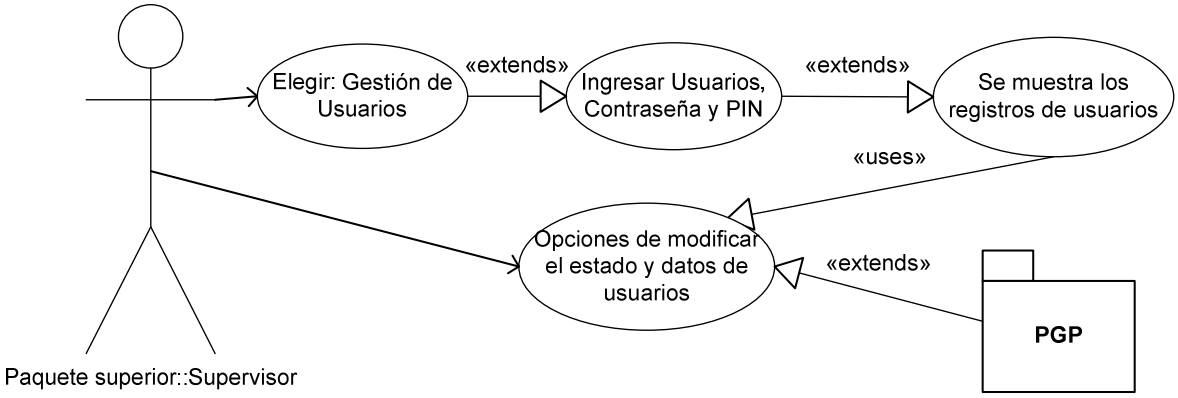


Fuente: Elaboración Propia

- La principal función que realiza el usuario (como se observa en la figura 5.9) en el presente caso de uso es elegir la opción de Clave Pública.
- Después de haber ingresado a la opción, se observará una lista llaves públicas con los nombres respectivos de los propietarios y una opción para descargar la llave pública.
- El portal le permitirá bajar la llave haciendo clic sobre la llave seleccionada y en cuanto se habrá la pantalla le pedirá su usuario y contraseña (necesario para mantener la integridad de la información de las llaves públicas).
- Si la respuesta es correcta le permitirá bajar la llave, en caso que se introdujera un usuario desconocido o una contraseña incorrecta, no permitirá bajar la llave.

g. Gestión de Usuarios

Figura 5.10: Caso de uso para la Gestión de Usuario



Fuente: Elaboración Propia

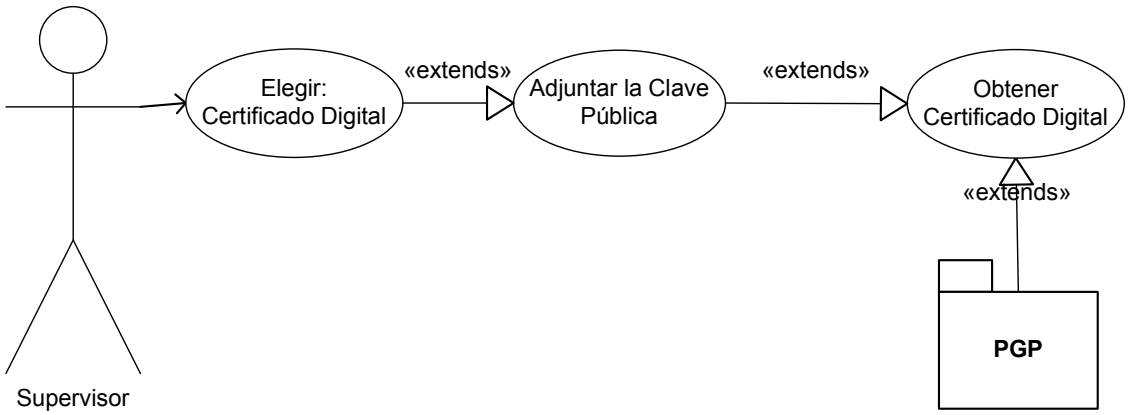
- La principal función que realiza el **administrador** (como se observa en la figura 5.10) en el presente caso de uso es elegir la opción de Gestión de Usuarios.
- Después de haber ingresado a la opción, le pedirá un usuario, su contraseña y un PIN (generado aleatoriamente y enviado semanalmente a su correo del administrador).
- En cuanto ingrese observará los registros de los usuarios, identificando su estado, ID, nombre y apellido, llave pública, certificado digital, y unos botón para modificar su estado y datos.
- En cuanto ingrese a modificar su estado y datos el administrador podrá actualizar los datos de la persona, deshabilitar en el caso que estuviera habilitado y habilitar en el caso de que estuviera deshabilitado, o eliminar la cuenta.
- Cualquier cambio en esta opción estará registrada por un Log de seguridad.

h. Identificación de Firma Digital por Certificado Digital

- La principal función que realiza el usuario (como se observa en la figura 5.11) en el presente caso de uso es elegir la opción de Certificado Digital.
- Después de haber ingresado a la opción, se observa una pantalla con la opción de adjuntar la clavé pública, en cuanto ingrese y apriete “Obtener Certificado Digital” obtendré el certificado de la misma clave pública.

- Por seguridad no obtendrá de la clave privada.

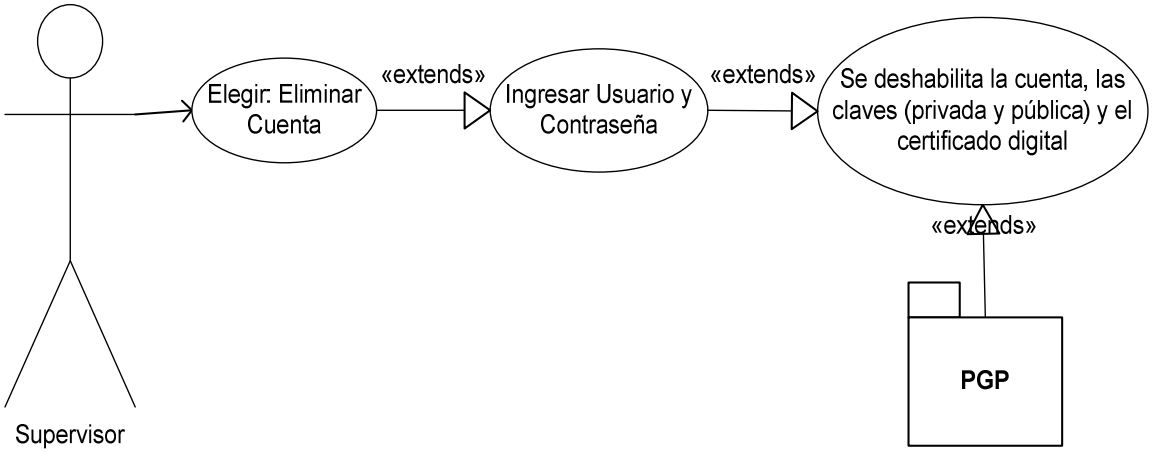
Figura 5.11: Caso de uso para la identificación de la Firma Digital por Certificado Digital



Fuente: Elaboración Propia

i. Eliminar el servicio de Firmas y Certificados Digitales

Figura 5.12: Caso de uso para eliminar el servicio de Firmas y Certificados Digitales



Fuente: Elaboración Propia

- La principal función que realiza el usuario (como se observa en la figura 5.12) en el presente caso de uso es elegir la opción de Borrar Firma Digital.
- Después de haber ingresado a la opción, se observa una pantalla solicitando usuario y contraseña, si son contestados correctamente, se deshabilita la cuenta, las claves (privada y pública) y el certificado digital.

Se **concluye** que el desarrollo de lo casos de uso nos sirvieron para determinar el correcto funcionamiento del sistema y la interacción con el usuario.

Por lo expuesto anteriormente se llega a la **conclusión** que habiéndose realizado el análisis de requerimientos a través de la técnica de Gauge y Weinberg, y el Modelado de Casos de Usos para determinar el funcionamiento del “Sistema de Administración de Firmas y Certificados Digitales”, logrando obtener los requisitos necesarios para proseguir con el diseño del Modelo Lineal Secuencial.

5.3.3 Diseño del Sistema (Diseño Lógico)

El proceso del diseño traduce los requisitos en una representación del software donde se puede evaluar su calidad antes de que comience la codificación. El diseño del software se centran en cuatro atributos distintos de programa:

- Modelado del Análisis
    - 1° Atributo: Diagrama entidad-relación (DER)
    - 2° Atributo: Diagrama de flujo de datos (DFD)
    - 3° Atributo: Diccionario de datos (DD)
- 4° Atributo: Diseño de Interfaz de Usuario (DIU)
- 5ª Atributo: Funcionalidad del Sistema (FS)

Los cuales son desarrollados a continuación.

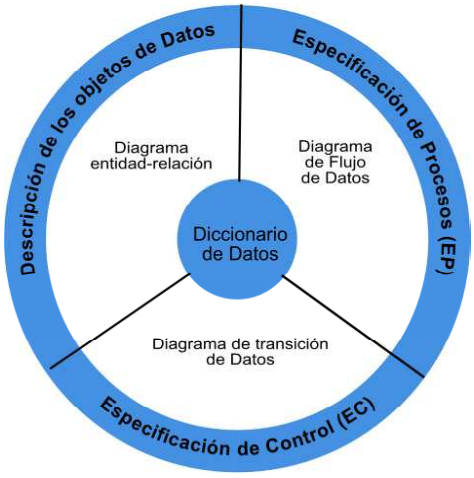
5.3.3.1 Modelado del Análisis

El modelado del análisis coadyuva a desarrollar el software, mediante una integración de las necesidades del usuario y diseño de herramientas para su construcción. El modelado de análisis (ver figura 5.13) tiene los siguientes fines:

- Describir lo que requiere el cliente.
- Establecer una base para la creación de un diseño de software
- Definir un conjunto de requisitos que se pueda validar una vez que se construya el software.

Para lograr estos objetivos, el modelo de análisis basado en el análisis estructurado toma la siguiente forma.

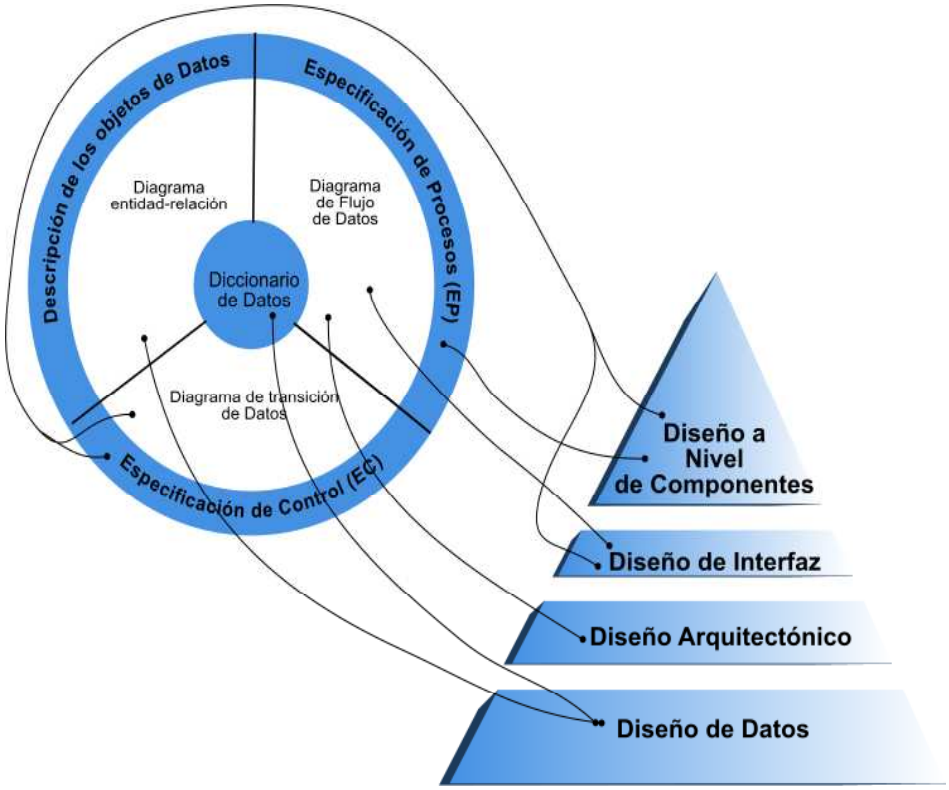
Figura 5.13: La estructura del modelo de análisis



Fuente: Roger Pressman, Ingeniería de Software

El mismo se relaciona al diseño del sistema a través de la conversión de análisis en un diseño de software explicado en la figura 5.14.

Figura 5.14: Estructura del Modelo Arquitectónico de Diseño



Fuente: Roger Pressman, Ingeniería de Software

La estructura del modelado arquitectónico diseña los siguientes puntos:

a. Diagrama entidad-relación (DER)

b. Diagrama de flujo de datos (DFD)

c. Diccionario de datos (DD)

Los cuales son desarrollados a continuación:

a) Diagrama entidad- relación (DER)

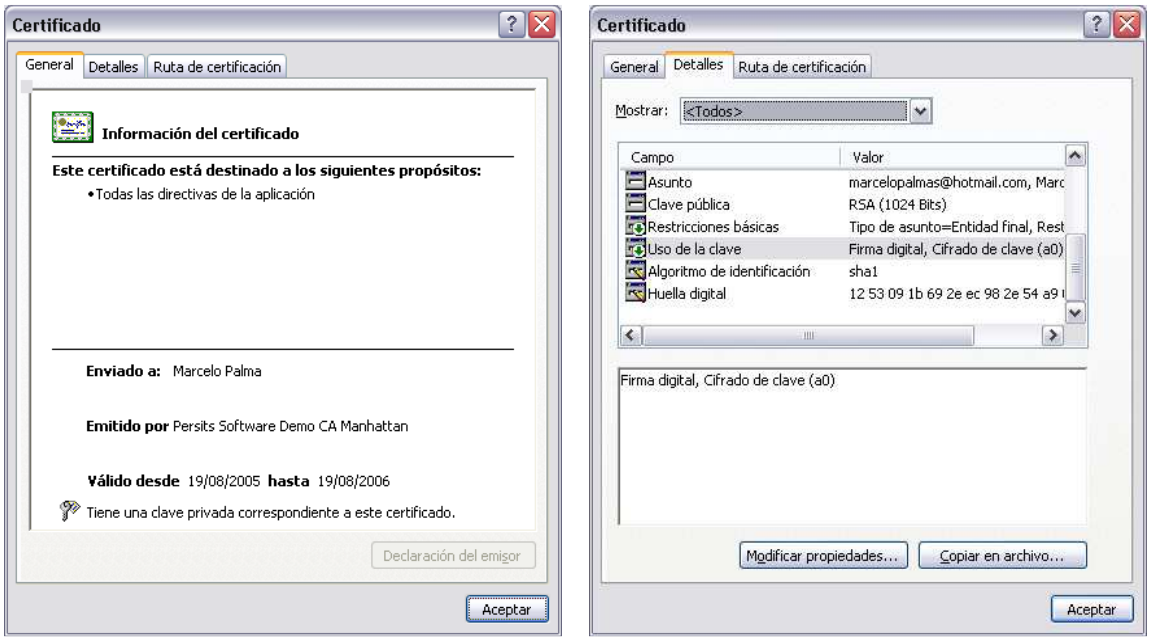
El diagrama entidad-relación representa las relaciones de los objetos de datos. A continuación se desarrolla el modelo entidad-relación hasta alcanzar las tres normalizaciones para el desarrollo de las base de datos:

Primera Normalización:

En la primera normalización se determinar los objetos de datos o las entidades llamadas ligaduras, con sus atributos o campos:

- Usuarios (**IDU**, nombres, apellidos, Departamento, e-mail, Tipo_cuenta)
- Firma Digital (**llave_publica**, llave privada, Valido_desde, Valido_hasta)

Figura 5.15: Modelo de Certificados Digitales X.509



Fuente: Microsoft Corporation

- Certificado Digital: se utilizo el Estándar Internacional **ITU X.509 S** para determinar los campos y sus atributos del certificado digital descritos en la **figura 5.15** (Version, **Numero_de_Serie**, Algoritmo_de_Firma, Emisor,

Valido_desde, Valido_hasta, Asunto, llave_Publica, restricciones_basicas, uso_de_la_clave, algoritmo_de_identificacion, huella_digital).

Segunda Normalización:

A continuación determinamos que tipo de atributos utilizan los datos de las entidades.

Usuarios: Los atributos de los campos de los usuarios son:

IDU: VARCHAR [4] – Identificador único del usuario – Llave Primaria de la tabla de Usuarios

Nombres: Char [10] – Nombres del usuario

Apellidos: Char [30] – Apellidos del usuario

Departamento: Char [30] – Departamento donde trabaja

E-mail: Char [20] – El E-mail de SITTEL el cual el usuario tiene asignado

Tipo_Cuenta: Num[1]

Firma Digital: Los atributos de los campos de las firmas digitales son:

Llave_publica: Char [1024] – almacena la llave pública del usuario - Identificador único de la Firma Digital– Llave Primaria de la tabla de Firma Digital

Llave_privada: Char [1020] – almacena la llave privada del usuario

Valido_desde: Date – Fecha de creación de la firma

Valido_hasta: Date – Fecha de caducidad de la firma

Certificado Digital: Los atributos de los campos de los certificados digitales son:

Version: Char [8] – Versión del certificado digital

Numero_de_Serie: CHAR [48] – Identificador único del certificado digital – Llave Primaria de la tabla de Certificado Digital

Algoritmo_de_Firma: Char [10] – Algoritmo de Encriptación de la Firma Digital

Emisor: Char [30] – Empresa emisora del certificado

Valido_desde: Date – Fecha de creación de la firma

Valido_hasta: Date – Fecha de caducidad de la firma

Asunto: Char [30] – E-mail del

Clave_Publica: Char [1024] – Copia de la clave pública

restricciones_basicas: Char [30] – El tipo de asunto de la firma digital

uso_de_la_clave: Char [30] – El empleo que se le da, en este caso Firma Digital

algoritmo_de_identificacion: Char [10] –Algoritmo de encriptación del Certificado Digital

huella_digital: Char [64] – Función Hash del Certificado Digital

Tercera Normalización:

Con el fin de obtener la tercera normalización se se obtiene las relaciones entre las entidades a través de las siguientes cuestiones:

Relación Usuario – Firma Digital

- Un usuario puede tener varias firmas digitales.
- Una firma digital puede tener un usuario.
- Por lo tanto la relación es **1:N**, porque **1 usuario** puede tener **N firmas digitales**.
    - Se deberá crear la tabla **crea** con el campo IDUFD Char [4] que relaciona a la tabla usuario con la tabla firma digital con una relación 1:N.
    - Se generó la tabla crea y las relaciones con las otras tablas obteniendo dos campos nuevos en la tabla crea, las llaves primarias de las tablas usuario (IDU) y firma digital (llave_publica), logrando la entidad – relación entre las tablas.

Relación Usuario – Certificado Digital

- Un usuario puede tener varios certificados digitales
- Una certificado digital puede tener un solo usuario
- Por lo tanto la relación es **1:N**, porque **1 usuario** puede tener **N certificados digitales**.
    - Se deberá crear la tabla **crea** con el campo IDUCD Char [4] que relaciona a la tabla usuario con la tabla certificado digital con una relación 1:N.

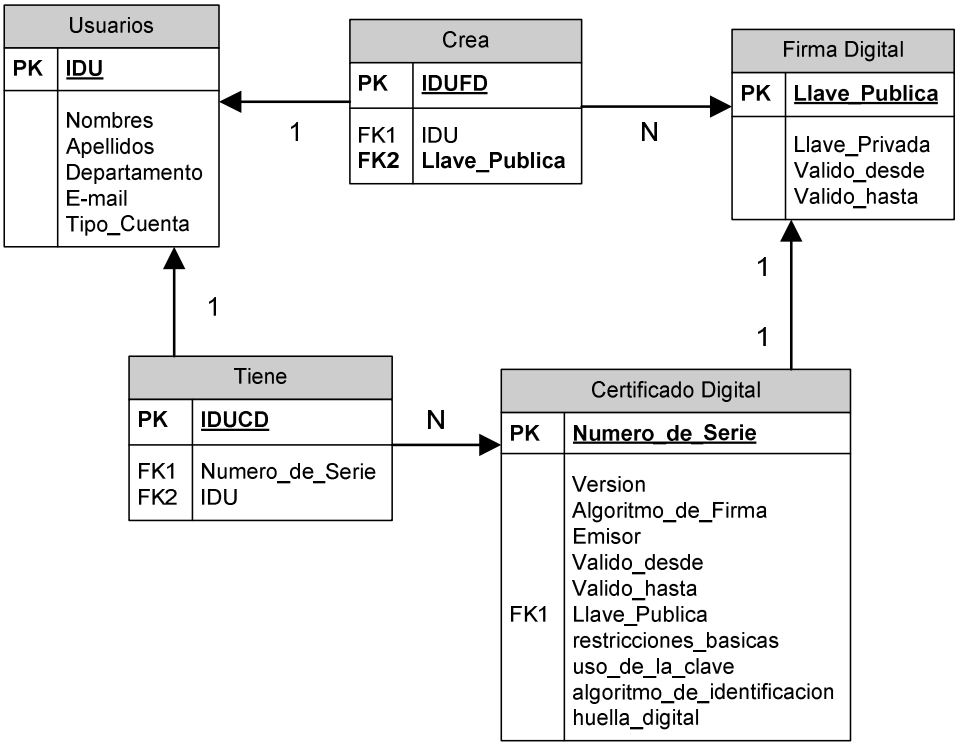
- Se generó la tabla tiene y las relaciones con las otras tablas obteniendo dos campos nuevos en la tabla crea, las llaves primarias de las tablas usuario (IDU) y certificado digital (numero_de_serie), logrando la entidad – relación entre las tablas.

Relación Firma Digital – Certificado Digital

- Una Firma Digital puede tener un Certificado Digital.
- Un Certificado Digital puede tener una Firma Digital
- Por lo tanto la relación es **1:1**, porque **1 firma digital** puede tener 1 **certificado digital**.
  - No se genera ninguna tabla adicional entre la relación de las tablas firma digital y certificado digital porque su relación es 1:1.

Con lo cual se genera el diagrama entidad relación en la figura 5.16.

Figura 5.16: Base de Datos Normaliza - Firmas Digitales



Fuente: Elaboración Propia

Se llega a la **conclusión** que habiéndose realizado el diagrama entidad-relación para el modelado de datos, se puede proseguir con el proceso de Modelado del Sistema para completar el Diseño Lógico del Modelo Lineal Secuencial.

b) Diagrama de flujo de datos (DFD)

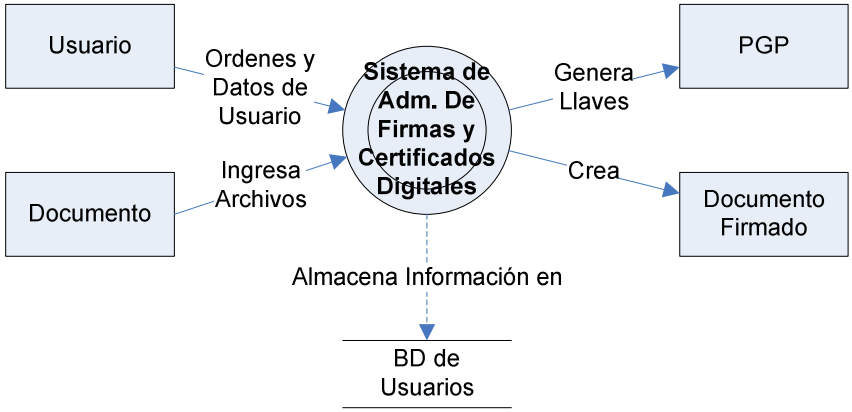
Un *diagrama de flujo de datos (DFD)* nos ayudó a desarrollar los modelos del ámbito de información y del ámbito funcional simultáneamente. Su utilización coadyuva a refinar la estructura del flujo de datos y refina en mayores niveles de detalle el sistema generando una mayor descomposición funcional del sistema. Funciona de la siguiente manera:

- A través del análisis léxico utilizado en los casos de uso, se analiza los verbos (acciones) que efectúa la información y se determina los flujos de información.
- Se realizó el DFD para los siguientes Casos:
    i. *Ingreso al Sistemas, iniciar sesión y selección de opciones*
    ii. *Inscripción y obtención de Claves Asimétricas*
    iii. *Recuperación y Modificación de Datos de Contraseña de la Firma Digital*
    iv. *Proceso de Firmado Digital*
    v. *Proceso de Autentificación de un mensaje por Firma Digital*
    vi. *Gestión de Claves Públicas y Anillos Públicos*
    vii. *Gestión de Usuarios*
    viii. *Autentificación de Firma Digital por Certificado Digital*
    ix. *Eliminar el servicio de Firmas y Certificados Digitales*
    x. *Cerrar Sesión del Programa*

Los DFD son desarrollados a continuación:

El nivel 0 o nivel contextual refleja al software o al sistema como una sola burbuja (ver figura 5.17).

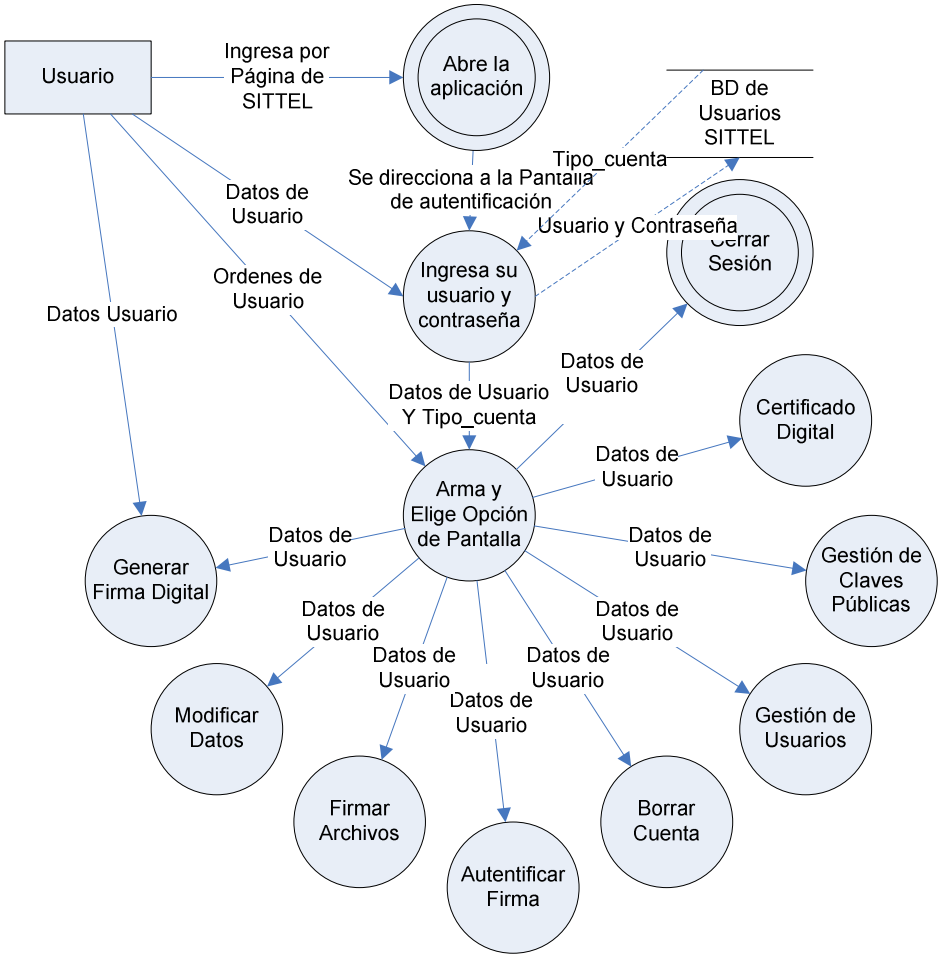
Figura 5.17: DFD de Nivel Contextual para el Sistema



Fuente: Elaboración Propia

i. Ingreso al Sistemas y selección de opciones

Figura 5.18: DFD de nivel 1 para Sistema de Administración de Firmas y Certificados Digitales

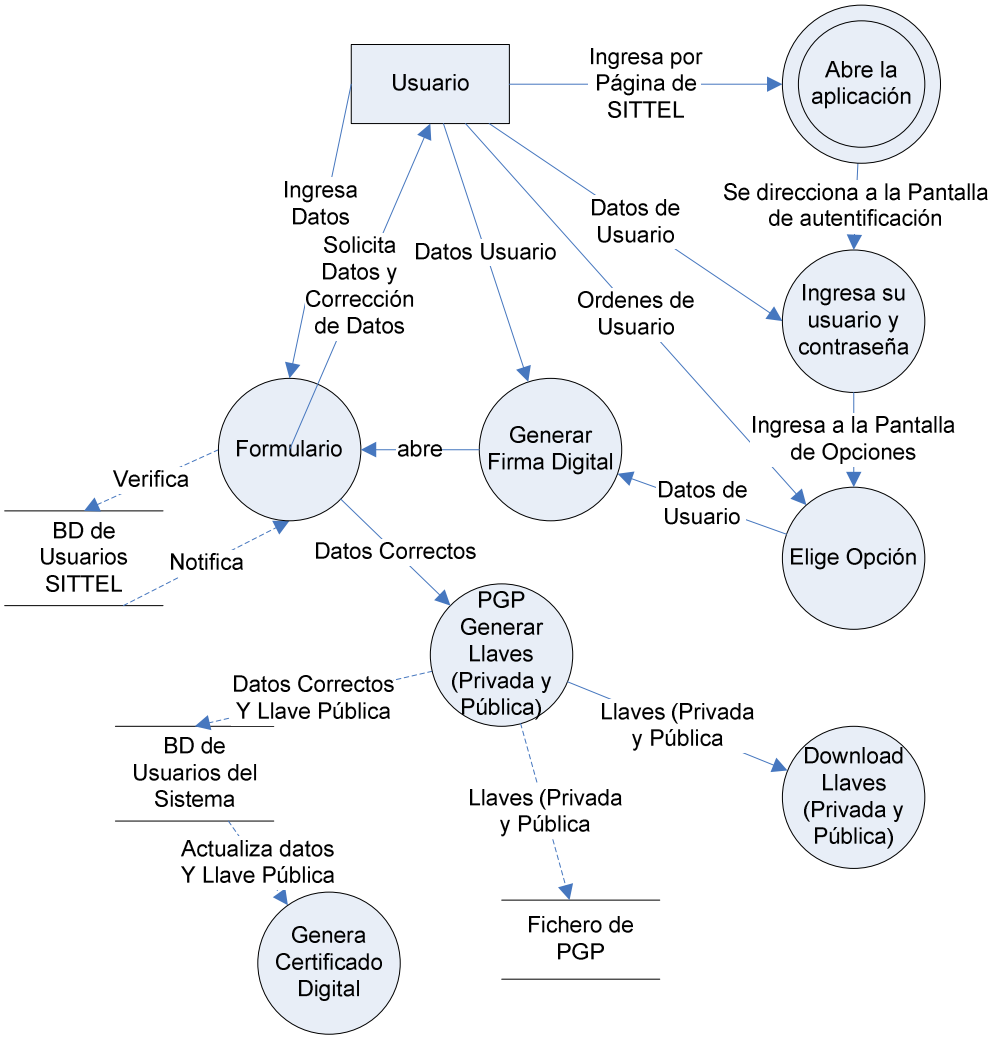


Fuente: Elaboración Propia

- Las principales tareas realizadas por el usuario (como se observa en la figura 5.18) será ingresar al sistema y elegir alguna de las opciones mencionadas en el inciso b.
- El usuario podrá elegir las ocho opciones básicas del sistema, las cuales son inscribirse y obtener sus claves asimétricas, recuperar y modificar su contraseña de firma digital, realizar el firmado digital, autentificación de un mensaje por firma digital, gestión de llaves públicas y anillos públicos, gestión de claves privadas y anillos privados.

ii. Inscripción y obtención de Claves Asimétricas

Figura 5.19: DFD de nivel 2 para inscripción y obtención de Claves Asimétricas



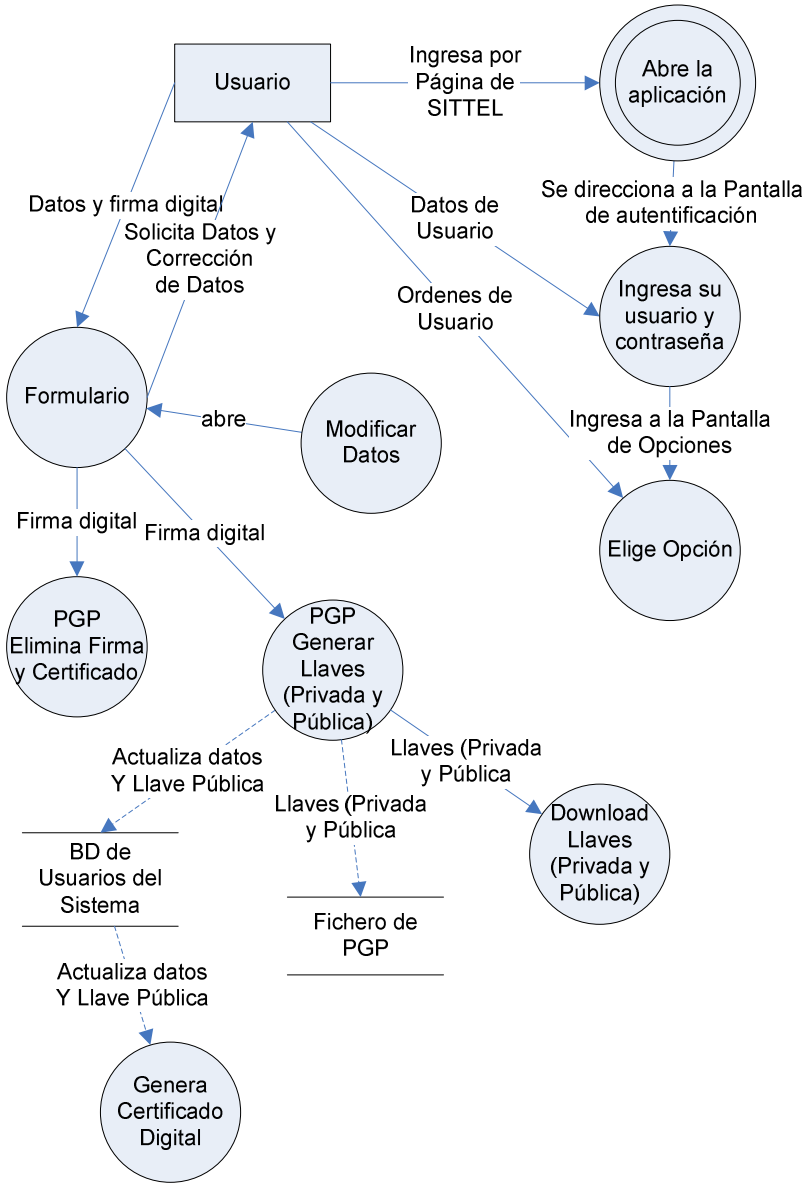
Fuente: Elaboración Propia

La principal función que realiza el usuario (como se observa en la figura 5.19) en el presente caso de uso es elegir la opción de Generar Firma Digital, después ingresa a un formulario.

Al llenar los datos correctamente ingresará a otra pantalla donde podrá descargar sus llaves (privada y pública).

iii. Recuperación y Modificación de Datos de Contraseña de la Firma Digital

Figura 5.20: DFD de nivel 2 para recuperar y modificar datos de la contraseña de la firma digital



Fuente: Elaboración Propia

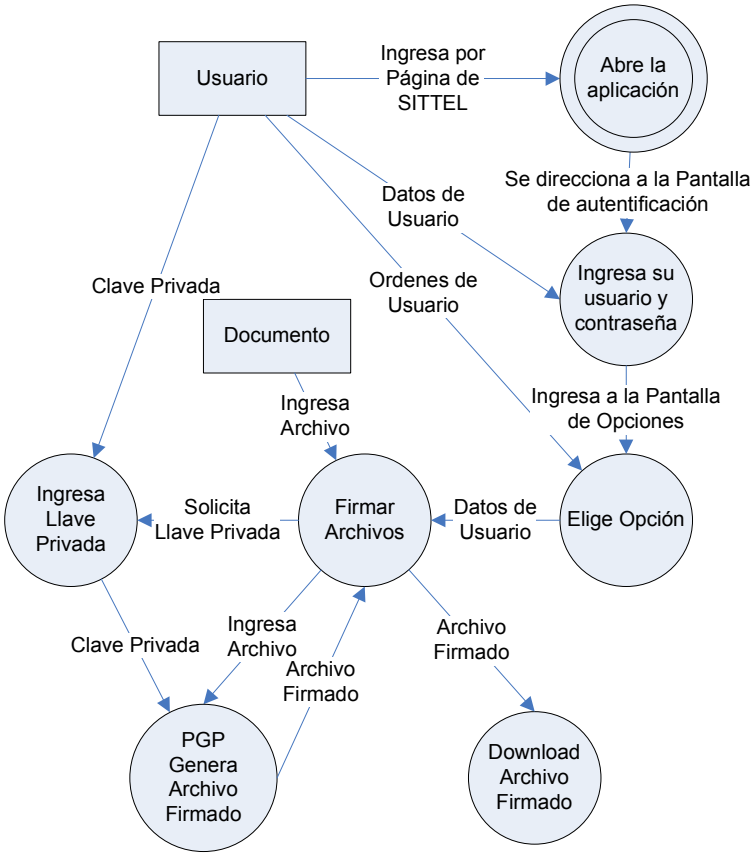
La principal función que realiza el usuario (como se observa en la figura 5.20) en el presente DFD es elegir la opción de Modificar Datos.

Después ingresará a un formulario el cual pedirá llenar su usuario y contraseña antigua, en cuanto ingrese correctamente sus datos le solicitará actualizar sus datos, inmediatamente se generara una nueva firma digital.

Si en caso que no recordará su contraseña, el sistema le pedirá ingresar su usuario y Correo Electrónico de SITTEL, en cuanto ingrese correctamente los datos se enviará un correo electrónico con sus datos.

iv. Proceso de Firmado Digital

Figura 5.21: DFD de nivel 2 para Firmado Digital de un archivo



Fuente: Elaboración Propia

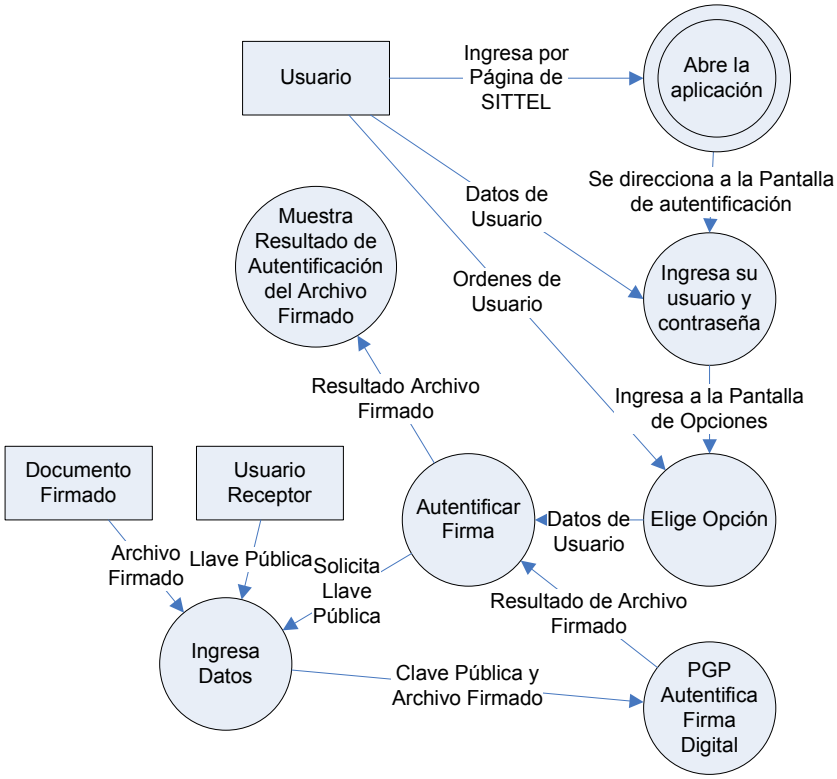
La principal función que realiza el usuario (como se observa en la figura 5.21) en el presente DFD es elegir la opción de Firmar Archivo.

En cuanto ingrese a la opción de “Firmar Archivo” aparecerá una pantalla solicitando su usuario y contraseña, a continuación se pedirá su clave privada y el archivo para firmarlo, después aparecerá una página para descargar el archivo firmado y listo para ser enviado.

En caso que se introdujera datos incorrectos en la autentificación del usuario, no ingresará y seguirá pidiendo los datos correctos.

v. Proceso de Autentificación de un mensaje por Firma Digital

Figura 5.22: DFD de nivel 2 para Autentificación del origen del mensaje



Fuente: Elaboración Propia

La principal función que realiza el usuario (como se observa en la figura 5.22) en el presente DFD es elegir la opción de Autentificación por Firma Digital.

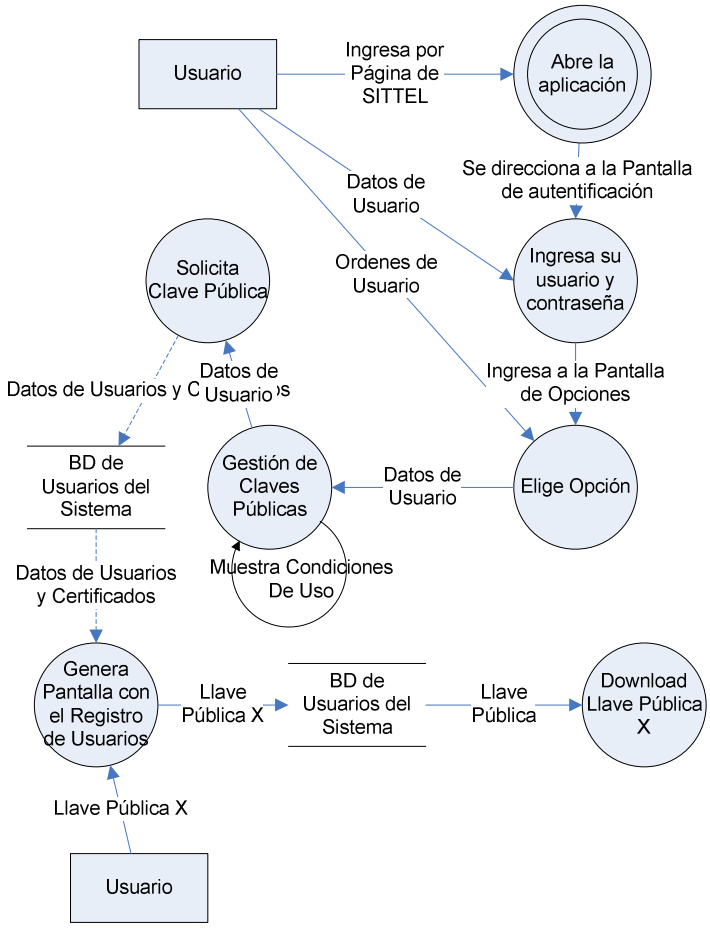
En cuanto tenga el archivo firmado y la clave pública del emisor para su autentificación, ingresará a la opción de autentificación del usuario, deberá adjuntar el archivo y la clave pública, apretar el botón de ”autentificación de Usuario”, consecuentemente aparecerá una pantalla con la respuesta afirmativa o negativo.

Si la respuesta es correcta mostrará en la misma pantalla el certificado digital de la clave pública.

En caso que se introdujera archivos incorrectos en la autentificación del usuario, no verificará la autenticidad y seguirá pidiendo los datos correctos.

vi. Gestión de Claves Públicas y Anillos Públicos

Figura 5.23: DFD de nivel 2 para Gestión de Claves Públicas



Fuente: Elaboración Propia

La principal función que realiza el usuario (como se observa en la figura 5.23) en el presente DFD es elegir la opción de Clave Pública.

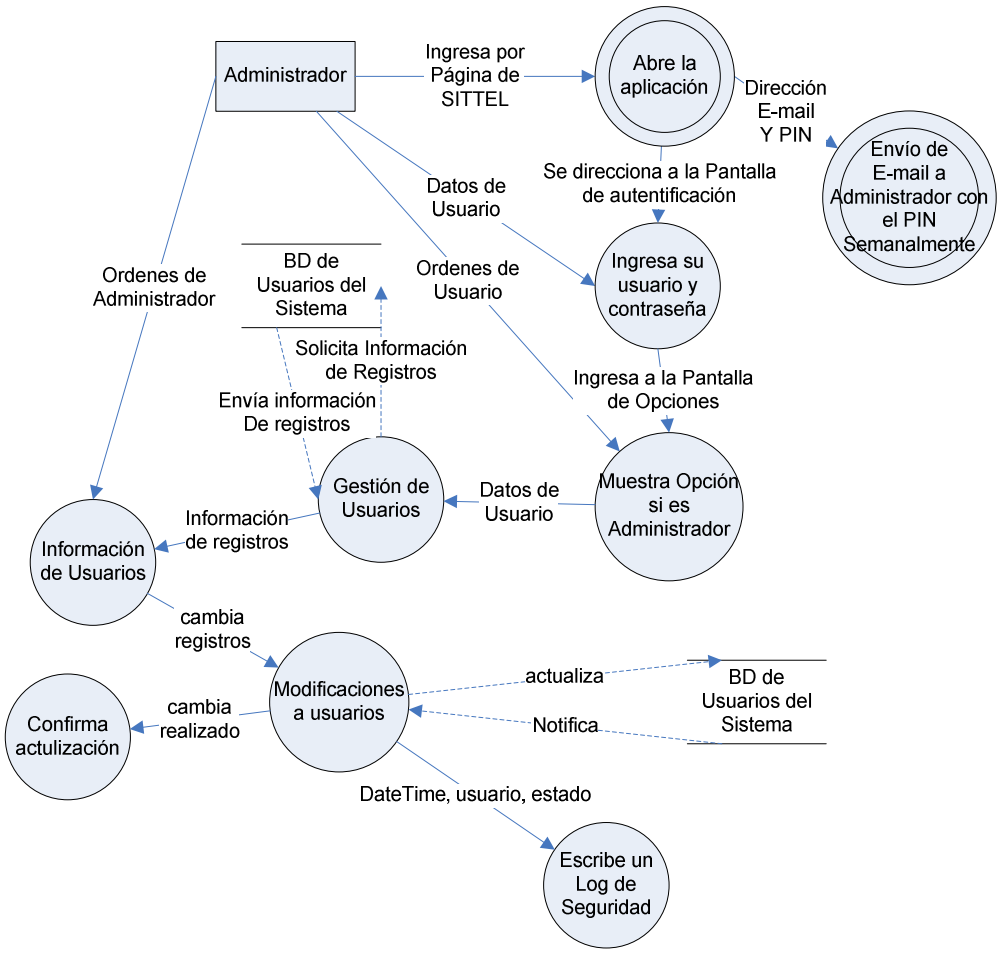
Después de haber ingresado a la opción, se observará una lista llaves públicas con los nombres respectivos de los propietarios y una opción para descargar la llave pública.

El portal le permitirá bajar la llave haciendo clic sobre la llave seleccionada y en cuanto se habrá la pantalla le pedirá su usuario y contraseña (necesario para mantener la integridad de la información de las llaves públicas).

Si la respuesta es correcta le permitirá bajar la llave, en caso que se introdujera un usuario desconocido o una contraseña incorrecta, no permitirá bajar la llave.

vii. Gestión de Usuarios

Figura 5.24: DFD de nivel 2 para la Gestión de Usuario



Fuente: Elaboración Propia

La principal función que realiza el **administrador** (como se observa en la figura 5.24) en el presente DFD es elegir la opción de Gestión de Usuarios.

Después de haber ingresado a la opción, le pedirá un usuario, su contraseña y un PIN (generado aleatoriamente y enviado semanalmente a su correo del administrador).

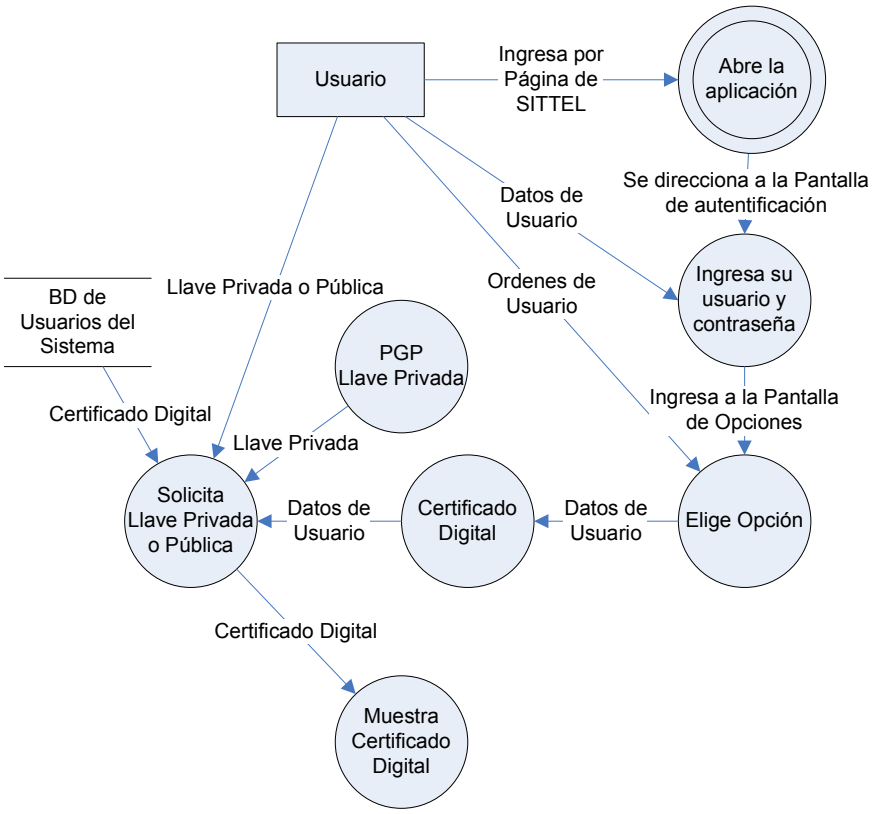
En cuanto ingrese observará los registros de los usuarios, identificando su estado, ID, nombre y apellido, llave pública, certificado digital, y unos botón para modificar su estado y datos.

En cuanto ingrese a modificar su estado y datos el administrador podrá actualizar los datos de la persona, deshabilitar en el caso que estuviera habilitado y habilitar en el caso de que estuviera deshabilitado, o eliminar la cuenta.

Cualquier cambio en esta opción estará registrado por un Log de seguridad.

viii. Identificación de Firma Digital por Certificado Digital

Figura 5.25: DFD de nivel 2 para la identificación de la Firma Digital por Certificado Digital



Fuente: Elaboración Propia

La principal función que realiza el usuario (como se observa en la figura 5.25) en el presente DFD es elegir la opción de Certificado Digital.

Después de haber ingresado a la opción, se observa una pantalla con la opción de adjuntar la clavé pública, en cuanto ingrese y apriete “Obtener Certificado Digital” obtendré el certificado de la misma clave pública.

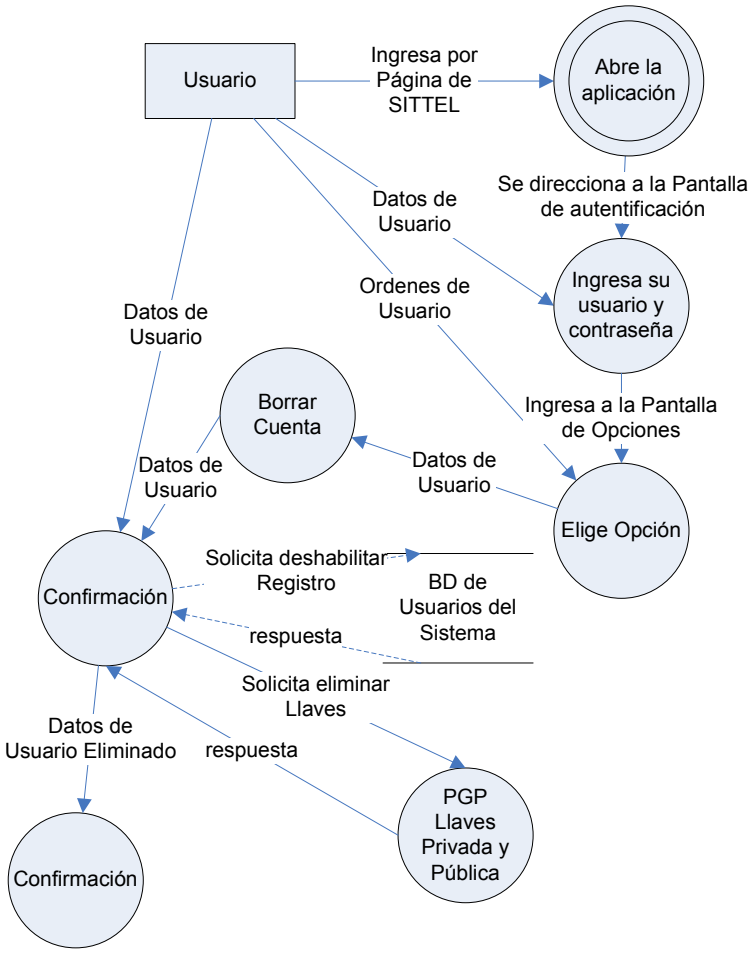
Por seguridad no obtendrá de la clave privada.

ix. Eliminar el servicio de Firmas y Certificados Digitales

La principal función que realiza el usuario (como se observa en la figura 5.26) en el presente DFD es elegir la opción de Borrar Firma Digital.

Después de haber ingresado a la opción, se observa una pantalla solicitando usuario y contraseña, si son contestados correctamente, se deshabilita la cuenta, las claves (privada y pública) y el certificado digital.

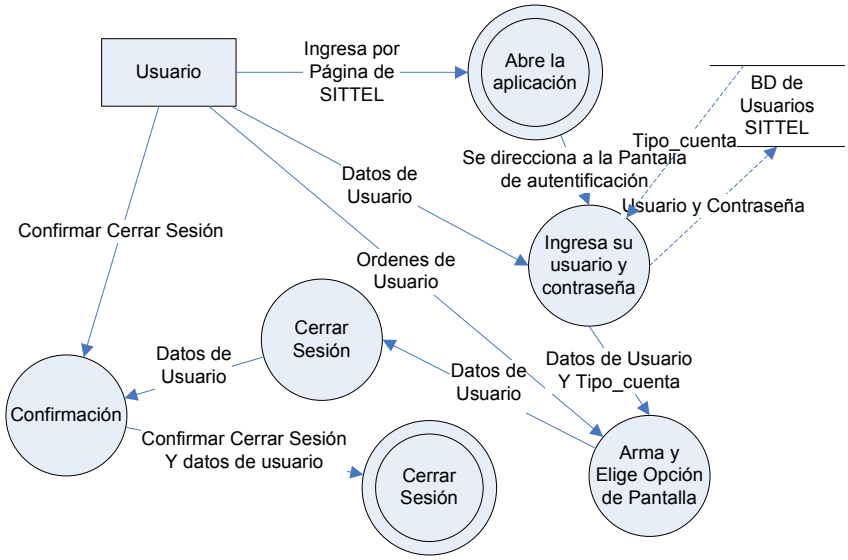
Figura 5.26: DFD de nivel 2 para eliminar el servicio de Firmas y Certificados Digitales



Fuente: Elaboración Propia

x. Cerrar Sesión

Figura 5.27: DFD de nivel 2 para eliminar el servicio de Firmas y Certificados Digitales



Fuente: Elaboración Propia

La principal función que realiza el usuario (como se observa en la figura 5.27) en el presente DFD es elegir la opción de Cerrar Sesión.

El programa cerrara la sesión del servidor al usuario que ingreso al programa.

Por lo expuesto anteriormente se llega a la **conclusión** que habiéndose realizado el diagrama de flujo de datos para el modelado del sistema en cada una de las situaciones previstas para el desarrollo, se puede proseguir con el proceso de Modelado del Sistema para completar el Diseño Lógico del Modelo Lineal Secuencial.

c) Diccionario de datos

El diccionario de datos es un listado organizado de todos los elementos de datos que son pertinentes para el sistema, con definiciones precisas y rigurosas que permiten al usuario y al ingeniero de software que tengan una misma comprensión de las entradas, salidas, de los componentes de los almacenes y de los cálculos intermedios. La estructura utilizada fue **nombre**, **alias**, **donde se usa/cómo se usa**; a continuación desarrollamos el Diccionario de Datos para el Sistema de Administración de Firmas y Certificados Digitales.

Nombre:	Usuario
Alias:	Ninguno
Donde/Cómo se usa:	Es el cliente final, el cual tiene interacción con el sistema a través de su usuario y contraseña, ingresa información y el sistema genera información de salida útil para el usuario.

Nombre:	Administrador
Alias:	Ninguno
Donde/Cómo se usa:	Tiene todos los privilegios del usuario y la posibilidad de modificar, habilitar y deshabilitar a un usuario a través de la opción de Gestión de Usuarios.

Nombre:	Contraseña
Alias:	Ninguno
Donde/Cómo se usa:	Contraseña de tiene cada usuario para ingresar al sistema.

Nombre:	BD de Usuarios SITTEL
Alias:	Ninguno
Donde/Cómo se usa:	Base de Datos de usuarios en SITTEL, el cual es utilizado para que el usuario ingrese al sistema por primera vez y se autentifique mediante su usuario y contraseña utilizada en SITTEL, genere sus llaves privada y pública.

Nombre:	BD de Usuarios del Sistema
Alias:	Ninguno
Donde/Cómo se usa:	Base de Datos de usuarios del Sistema de Administración de Firmas y Certificados Digitales, su fin es almacenar información del usuario, contraseña del sistema y su llave pública para genera el Certificado Digital de la Firma Digital.

Nombre:	Llave Privada
Alias:	Ninguno
Donde/Cómo se usa:	Es la clave privada solo conocido por el usuario, ni el administrador tendrá acceso a obtener la llave, su ubicación es dentro de un fichero de PGP y se encuentra encriptada, ayuda a firmar documento y archivos.

Nombre:	Llave Pública
Alias:	Ninguno
Donde/Cómo se usa:	Es la clave pública, esta a disposición de cualquier usuario del sistema a través de la opción de Gestión de Claves Públicas, ayuda a autentificar a un usuario por su certificado digital.

Nombre:	Generar Firma
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 2 del Diagrama de Flujo de Datos un usuario puede generar su propia firma digital y automáticamente el sistema genera su certificado digital, en el proceso interactuamos con el criptosistema PGP para generar las llaves pública y privada.

Nombre:	Modificar Datos
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 3 del Diagrama de Flujo de Datos un usuario puede modificar sus datos, incluido su contraseña, y automáticamente el sistema genera su nueva firma digital, su certificado digital y actualiza la BD del sistema.

Nombre:	Firmar Archivos
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 4 del Diagrama de Flujo de Datos un usuario puede generar su firma digital sobre un archivo y obtener el archivo firmado, el mismo interactúa con el criptosistema PGP.

Nombre:	Autentificar Firma
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 5 del Diagrama de Flujo de Datos un usuario para autentificar el origen del mensaje utiliza la clave pública para utilizar en la opción de la firma digital y autentificar si el documento o archivo firmado pertenece al emisor, la opción solicita el archivo firmado y la llave publica del emisor, y devuelve el valor positivo si existe relación entre el archivo firmado y la llave pública y negativo si no existe relación entre la llave y el archivo.

Nombre:	Gestión de Claves Públicas
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 6 del Diagrama de Flujo de Datos un usuario puede obtener las llaves públicas de diferentes usuarios y utilizarlas para autentificar los mensajes enviados por el mismo, al mismo tiempo que descarga las mismas se genera un Log de seguridad para evitar suplantación de usuarios.

Nombre:	Gestión de Usuarios
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 7 del Diagrama de Flujo de Datos el administrador puede modificar datos, habilitar y deshabilitar a usuarios, además se genera un Log de seguridad el cual almacena los cambios realizados, para ingresar al mismo necesitara autentificarse en la opción e introducir el PIN almacenado en su correo electrónico que es actualizado semanalmente.

Nombre:	Certificado Digital
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 8 del Diagrama de Flujo de Datos un usuario puede autentificar las llaves públicas adquiridas por otros usuarios del sistema y autentificar su llave privada, la opción consiste en ingresar cualquiera de estas llaves dependiendo de su necesidad y el sistema le mostrará el certificado digital de la llave con los datos del usuario, caducidad, etc.

Nombre:	Borrar Cuenta
Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 9 del Diagrama de Flujo de Datos un usuario puede eliminar su cuenta, quedando deshabilitado el registro para registro del historial, eliminando sus llaves privadas, públicas y su certificado digital.

Nombre:	Cerrar Sesión

Alias:	Ninguno
Donde/Cómo se usa:	A través de los pasos indicados en el punto 10 del Diagrama de Flujo de Datos un usuario **debe** cerrar sesión al terminar sus tareas en el sistema de información, quedando deshabilitado las acciones del usuario mientras no vuelva a autentificarse con el servidor.

Nombre:	Pretty Good Privacy
Alias:	PGP
Donde/Cómo se usa:	Criptosistema utilizado para el desarrollo del sistema, se basa en criptosistemas RSA para generar las llaves públicas y privadas, SHA para generar la función resumen o Hash, y utiliza los anillos que son un conjunto de ficheros encriptados donde almacena las llaves.

Nombre:	Documento
Alias:	Ninguno
Donde/Cómo se usa:	Documento o Archivo a ser introducido en la opción de Firmar Documento para generar un Hash, encriptar el hash con la llave privada y se adjunta al documento el hash encriptado llamado Firma Digital.

Nombre:	Documento firmando
Alias:	Ninguno
Donde/Cómo se usa:	Documento o Archivo que se encuentra adjunta la firma digital, se introducido en la opción de Autentificar Firma para generar un hash del archivo y desencriptar la firma digital a través de la llave pública, si los valores de los hash son iguales se autentifica la procedencia del archivo.

Por lo expuesto anteriormente se llega a la **conclusión** que habiéndose realizado el diccionario de datos para todos los elementos permitentes del sistema, se puede proseguir con el diseño de interfaz de usuario para completar el Diseño Lógico del Modelo Lineal Secuencial.

5.3.3.2 Diseño de Interfaz de Usuario

El diseño de la interfaz de usuario es la categoría de diseño que crea un medio de comunicación entre el hombre y la máquina. Con un conjunto de principios para el diseño de la interfaz se determino las siguientes reglas de oro:

- Dar el control al usuario: Se lo realizará mediante las múltiples opciones que utilizaremos al desarrollar el software.
- Reducir la carga de memoria del usuario: Se utilizará como se indico paquetes de diseño gráfico (DreamWeaver, PhotoShop) los cuales redicen entre un 30% a 80% el tamaño de las imágenes y la aplicación será utilizada en una Intranet, obteniéndose gran prestancia en la velocidad de la transferencia de información, pudiendo llegar a 100 Mbps.

- Construir una interfaz consecuente: Se construyo una interfaz similar a SITTEL (ver figura 5.28), consecuentemente se desarrollo una pantalla interactiva que no modifique el espacio vectorial de la pantalla en interfaz web. Consecuentemente la interfaz será la misma para cada una de las opciones.

Se utilizó el modelo de diseño para usuarios principiantes por no tener conocimientos generales, ni conocimientos sintácticos[35] ni conocimientos semánticos[36] de la utilización de la aplicación o del Sistema de Administración de Firmas y Certificados Digitales, ni el manejo de Criptosistemas como el PGP.

Figura 5.28: Pagina Actual de SITTEL

Fuente: Superintendencia de Telecomunicaciones ©2005

Como se observa la figura 5.28 muestra la actual página web, desarrollada en una interfaz web, utiliza una cabecera, debajo tres columnas, la columna izquierda esta compuesto por

[35] En el contexto el conocimiento sintáctico se refiere a la mecánica de interacción que se requiere para utilizar la interfaz de forma eficaz.
[36] El conocimiento semántico se refiere al sentido subsiguiente de aplicación –una comprensión de la realización de todas las funciones, del significado de entrada y salida, de las metas y objetivos del sistema–.

hipervínculos a las opciones principales de la página, la columna derecha hace un enlace a las noticias secundarias o no relevantes de SITTEL y la columna central donde trabajara el Sistema de Administración de Firmas y Certificados Digitales esta compuesta por las noticias principales o relevantes de SITTEL.

Respecto a un análisis de colores se utilizara los colores del logo de SITTEL:

- **Azul:** Utilizado en negocios donde intervenga la verdad, curación, tranquilidad, estabilidad, paz, armonía, sabiduría, confianza, calma, certeza, protección, seguridad, lealtad Significado internacional: China = inmortalidad; Hindúes = color de Krishna. Utilizada en empresas Tecnológicas.
- **Azul claro:** Utilizado en negocios donde intervenga la paz, tranquilidad, silencio, frialdad, limpieza, suavidad, pureza, entendimiento. Utilizado en iglesias y centros de acogimiento espiritual.
- **Gris neutro:** Utilizado en negocios donde intervenga la neutralidad, empresa, clásico, práctico, frialdad, temporalidad, silencio, calidad. Utilizado en empresas clásicas.

Y para finalizar la interfaz tendría la siguiente forma:

Figura 5. 29: Interfaz del Sistema de Administración de Firmas y Certificados Digitales

Fuente: Elaboración Propia

Con lo expuesto anteriormente se llega a la **conclusión** que habiéndose realizado el diseño de la interfaz de usuario y habiéndose catalogado como una interfaz de usuario principiante, se puede proseguir el Desarrollo del Modelo Lineal Secuencial para las

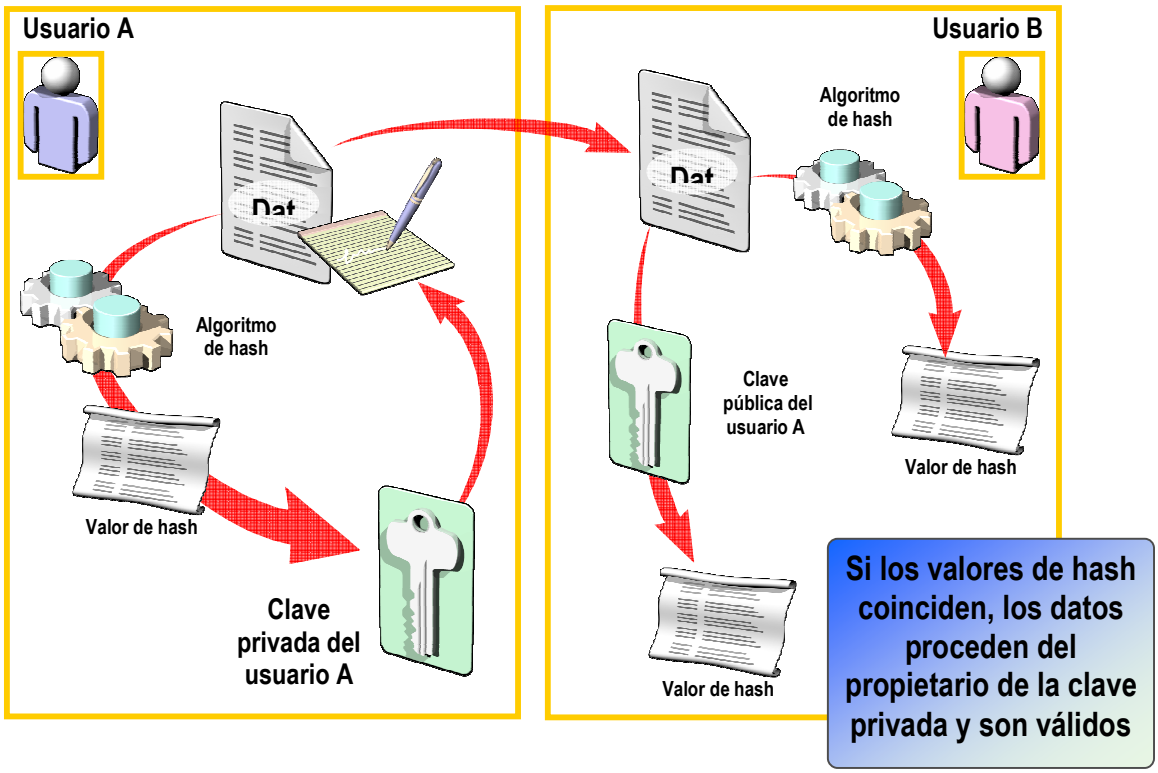
Firmas Digitales y Certificados Digitales para completar la fase de Diseño del Sistema (Diseño Lógico).

5.3.3.3 Funcionalidad del Sistemas

La funcionalidad del Sistema es catalogada desde el funcionamiento de las firmas digitales y certificados digitales desarrollados a continuación:

a. Funcionalidad de las Firmas Digitales

Figura 5. 30: Funcionamiento de una Firma Digital



Fuente: Microsoft ©2004

Cuando se firman datos con una firma digital ocurre lo siguiente:

- Se aplica un algoritmo de hash a los datos para crear un valor de hash.
- Se cifra el valor de hash con la clave privada del usuario A, creando así la firma digital.
- Se envía al usuario B la firma digital y los datos.

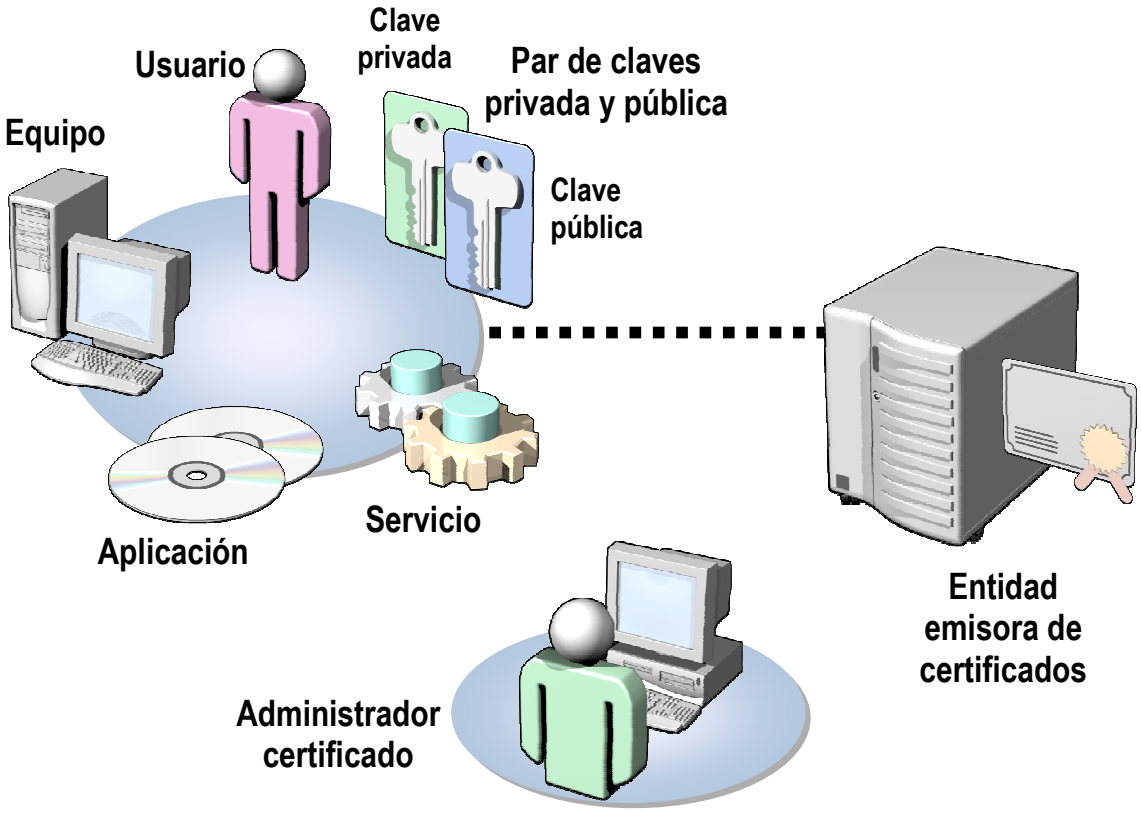
Cuando se descifran datos firmados digitalmente ocurre lo siguiente:

- El usuario B descifra la firma mediante la clave pública del usuario A y después recupera el valor de hash. Si la firma se puede descifrar, el usuario B sabe que los datos proceden del usuario A (o del propietario de la clave privada).
- Se aplica el algoritmo de hash a los datos para crear un segundo valor de hash.
- Se comparan los dos valores de hash. Si los valores de hash coinciden, el usuario B sabe que no se han modificado los datos.

El diseño de las firmas digitales se basa en su funcionamiento (ver figura 5.30):

b. Funcionalidad de los Certificados Digitales

Figura 5. 31: Funcionamiento de los Certificados Digitales



Fuente: Microsoft ©2004

Respecto a los certificados digitales tiene lugar el siguiente proceso:

1. Un usuario, equipo, servicio o aplicación crea el par de claves pública y privada.

2. La clave pública se transmite a la entidad emisora de certificados (CA) a través de una conexión de red segura.
3. El administrador certificado examina la solicitud de certificado para comprobar la información.
4. Para la aprobación, el administrador certificado firma la clave pública con la clave privada de la CA.

El diseño de las firmas digitales se basa en su funcionamiento (ver figura 5.31):

Conclusión

Se llega a la **conclusión** que habiéndose diseñado el funcionamiento de las firmas y certificados digitales, se completó el Desarrollo del Modelo Lineal Secuencial para las Firmas Digitales y Certificados Digitales en la fase de Diseño del Sistema (Diseño Lógico).

5.3.4 Desarrollo del Sistema (Diseño Físico)

El diseño se debe traducir en una forma legible por la máquina. El paso de generación de código lleva a cabo esta tarea. Si se lleva a cabo el diseño de una forma detallada, la generación de código se realiza mecánicamente.

A continuación se desarrolla el código fuente del Generador de Firmas Digitales y el autentificador.

Código Fuente Generador de Firma Digital

```
<HTML>
<HEAD>
<TITLE>AspEncrypt - Client-Side Digital Signing</TITLE>
<OBJECT
    classid="CLSID:F9463571-87CB-4A90-A1AC-
2284B7F5AF4E"
    codeBase="aspencrypt.dll"
    id="XEncrypt">
</OBJECT>
<SCRIPT LANGUAGE="VBSCRIPT">
Sub Sign
    ' Open "MY" certificate store which contains client certs
    Set Store = XEncrypt.OpenStore("MY", False )
    ' Does the store contain certificates?
    Count = Store.Certificates.Count
    If  Count = 0 Then
        MsgBox "You have no certificates."
        Exit Sub
    End If
    ' If store contains more than one, enable user to pick
one
    If Count > 1 Then
        Set Cert = XEncrypt.PickCertificate(Store, 4+8+16,
"Select Certificate Please", "Select the one you want to be
used for signing")
        If Cert Is Nothing Then Exit Sub
    ' Make sure the cert has a private key associated with it
    If Cert.PrivateKeyExists = False Then
        MsgBox "This certificate has no private key
associated with it."
        Exit Sub
    End If
    ' obtain private key context for this cert
    Set Context = Cert.PrivateKeyContext
    ' create empty hash object associated with this context
    Set Hash = Context.CreateHash
    Hash.AddText document.frmSign.txtToSign.value
    Set Blob = Hash.Sign(Context.KeySpec)
    document.frmSign.txtSignature.value = Blob.Base64
End Sub
</SCRIPT>
</HEAD>
<BODY>
<FORM NAME="frmSign" ACTION="verify.asp">
Text to sign:<BR>
<TEXTAREA NAME="txtToSign" COLS="80"
ROWS="3">Hello World!</TEXTAREA><BR>
<INPUT TYPE="BUTTON" OnClick="Sign" VALUE="Sign">
<P>
<TEXTAREA NAME="txtSignature" COLS="80"
ROWS="3"></TEXTAREA>
<P>
```

```
    Else
        ' otherwise just pick that only one cert
        Set Cert = Store.Certificates(1)
    End If
```

```
<INPUT TYPE="SUBMIT" VALUE="Submit for verification">
</FORM>
</BODY>
</HTML>
```

Código Fuente del Autentificador de Firma Digital

```
<HTML>
<HEAD>
<TITLE>AspEncrypt - Verify.asp (signature verification)</TITLE>
</HEAD>
<BODY>
<%
    ' Verify digital signature using certificate's public key
    Set CM = Server.CreateObject("Persits.CryptoManager")
    Set Context = CM.OpenContext("mycontainer", True)
    Set Hash = Context.CreateHash
    ' add the same text to hash
    Hash.AddText Request("txtToSign")
    ' obtain certificate we will use for verification
    Set Cert = CM.ImportCertFromFile("d:\mycert.cer")
    Set Key = Context.ImportKeyFromCert( Cert )
    ' Put signature to be verified in a Blob object
    Set Blob = CM.CreateBlob
    Blob.Base64 = Request("txtSignature")
    Verified = Hash.VerifySignature(Blob, Key)
    If Verified Then
        Response.Write "Signature is verified."
    Else
        Response.Write "Signature is NOT verified."
    End If
%>
</BODY>
</HTML>
```

Con lo expuesto se llega a la **conclusión** que habiéndose realizado el Desarrollo Sistema del Modelo Lineal Secuencial, con el cual se completa el Desarrollo del Modelo Lineal Secuencial para las Firmas Digitales y Certificados Digitales.

Conclusiones del Capítulo

A la finalización del presente capítulo se llega a la conclusión que:

- La metodología del Modelo PHVA (Planificar, Hacer, Verificar y Actuar) ofreció un entorno organizado para realizar la auditoria de sistemas de seguridad con la herramienta ISO/IEC 17799 en SITTEL y comprobar que su mayor falencia se encuentra en prescindir de herramientas criptográficas para la protección de información.
- SITTEL No cumple con la Norma Boliviana ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información.
- En la ingeniería de software se utilizo el modelo de las 4P’s (proyecto, personal, producto y proceso) que nos coadyuvo o obtener los requisitos mínimos para el desarrollo del sistemas.
- El estudio de factibilidad realizado en Capítulo 4 complemento al desarrollo del Modelo Lineal Secuencial en la fase de Investigación Preliminar.

- Consecuentemente se utilizo el Modelo Lineal Secuencial para el Desarrollo del Sistema de Administración de Firmas y Certificados Digitales, el cual forma parte de la Fase de Proceso, ofreciendo información detallada y específica en sus fases de diseño y desarrollo del software (investigación preliminar, análisis de requisitos, diseño de sistema).
- El Modelo Lineal Secuencial fue utilizado para el desarrollo de las Firmas y Certificados Digitales, mostrando una de las pantallas utilizadas en la figura 5.29.
- Con el presente capítulo se cumple una parte del objetivo principal planteado en la sección 1.4.1, puesto que para realizar el desarrollo del Sistema es necesario realizar un previo análisis y diseño del mismo, y su entorno.

Capítulo 6
Garantía de Calidad del Software

"La calidad nunca es un accidente;
siempre es el resultado de un esfuerzo
de la inteligencia."

Jhon Ruskin

Resumen

El presente capítulo se centra en la finalización del Modelo Lineal Secuencial Prueba y Mantenimiento del software, consecuentemente se utilizó técnicas métricas para mejorar la calidad del desarrollo del software, y se realizó la comprobación de la hipótesis del proyecto de grado de firmas y certificados digitales.

El desarrollo del Modelo Lineal Secuencial nos coadyuvo a mejorar la calidad del software, sin embargo no se puede concluir ni implantar en la Superintendencia de Telecomunicaciones antes de realizar un análisis de prueba, mantenimiento y métricas de calidad de software, a continuación se desarrolla la subsección de prueba y mantenimiento para las Firmas y Certificados Digitales.

6.1. Prueba y Mantenimiento para las Firmas y Certificados Digitales

Dado el concepto de Prueba y Mantenimiento del Software en la Segunda Sección del Capitulo de Marco Teórico y Metodológico, y habiéndose desarrollado la Investigación Preliminar, el Análisis de Sistemas, el Diseño y Desarrollo para las Firmas y Certificados Digitales, se concreta a continuación el Modelo Lineal Secuencial[37] en las fases de Prueba y Mantenimiento desarrolladas en prosecución:

6.1.1. Prueba la Firma y Certificado Digital

Se diseño un modelo de prueba para el software consistente en la Prueba de Caja Blanca o Caja de Cristal descrito en la subsección 3.2 del Marco Teórico y Metodológico, el cual se basa en la lógica del programa y no en la especificación.

Las baterías de pruebas que se construye en base a la prueba de caja blanca, revisa el código fuente del software, proporcionando las **coberturas de sentencia, decisión y**

[37] Obtenido de http://www.ii.uam.es

condición, con el objetivo de alcanzar un nivel aceptable de calidad en el desarrollo del software, asegurándose el buen funcionamiento y la disminución del tiempo de mantenimiento.

Las tres coberturas son desarrolladas a continuación:

6.1.1.1. Cobertura de sentencia:

La cobertura de sentencia garantiza que se ejecuta cada sentencia del programa al menos una vez. Se utilizó los siguientes procesos para su verificación:

a) **Se verificó el proceso del firmado digital de un documento en cada uno de los procesos a ser realizados para la obtención de la signatura del documento por el modelo MD5, el cual tomó 512 bits del archivo, y produjo una salida de 128 bits mediante el siguiente proceso:**

   i. El primer bloque del mensaje, se inicializó en cuatro registros de 32 bits con los siguientes valores hexadecimales, según el criterio little endian —el byte menos significativo queda en la dirección de memoria más baja—:

      A = 67452301

      B = EFCDAB89

      C = 98BADCFE

      D = 10325476

   ii. Posteriormente comienza el lazo principal del algoritmo, que se repetirá para cada bloque de 512 bits del mensaje para finalizar con la sumatoria. En primer lugar copiaremos los valores de A, B, C y D en otras cuatro variables, a, b, c y d. Luego definiremos las siguientes cuatro funciones para obtener los valores de F, G, H, I bases para la generación de la función resumen:

      F(X, Y, Z) = (X ^ Y) v ((-X) ^ Z)

      G(X, Y, Z) = (X ^ Z) v ((Y ^ (-Z))

      H(X, Y, Z) = X o Y o Z

      I(X, Y, Z) = Y o (X v (-Z))

iii. Ahora se representa el mj-ésimo bloque de 32 bits del mensaje m (de 0 a 15), y se define otras cuatro funciones iniciales a las cuatro corridas:

FF(a, b, c, d, mj, s, ti) representa a = b + ((a + F(b, c, d) + mj + ti) / s)

GG(a, b, c, d, mj, s, ti) representa a = b + ((a + G(b, c, d) + mj + ti) / s)

HH(a, b, c, d, mj, s, ti) representa a = b + ((a + H(b, c, d) + mj + ti) / s)

II(a, b, c, d, mj, s, ti) representa a = b + ((a + I(b, c, d) + mj + ti) / s)

iv. Donde la función a/s representa desplazar circularmente la representación binaria del valor a s bits a la izquierda, con reentrada.

v. Las 64 operaciones que se realizan en total quedan agrupadas en cuatro rondas.

Primera Ronda: En esta ronda obtenemos la primera función hash del bloque de 512 bits de un total de 2048.

FF(a, b, c, d, m0, 7,D76AA478)

FF(d, a, b, c, m1, 12,E8C7B756)

FF(c, d, a, b, m2, 17, 242070DB)

FF(b, c, d, a, m3, 22,C1BDCEEE)

FF(a, b, c, d, m4, 7, F57C0FAF)

FF(d, a, b, c, m5, 12, 4787C62A)

FF(c, d, a, b, m6, 17,A8304613)

FF(b, c, d, a, m7, 22, FD469501)

FF(a, b, c, d, m8, 7, 698098D8)

FF(d, a, b, c, m9, 12, 8B44F7AF)

FF(c, d, a, b, m10, 17, FFFF5BB1)

FF(b, c, d, a, m11, 22, 895CD7BE)

FF(a, b, c, d, m12, 7, 6B901122)

FF(d, a, b, c, m13, 12, FD987193)

FF(c, d, a, b, m14, 17,A679438E)

FF(b, c, d, a, m15, 22, 49B40821)

Segunda Ronda: En esta ronda obtenemos la segunda función hash del bloque de 512 bits de un total de 2048.

GG(a, b, c, d, m1, 5, F61E2562)

GG(d, a, b, c, m6, 9,C040B340)

GG(c, d, a, b, m11, 14, 265E5A51)

GG(b, c, d, a, m0, 20,E9B6C7AA)

GG(a, b, c, d, m5, 5,D62F105D)

GG(d, a, b, c, m10, 9, 02441453)

GG(c, d, a, b, m15, 14,D8A1E681)

GG(b, c, d, a, m4, 20,E7D3FBC8)

GG(a, b, c, d, m9, 5, 21E1CDE6)

GG(d, a, b, c, m14, 9,C33707D6)

GG(c, d, a, b, m3, 14, F4D50D87)

GG(b, c, d, a, m8, 20, 455A14ED)

GG(a, b, c, d, m13, 5,A9E3E905)

GG(d, a, b, c, m2, 9, FCEFA3F8)

GG(c, d, a, b, m7, 14, 676F02D9)

GG(b, c, d, a, m12, 20, 8D2A4C8A)

Tercera Ronda: En esta ronda obtenemos la tercera función hash del bloque de 512 bits de un total de 2048.

HH(a, b, c, d, m5, 4, FFFA3942)

HH(d, a, b, c, m8, 11, 8771F681)

HH(c, d, a, b, m11, 16, 6D9D6122)

HH(b, c, d, a, m14, 23, FDE5380C)

HH(a, b, c, d, m1, 4,A4BEEA44)

HH(d, a, b, c, m4, 11, 4BDECFA9)

HH(c, d, a, b, m7, 16, F6BB4B60)

HH(b, c, d, a, m10, 23,BEBFBC70)

HH(a, b, c, d, m13, 4, 289B7EC6)

HH(d, a, b, c, m0, 11,EAA127FA)

HH(c, d, a, b, m3, 16,D4EF3085)

HH(b, c, d, a, m6, 23, 04881D05)

HH(a, b, c, d, m9, 4,D9D4D039)

HH(d, a, b, c, m12, 11,E6DB99E5)

HH(c, d, a, b, m15, 16, 1FA27CF8)

HH(b, c, d, a, m2, 23,C4AC5665)

Cuarta Ronda: En esta ronda obtenemos la cuarta función hash del bloque de 512 bits de un total de 2048.

II(a, b, c, d, m0, 6, F4292244)

II(d, a, b, c, m7, 10, 432AFF97)

II(c, d, a, b, m14, 15,AB9423A7)

II(b, c, d, a, m5, 21, FC93A039)

II(a, b, c, d, m12, 6, 655B59C3)

II(d, a, b, c, m3, 10, 8F0CCC92)

II(c, d, a, b, m10, 15, FFEFF47D)

II(b, c, d, a, m1, 21, 85845DD1)

II(a, b, c, d, m8, 6, 6FA87E4F)

II(d, a, b, c, m15, 10, FE2CE6E0)

II(c, d, a, b, m6, 15,A3014314)

II(b, c, d, a, m13, 21, 4E0811A1)

II(a, b, c, d, m4, 6, F7537E82)

II(d, a, b, c, m11, 10,BD3AF235)

II(c, d, a, b, m2, 15, 2AD7D2BB)

II(b, c, d, a, m9, 21,EB86D391)

vi. Finalmente, los valores resultantes de a, b, c y d fueron sumados con A, B, C y D, quedando listos para procesar el siguiente bloque de datos para obtener la función hash.

vii. El resultado final del algoritmo es la concatenación de A, B, C y D y adjuntos al documento del cual se obtuvo los 512 bits de entrada a continuación:

mQGiBDRkk6kRBADKYHrNnFeXlggr14IVGy6FudLG2Cd1wb3yKOaNnodyjZa0a5oiLs9jDf
DfEdq8K+W6QBLv06w7oVFPNMYsU+ufb0pa/bHWq6IrHxKkTVH4o4PUYTmHW0jfGjoXE
tAUZ0vp9wYR0Yqi7wXO3L/N5KuVNjLj7rXOT7rOmHsOjmY1cQCg//2wOcyAnkaDCODFN
if/VdowntcD/j5midszzU6M7BWmeDJoqEEGzSuxfmRSNyNZe6/65k8TFXIVpB0vnxwsZSh
0POSlNgz1cmX6VbEmmUXoYsMRfq7iXHSAZ3DLB333yR2bQUbkrH5WZF75G2vvTO7r
KS5KtmROJ8E+vX/py6PGz1f3tBZJ94KwM787g6j43F4XIYTAA/9L5GZzClHOGt01BtZkioH
5YoHnDGHKC8mMXcykXA5KdJvl+9jGz3InUHiG04StaMxMcDcWLzL5FVLz3LBzlOXGs7ji
kgH3BYBI3p7dIExfRADucDHyKL/CpIl5zqHBI+5bxY3Tysu3UlA1UkQloJMsSInlkkjQhwihN
Ysj8Avr9LYAAAAmTWFudWVsIEx1Y2VuYSBMb3BleiA8bWx1Y2VuYUB1amFlbi5lcz6IVg
QTEQIAFgUCOHyzZAQLCgQDAxUDAgMWAgECF4AACgkQSLJRYWmrV4TqngCgsDk/y
snBdpPwp/r2dL0Lzcq01J8AnRxUUiS3SoVb3WfnaSQmdb6eaJ3qiEsEEBECAAsFAjTa4F
oECwMBAgAKCRBIslFhaatXhO9yAJ9vI1QWihIKMUa4g3S8t3EZZ9SXxgCaAjfnHx8Kayyl
m6XXjjsC6iJKBmaIPwMFEDTa5h2buAet57tpPxEC8K4AoOTP5I1fJFN6KtZdmLtENKSRr
KfxAJ4gwl5R1MzpeTFiysWKab/PsU5GwohGBBARAgAGBQI3eQrfAAoJEPi4YmyN8qnzA
1sAniVQF6V/6gBVPq0Idt1Yrtuy4+aQAKDTuyVvfU1tRNy/U89FhzMmBVRL44htBBERAgA
tBQI+JnRPBYMB4TOAIBpodHRwOi8vd3d3LnRvZWhvbGQuY29tL3JvYm90Y2EvAAoJEB
BYFoXFIQl+g80An1lb7UmR7euGyIwluvc4n84w3opTAJwKLudIa08d6eOKeSmDMwMYsm
HCZrkCDQQ0ZJRfEAgAw/iGbTW9OaTyfV4RNZdg1HRDGEyasZdEPCM9ihPkfvQyK44n
H13OseaikIYoyoA/BFiWeTNcHvb/4KOuCK2GnO/p/6ohFcAOK5anEygGrhUUttUw8kYZ0r
UBFlJnurtDcxwawugbPFv3qA+sn756q7XUxjnTtpou+lWyj6VkN/EvrZDf9E7ikPUqRuIsHzJ
5PUwypWtXaKg2HfClKkZlYFqzdPDCssrXOfjZDx2q6GSek6Sgj5Ph3X4opoXIx6Cfmp4EL
YmvdmnDu4oe6A6l/XIQ8NNhj+GxdtOgTq8QKDRWl2f6M3pQgPnYzBHoDIqnr/ie8jK4seD
ezRPtL1/TlQACAgf+JXw03Q1opLBAaO/WZlcs2SiEzqv+gCkFW9vk2bJbSY4PQHwiLc0H
wcPEDi7jIu9QxJfZcHkax8XgXkCvfFJFFmqgqarIOzXp/BgiYyma6GVAmXcI6lI9ZSgzPvva
NFGe0/7R6Yroee7nJ/9RyxF89SI++5tZY+/bpLuKAbnX9SA3PEnUWiHD2ah3cC3VXNrus3

lsKA7MEh3q9xnoF/8Z7vwldrKUyLZdaDqSM7isyI5Fe0PWn/mtW4+7/rjboaY7PGJCAqtn8c
HDvByRYCZ8kLRlobQHzL8XN1fsdfBv6WDNeS9IqBCXcPME7R21wytsi2WMDnYL7rQW
U/CgLqFx2Ig/AwUYNGSUX0iyUWFpq1eEEQL3JACfTfvh6A70A9N2SbnRBmktuRBp9Ns
An2ZQbpg0eaeVRuzejA2QM7ldrz53mQENAzRkY3EAAAEIAOy6UGjPly4OJtrPookV6kxUj
mL83LY6jI+ZRH5/ZkHeLcQ+Qufmme+bOms5XHv+KTOkKV5RUdJwUXTQtHe+yX7Xcvn
LlxnxE/dmhgeNHcLH0XfQ9rBjIvREcKtRhUBP1t0d+QTnUro7Jrg8ZQSTupLTb5LO7683Ff
F/2eBSMsn1QZx6ODSir4t05EqMOzlHc53jV8y2bYDRDMhQ5r1C1ap0vZS6tp85Wb64+au
n0et1yee4voeUwNubnr1FBXzfBwQUy4e4IdkJbXYb1f8Iy7+t5B3WviU1BgGQOP29fObjg7
eMtXUgaF6eYK88Byu7tHMuFYQROeq37dWwHELi6LEABRO2AAAAJE1hbnVlbCBMdW
NlbmEgUlNBIDxtbHVjZW5hQHVqYWVuLmVzPokBFQMFEDY7Tx/t1bAcQuLosQEBsCEI
AOvHEw9fuHTqWpRMxtvqYZnfoslqg27vNC4fE4QGc/KhyxwCeqm/fUh51geVMna7QwLu
bbHcmd4IPAZT614LdAhwzDzv99o+iHDwL3fv+LJWqdmkxCZYHJs7vKMSShaVCd9JXPe
5FT6iXIuklY3oCU5TkjumRZNzr40MgQZzYW5rxCfYX+feoLaX8SBR7EU2mdX1LaMy+RJ3
cG7a76btqdKnLx+E5USlIDWC26sk7Y+Dutp987F3ZHW9TVO5IUHn5TqirxnL7a6ZGn2c2o
q4V27loCuFxo6/KJ1m92tddM35SHzoijA6hWWH9OsaMiA6d4Qu1LbK28NElnAo+FZUitOJ

ARUDBRA3eQqZGIrd0JPxO/EBAcE1B/0WG4aU63s6E5lLvlUSsZ0yTtUBPETH0K2yl5sca
cX5+uF/7+hHGAoN0/yTbpB0ODoxVNxgctkRDf82QHtDr4HkGdvdux/GrwuuFigKQoeBEpP
Z1yAcLX/zcWKPjveysNhywngFHmzdnvCXJeegWsila1BEoWT4OeMpelY7U9zH7RLY/u66
yKM5TIitFYd5uOWO+SSWnkvD8KvbAv2UYYXbK9aXieIKnrt/F8SB8nCQzxAUy2A1JBJo
Qt07B4AyevHhjOZ1zAsUdwVk0zcfx1AsI0N9hWE9NUh/3WLyKSe4IF35wYZEdcy7+i0Sw
BinZ4dls8wwvcISF3JwqJmDhL+c=2wgK

viii. Obteniéndose la función hash del documento encriptado para adjuntarlo y enviarlo por un medio de comunicación inseguro.

b) Posteriormente se codifica empleando la clave privada SHA-1 correspondiente para su posterior envió, utilizando cinco registros de 32 bits (un total de 128 bits más uno de prueba).

i. Emplea cinco registros de 32 bits en lugar de cuatro, que deben ser inicializados antes de procesar el primer bloque con los siguientes valores:

A = 67452301

B = EFCDAB89

C = 98BADCFE

D = 10325476

E = C3D2E1F0

ii. Una vez que los cinco valores están inicializados, se copian en cinco variables, a, b, c, d y e. El lazo principal tiene cuatro rondas con 20 operaciones cada una que servirán para generar el valor de wt:

F(X, Y, Z) = (X ^ Y) v ((-X) ^ Z)

G(X, Y, Z) = X o Y o Z

H(X, Y, Z) = (X ^ Y) v (X ^ Z) v (Y ^ Z)

iii. La operación F se emplea en la primera ronda (t comprendido entre 0 y 19), la G en la segunda (t entre 20 y 39) y en la cuarta (t entre 60 y 79), y la H en la tercera (t entre 40 y 59). Además se emplean cuatro constantes obtenidos de la clave privada, una para cada ronda:

K0 = 5A827999

K1 = 6ED9EBA1

K2 = 8F1BBCDC

K3 = CA62C1D6

iv. El bloque de mensaje m se trocea en 16 partes de 32 bits m0 a m15 y se convierte en 80 trozos de 32 bits w0 a w79 usando el siguiente algoritmo para su encriptación:

wt = mt para t = 0 . . . 15

wt = (wt−3 _ wt−8 _ wt−14 _ wt−16) / 1 para t = 16 . . . 79

v. Todos los wt obtenidos se interpretan como enteros en las operaciones del algoritmo empleando la ordenación big endian.

vi. El lazo principal del algoritmo es entonces el siguiente:

FOR t = 0 TO 79

i = t div 20

Tmp = (a / 5) + A (b, c, d) + e + wt + Ki

e = d

d = c

c = b / 30

b = a

a = Tmp

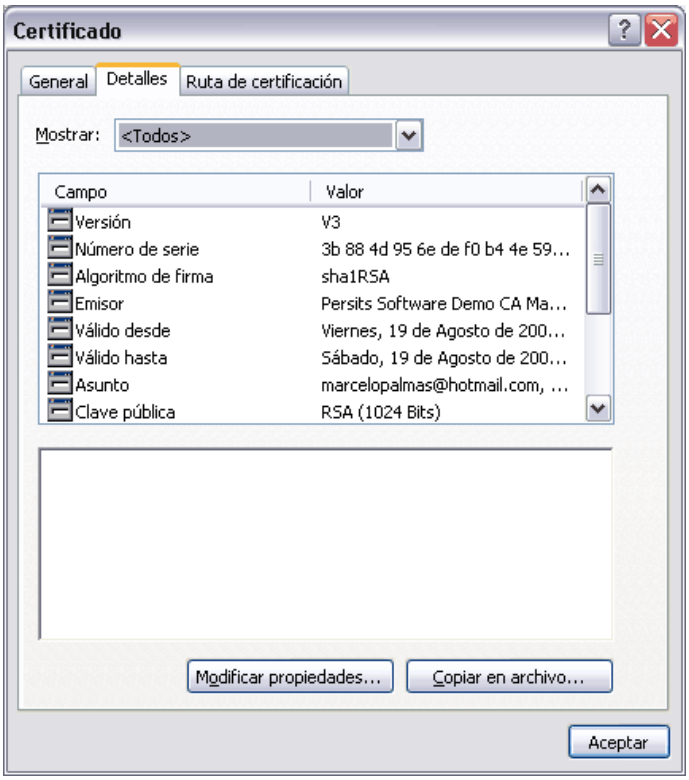
End for

vii. Siendo A la función F, G o H según el valor de t (F para t 2 [0, 19], G para t 2 [20, 39] y [60, 79], H para t 2 [40, 59]). Después los valores de *a* → *e* son sumados a los registros A → E y el algoritmo continúa con el siguiente bloque de datos. Finalmente, el valor de la función resumen será la concatenación de los contenidos de los registros A → E resultantes de procesar el último bloque del mensaje, almacenando la información encriptada.

viii. Finalmente será enviado al destinatario y realizará la función inversa a lo detallado para obtener la autentificación del mensaje.

c) Autentificación de la firma digital por certificado digital

Figura 6. 1: Certificado Digital



Fuente: Elaboración Propia

a. Cada certificado digital tiene un campo denominando clave_publica y clave_privada que como su nombre indica, almacena la clave pública o privada.

b. El sistema solicita la clave pública o privada del usuario, al momento de ingresar determina que cumpla con el tamaño de 128 bits, consecuentemente revisa el registro del certificado digital, cuando encuentre armara el certificado digital con los datos del usuario, caso contrario mostrara un mensaje de inexistencia de usuario como se observa en la figura 6.1.

El proceso de firmado, encriptación y autentificación de la firma por certificado digital cumples con las condiciones de cobertura de sentencia con lo cual se **concluye** la condición.

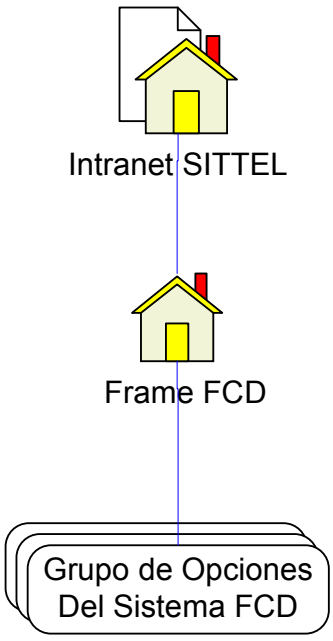
6.1.1.2. Cobertura de decisión:

La cobertura de decisión proporcionó la garantía que en cada nodo de decisión se toma al menos una vez cada salida. Utilizada para los siguientes procesos:

a) Ingreso y selección de opciones

i. Se determino que el sistema funcione como un frame de la página principal de SITTEL (ver figura 6.2).

Figura 6. 2: Mapa resumido del Sitio



Fuente: Elaboración Propia

ii. Se realizó la prueba de ingreso y salida a cada una de las pantallas a través de Hipervínculos para verificar si existe conectividad entre estos.

iii. Para su **mejor interactividad** se desarrollo menús desplegadles en Java Script, un menú principal a lado izquierdo, mapa del software y un manual en línea.

b) Gestión de usuarios

i. El administrador tiene la posibilidad de eliminar, deshabilitar y habilitar las diferentes cuentas de usuarios, pero no cuenta con la posibilidad de modificar la información de un usuario por seguridad del sistema.

ii. La restricción se realiza a través de la eliminación de la opción, siendo que la única forma es ingresar a la Base de Datos, esta se encontrará protegida a través de una contraseña de ingreso que solo el desarrollador del software la tendrá para brindar mayor seguridad al sistema.

iii. Además se realizará una copia de seguridad mensualmente para que en caso de fallo o perdida de información se restablezca el sistema rápidamente.

c) Eliminación del servicio de firma y certificado digital

i. El usuario podrá ingresar a la opción de eliminación del servicio de firma y certificado digital, solo necesitará su usuario y contraseña, consecuentemente se enviara un e-mail a su correo para la confirmación.

Con lo cual el ingreso y selección de opciones, la gestión de usuarios y la eliminación de servicios de firma y certificado digital cumplen con las condiciones de cobertura de decisión, **concluyendo** su verificación.

6.1.1.3. Cobertura de condición:

La cobertura de condiciones garantizó que en cada decisión de condición tomará los valores posibles. Utilizada para los siguientes procesos:

a) Inscripción y obtención de claves asimétricas

i. Se verificó el ingreso de datos en el formulario de inscripción, los cuales deberían cumplir con diferentes los requisitos dependiendo del tipo de campo al que pertenecen (carácter, numérico, alfanumérico, date y contraseña), en la tabla 6.1 se resumen las características que deberán cumplir los usuarios al momento de ingresar sus datos al sistemas.

Tabla 6. 1: Condición de Ingreso de Datos

Tipo de Campo	Condiciones
Numérico	i. Evitar el ingreso de caracteres alfabéticos. ii. Limitar la cantidad de caracteres numéricos. iii. Encriptar la información al momento de enviar la información.
Carácter	i. Evitar el ingreso de caracteres numéricos. ii. Limitar la cantidad de caracteres alfabéticos. iii. Encriptar la información al momento de enviar la información.
Alfanumérico	i. Limitar la cantidad de caracteres numéricos. ii. Encriptar la información al momento de enviar la información.
Date	i. Evitar el ingreso de caracteres alfabéticos y numéricos que no correspondan al formato del campo ii. Limitar la cantidad de caracteres innecesarios. iii. Encriptar la información al momento de enviar la información.
Contraseña	i. Evitar el ingreso de caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.[38] ii. Restringir el tamaño de la contraseña entre seis y doce caracteres. iii. Encriptar la información al momento de enviar la información.

Fuente: NB ISO/IEC 177999

ii. Además se verificó la generación de las llaves asimétricas revisando los archivos pubring.pkr para las públicas, secring.skr para las privadas, y la base de datos al momento de generar las llaves para la firma digital.

[38] NB ISO/IEC 17799 SGSI

iii. Se revisó la generación de las huellas para las llaves públicas y privadas en la Base de Datos del software y del anillo en el criptosistema PGP obteniendo la siguiente tabla 6.2:

Tabla 6. 2: Generación de Huellas Digitales por Inscripción

HUELLA DE LA CLAVE PÚBLICA	**HUELLA DE LA CLAVE PRIVADA**
PUBRING.PKR	**SECRING.SKR**
9E2B 9D14 CBCE FE12 16A8 8E9A 0S18 TSJT PO35 15D8 6S2S 5A89 ASFS SD98 56R9	C103 48B2 5161 69AB 5784 D506 45S2 6482 68SD 8598 F605 45S6 6525 98RH 1486
BASE DE DATOS DEL PROGRAMA	
Campo clave_publica	**Campo clave_privada**
9E2B 9D14 CBCE FE12 16A8 8E9A 0S18 TSJT PO35 15D8 6S2S 5A89 ASFS SD98 56R9	C103 48B2 5161 69AB 5784 D506 45S2 6482 68SD 8598 F605 45S6 6525 98RH 1486

Fuente: Elaboración Propia

b) Recuperación y modificación de datos del usuario

i. La recuperación de la firma digital genera nuevas claves para preservar la seguridad de la información del usuario en caso de pérdida o sustracción de claves, y modificación de contraseña, creando una caducidad a la contraseña de 72 días automáticamente y generando nuevas claves.

ii. Se realizó modificaciones a las contraseñas de las firmas digitales obteniéndose las siguientes huellas para sus claves asimétricas en la tabla 6.3.

Tabla 6. 3: Generación de Huellas Digitales por Modificación

ANTIGUAS HUELLAS DE LAS CLAVES	**NUEVAS HUELLAS DE LAS CLAVES**
Campo clave_publica	**Campo clave_publica**
9E2B 9D14 CBCE FE12 16A8	6S9S 9S15 DFDF RT62 19H9

8E9A 0S18 TSJT PO35 15D8 6S2S 5A89 ASFS SD98 56R9	8S6S 6E25 SGWY RA68 89D7 7W6A 9S94 GDSF SD85 56R5
Campo clave_privada	**Campo clave_privada**
C103 48B2 5161 69AB 5784 D506 45S2 6482 68SD 8598 F605 45S6 6525 98RH 1486	W445 45D9 5645 68GA 1579 A506 74S6 4778 98GR 8451 S584 45A9 41592 85SR 1568

Fuente: Elaboración Propia

c) Gestión de claves públicas y anillos.

i. La administración de la seguridad sobre los archivos de claves públicas y los anillos determinó que se oculte y evite el ingreso a los archivos para impedir su sustracción, modificación y mantener la integridad de la información, en especial de las claves asimétricas.

ii. Se determino que para asegurar la integridad, y evitar la modificación y sustracción de la información realizar una revisión al centro de servidores de SITTEL, para lo cual se determino que:

- El centro de Servidores cumple con los requisitos necesarios para brindar seguridad al programa de firmas y certificados digitales, por que evita el ingreso a terceros por seguro en la puerta y permite su supervisión por ser visible a los supervisores (cuarto de vidrio), además tiene extinguidotes, piso falso y la ventilación necesario.[39]
- La red interna de SITTEL tiene un firewall o cortafuego que revisa el ingreso y salida de la información, evitan ataques externos.

Con lo cual se **concluye** que el ingreso y selección de opciones, la gestión de usuarios y la eliminación de servicios de firma y certificado digital cumplen con las condiciones de cobertura de condición, al elegir la opción correspondiente y pudiendo tomas los valores correspondientes.

[39] NB ISO/IEC 17799 SGSI

6.1.2. Mantenimiento de Firmas y Certificados Digitales

Las métricas y factores de calidad expuestos en la sección 6.2 del presente capítulo fueron usadas para el desarrollo y mantenimiento del software de firmas y certificados digitales, sin embargo se utilizó el estándar IEEE[40] 982.1-1988, el cual sugiere un índice de madurez del software (IMS) que proporciona una indicación de la escalabilidad de un producto software (basados en los cambios que ocurren con cada versión del producto), para lo cual se determino la siguiente información:

Mt = 2 módulos de la versión actual (Firmas y Certificados Digitales)

Fc = 0 módulos de la versión actual que se han desarrollado o modificado

Fa = 0 módulos de la versión actual que se añadieron (Firmas y Certificados Digitales)

Fd = 0 módulos de la versión anterior que se han borrado en la versión actual.

Mediante la siguiente ecuación se determina el índice de madurez del software (Ecuación 6.1)

IMS = [Mt – (Fa + Fc + Fd)] / Mt (Ecuación 6.1)

IMS = [2 – (0 + 0 + 0)] / 2

IMS = 1.0

Mientras más se acerque a 1.0 el producto tiende a estabilizarse, con la consecuencia de realizar por lo menos dos veces al año el mantenimiento al sistema de Firmas y Certificados Digitales.

Con lo cual se concluye la **verificación** de la subsección de Mantenimiento de software para las firmas y certificados digitales, determinando un nivel de IMS 1.0 con mantenimiento de dos veces al año.

6.1.3. Conclusiones

Se llega a la **conclusión** que habiéndose realizado las Pruebas y la planificación del Mantenimiento del software, se completa el desarrollo del Modelo Lineal Secuencial para las Firmas Digitales y Certificados Digitales, logrando obtener las condiciones de sentencia, decisión y condición para las pruebas y el Índice de Madurez de Software para el Mantenimiento de Firmas y Certificados Digitales.

[40] Instituto de Ingeniero Eléctricos y Electrónicos

Habiéndose concluido las pruebas y mantenimiento del software, se prosigue con los Factores de Calidad de McCall e ISO 9126 para obtener un producto que refleje las necesidades de SITTEL.

6.2. Factores de Calidad de McCall e ISO 9126

Dado el concepto de Calidad de Software en la Segunda Sección del Capitulo de Marco Teórico y Metodológico, habiéndose desarrollado el Modelo Lineal Secuencial para las Firmas y Certificados Digitales, se desarrolla a continuación los factores de calidad de McCall e ISO 9126.

6.2.1. Factores de Calidad de McCall

Los factores que afectan a la calidad de software se concentran en tres aspectos importantes de un producto software: sus características operativas su capacidad de cambios y su adaptabilidad a nuevos entornos (ver figura 6.3).

Figura 6. 3: Factores de Calidad de McCall

Fuente: Pressman ©2003

El esquema de puntuación propuesto por McCall es una escala del 0.00% (bajo) al 100.00% (alto) obtenido a través de las métricas del esquema de puntación, 1 si se

cumple y 0 si no, al final se promediará todas las métricas desarrolladas a continuación y se multiplicará por 100.

- *Facilidad de auditoria y Seguridad*. La facilidad con la que se puede comprobar el cumplimiento de los estándares, para lo cual se determino los siguientes procedimientos para auditar Integridad, Autenticidad y confidencialidad:
  - Integridad: La información es protegida en la Base de Datos por contraseña y una copia de seguridad mensual.
  - Autenticidad: El sistema esta orientado a la autenticidad de usuarios por certificados digitales.
  - Confidencialidad: Los usuarios y el administrador no tienen la posibilidad de obtener las contraseñas de usuarios y su clave privada.
  - Para mayor auditabilidad se puede realizar pruebas CAT entre la base de datos, las claves públicas y los certificados digitales, la regla que deberá verificar la prueba CAT es la existencia de una clave pública, certificado digital y el registro en la Base de Datos por usuario.
  - El nivel de cumplimiento de la métrica llego al 100%, por que cumple con la facilidad de auditoria y seguridad mediante lo mencionado anteriormente.
- *Exactitud*. La exactitud de los cálculos y del control fueron desarrollados en la etapa de prueba del modelo lineal secuencial, pero controlados por Framework de Microsoft, en la subsección 6.1.1.
  - El nivel de cumplimiento de la métrica llego al 75%, por que se utilizó librerías de Framework de Microsoft para la generación del criptosistema PGP y el firmado RSA.
- *Complexión*. El sistema funciona sobre tecnología Web y necesita de Navegadores como Internet Explore, Opera, Netscape, etc., para su normal funcionamiento.

- El nivel de cumplimiento de la métrica llego al 75%, por que funciona sobre un navegador y es dependiente del mismo.

- *Concisión.* La utilización de tecnología cliente-servidor en la red interna de SITTEL garantiza una gran velocidad en la transferencia y procesamiento de información.
  - El nivel de cumplimiento de la métrica llego al 100%, por que se comprobó que el nivel de respuesta del sistema en una red interna es altamente veloz.

- *Consistencia.* Se utilizó tecnología y técnicas uniformes y complementarias a lo largo del proyecto (Seguridad, NB ISO/IEC 17799, Tecnología Cliente-Servidor y Asp).
  - El nivel de cumplimiento de la métrica llego al 100%, por que se utilizó el Modelo Lineal Secuencial y el modelo de las 4P's para el desarrollo del software, la Norma Boliviana ISO/IEC 17799 y el Modelo P.H.V.A. para la auditoria de sistemas en SITTEL, y el Modelo de Calidad de Software ISO 9126, y el McCall para garantizar la calidad del mismo.

- *Estandarización de datos.* Se utilizó la norma **IUT X.509 S**[41] para la generación de Certificados Digitales, en cambio para el desarrollo de las firmas digitales se utilizó el criptosistema PGP, además se realizo la normalización de los datos a través del Modelo Entidad-Relación.
  - El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.

- *Tolerancia al Error.* El software no puede dañar a ninguna máquina por que el programa se ejecuta en el servidor y funciona sobre la interfase de la máquina del cliente, además no es necesario instalarlo.
  - El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.

- *Eficiencia de ejecución.* El rendimiento del programa frente a la velocidad de transferencia de información es alto, por que el software solo transfiere

[41] Ver la subsección 3.1.12.3 del Marco Teórico y Metodológico

código html y el programa fuente se ejecuta en el servidor, además la transferencia de información llega a 100Mbps[42] en la red interna de SITTEL.

- El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.

- *Capacidad de expansión.* El software tiene la capacidad de generar nuevos módulos y acoplarlos por la tecnología asp.Net que es utilizada actualmente en SITTEL.[43]
  - El nivel de cumplimiento de la métrica llego al 75%, por que al funcionar sobre la plataforma Microsoft .Net restringe el uso de métodos convencionales y utilizados por PHP, Java, JavaScript, entre otros para el desarrollo de software.
- *Generalidad.* El programa tiene el objetivo de administrar firmas y certificados digitales bajo tecnología asp y criptosistema PGP, además no funciona como una PKI, por tanto no cumple con la métrica de Generalidades.
  - El nivel de cumplimiento de la métrica llego al 25%, por que no funciona como una PKI, es parte de una PKI.
- *Independencia del Hardware.* La independencia del hardware fue verificable, porque funciona bajo plataformas de máquinas genéricas, IBM y DELL, demostrando su independencia del hardware.
  - El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.
- *Instrumentación.* La plataforma asp.Net de Microsoft vigila que el programa funciona correctamente, caso contrario no funcionara y generara una página de error.
  - El nivel de cumplimiento de la métrica llego al 75%, por que la Tecnología Microsoft, las plataformas Web, el funcionamiento correcto del servidor, son recursos que pueden fallar por diferentes razones, como virus, inundaciones, caída de la red, etc.

[42] Información entregada por el Analista de Sistemas de SITTEL.
[43] Microsoft Corp.

- *Modularidad.* El programa tiene un funcionamiento modular, por que esta construido en páginas (módulos) independientes a la opción manipulada.
    - El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.
- *Auto documentación.* El código fuente del programa cumple el estándar de una línea de comentario por línea de código fuente.
    - El nivel de cumplimiento de la métrica llego al 75%, por que los comentarios y la documentación del software podrá se mejorable.
- *Simplicidad.* El programa no cumple el grado de simplicidad, por que su programación tiene manejo de objetos ADO.Net y librerías para administrar las firmas y certificados digitales, el tipo de programación corresponde a un nivel medio a superior.
    - El nivel de cumplimiento de la métrica llego al 25%, por lo mencionado anteriormente.
- *Independencia del sistema software.* El software para firmas y certificados digitales es dependiente del lenguaje de programación (asp.Net) y del servidor (IIS) con Framework en el que corre, por tanto no cumple con los requisitos de la métrica.
    - El nivel de cumplimiento de la métrica llego al 50%, por lo mencionado anteriormente.
- *Trazabilidad.* Se realizó el análisis y diseño del software cumpliendo con los requisitos de SITTEL y desarrollando un software que se acople a su entorno de trabajo de SITTEL.
    - El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.
- *Formación.* El software esta desarrollado interactivamente con el objetivo de facilitar su uso frente al usuario.
    - El nivel de cumplimiento de la métrica llego al 100%, por lo mencionado anteriormente.

Para finalizar se realizó en análisis de regresión lineal con las métricas de calidad de McCall (ver tabla 6.4) obtenidas a través del nivel de cumplimiento de la métrica heurísticamente, con el 100% al cumplimiento total de la métrica, 75% al necesario cumplimiento, 50% cuando se encuentra en implantación, al 25% cuando no se tiene planeado pero no se implanto y el 0% no se pensó en su implantación:

Tabla 6. 4: Métricas de Calidad de McCall

Métricas de Calidad	Cumplimiento	Valor	Cumplimiento de la Métrica según McCall
Facilidad de auditoria y Seguridad	Si	1.00	100%
Exactitud	Si	1.00	75%
Estandarización de comunicaciones	Si	1.00	75%
Complexión	Si	1.00	100%
Concisión	Si	1.00	100%
Consistencia	Si	1.00	100%
Estandarización	Si	1.00	100%
Tolerancia al error	Si	1.00	100%
Eficiencia de expansión	Si	1.00	100%
Generalidad	No	0.00	25%
Independencia del hardware	Si	1.00	100%
Instrumentación	Si	1.00	75%
Modularidad	Si	1.00	100%
Auto documentación	Si	1.00	75%
Simplicidad	Si	0.00	25%
Independencia del Sistema Software	No	0.00	50%
Trazabilidad	No	1.00	100%
Formación	Si	1.00	100%

Fuente: Elaboración Propia

A continuación se obtiene la tabal de regresión lineal para el modelo de métricas de McCall:

Tabla 6. 5: Métricas de Calidad de McCall

Métricas de Calidad	**Cumplimiento de la Métrica según McCall X**	**Valor Y**	**X*Y**	**X^2**
Facilidad de auditoria y Seguridad	1.00	1.00	1.00	1.00
Exactitud	0.75	1.00	0.75	0.5625
Estandarización de comunicaciones	0.75	1.00	0.75	0.5625
Complexión	1.00	1.00	1.00	1.00
Concisión	1.00	1.00	1.00	1.00

Consistencia	1.00	1.00	1.00	1.00
Estandarización	1.00	1.00	1.00	1.00
Tolerancia al error	1.00	1.00	1.00	1.00
Eficiencia de expansión	1.00	1.00	1.00	1.00
Generalidad	0.25	0.00	0.00	0.0625
Independencia del hardware	1.00	1.00	1.00	1.00
Instrumentación	0.75	1.00	0.75	0.5625
Modularidad	1.00	1.00	1.00	1.00
Auto documentación	0.75	1.00	0.75	0.5625
Simplicidad	0.25	0.00	0.00	0.0625
Independencia del Sistema Software	0.50	0.00	0.00	0.25
Trazabilidad	1.00	1.00	1.00	1.00
Formación	1.00	1.00	1.00	1.00
Sumatoria ($\sum$)	**15.00**	**15.00**	**14.00**	**13.625**
Promedio	**0.8333**	**0.8333**		

Fuente: Elaboración Propia

Posteriormente se estima los coeficientes por medio de mínimos cuadrados para obtener los datos necesarios para la obtención de la regresión lineal.

$$b_1 = \frac{\sum XY - \overline{Y}\sum X}{\sum X^2 - \overline{X}\sum X} \qquad \text{Ecuación 6.1}$$

$$b_0 = \overline{Y} - b_1\overline{X} \qquad \text{Ecuación 6.2}$$

Aplicando las fórmulas a los resultados tenemos:

$$b_1 = \frac{14.00 - 0.8333 * 15.00}{13.625 - 0.8333 * 15.00} = 1.333 \qquad \text{Ecuación 6.1}$$

$$b_0 = 0.8333 - 1.333 * 0.8333 = -0.277 \qquad \text{Ecuación 6.2}$$

Expresado en la fórmala de regresión lineal se tiene:

$$f(y) = -0.277 + 1.333X$$

Podemos concluir que cada mejora adicional del 100%, mejora la calidad del sistema en un 1.056 sobre 18 métricas (17.54% de mejora) en el caso del desarrollo del software de Firmas y Certificados Digitales, además se determina que el sistema cumple el 90% de las métricas (15 métricas de 100% divido entre 17.54 métrica necesarias para su óptimo funcionamiento).

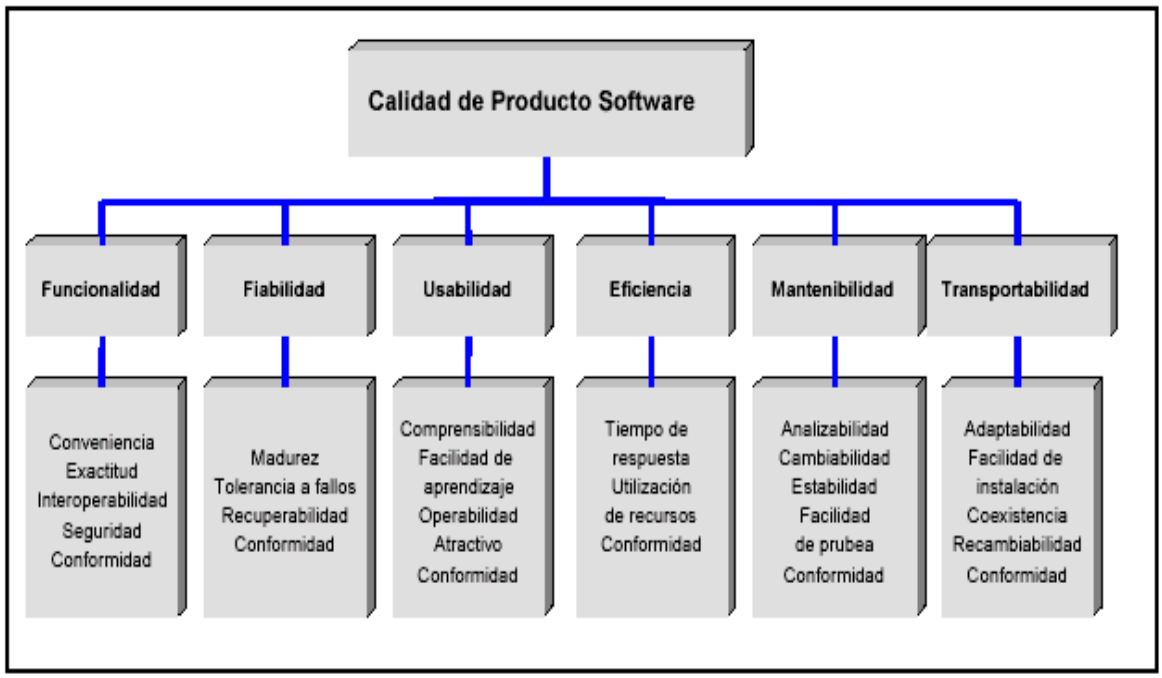
Desarrollado el análisis de regresión lineal, se **verifica** la subsección de Factores de Calidad de McCall para el software de firmas y certificados digitales concluyéndose que cumplen con los requisitos de calidad de la Norma.

6.2.2. Factores de Calidad del ISO 9126

El estándar ISO 9126 define un modelo de calidad del software como la totalidad de características relacionadas con su habilidad para satisfacer necesidades establecidas o implicadas en:

- Los atributos de calidad según la clasificación en seis características, las cuales a su vez se subdividen en subcaracterísticas (ver figura 6.4).
- Se describen métricas de calidad del software basadas en atributos internos y en el comportamiento externo del sistema.
- El estándar se establece que cualquier componente de la calidad del software puede ser descrito en términos de algunos aspectos de una o más de estas seis características

Figura 6. 4: Componentes del ISO 9126



Se desarrollo a continuación la comprobación de los componentes del ISO 9126 descritos en la figura 6.4, analizados a través del Modelo descrito en el Anexo E de Acreditación de Sistemas - Calidad.

- *Funcionalidad.* El software de firmas y certificados digitales brinda:
  - Conveniencia frente a la utilización de otro software por costo[44] y plataforma tecnológica[45].
  - Exactitud para generar firmas y certificados digitales, utilizarlos y eliminar el uso de los mismos,
  - Interoperatividad porque trabaja por módulos y entre ellos administran el sistema de firma y certificado digital.
  - Seguridad por que el sistema esta creado bajo el estándar de seguridad NB ISO/IEC 17799 para Sistemas de Gestión de Seguridad de la Información en el capítulo diez de Desarrollo y Mantenimiento de Sistemas.
  - Conformidad por que cumple los requisitos obtenidos en el análisis de sistemas de información realizado en SITTEL.
- *Confiabilidad.* El software esta disponible en línea por que cumple con:
  - Madurez por que fue desarrollado por el Modelo Lineal Secuencial para generar un desarrollo cíclico de mejoras consecutivas.
  - Tolerancia a Fallos por que utiliza tecnología Web sobre el servidor IIS que garantiza que en caso de fallos aparecerá una pantalla de Error.
  - Recuperabilidad por que al no necesitar instalación alguna, necesitara configuración sobre el servidor donde funcionará y por tanto su recuperación es rápida.
  - Conformidad por que cumple los requisitos obtenidos en el análisis de sistemas de información realizado en SITTEL.
- *Usabilidad.* El software de firmas y certificados digitales tiene un buen grado de facilidad de uso por que cumple con:

[44] Ver capítulo de Factibilidad del Proyecto, en la sección de Factibilidad Económica.
[45] Ver Anexo M. Tecnología Cliente-Servidor con Asp.

- Comprensibilidad por que utiliza una interfaz amigable al usuario que cumple con las tres reglas de oro para el diseño gráfico de pantallas: dar control al usuario, reducir la carga de memoria del usuario y construir una interfaz consecuente.
- Facilidad de Aprendizaje por que tiene una interfaz amigable.
- Operatibilidad por que puede utilizar el programa de firmas y certificados digitales sin la necesidad de abrir otros programas que no sea un browser.
- Atractivo por que llama la atención a la gente de SITTEL.
- Conformidad por que cumple los requisitos obtenidos en el análisis de sistemas de información realizado en SITTEL.

- *Eficiencia.* El software de firmas y certificados digitales es eficiente por que optimiza el uso de recursos del servidor de SITTEL mediante:
  - Tiempo de Respuesta. El tiempo de respuesta en servidores Web es alto, teniendo un tiempo menor a 2 segundos entre el envió, recepción y proceso, y envió de la información.
  - Utilización de Recursos. Por que el sistema funciona de manera adecuada en el Servidor de SITTEL, el cual tiene recursos óptimos para el software de firmas y certificados digitales.
  - Conformidad por que cumple los requisitos obtenidos en el análisis de sistemas de información realizado en SITTEL.
- *Mantenibilidad.* El software de firmas y certificados digitales tiene la posibilidad de realizarse modificaciones por que cumple con:
  - Analizabilidad del código fuente con comentarios y manuales del desarrollador.
  - Cambiabilidad de uno o más módulos en el mismo instante sin afectar a otros módulos del software por uso de la tecnología Web y desarrollo en módulos.
  - Estabilidad dentro de la tecnología .Net de Microsoft para llegar a ser asp.net.

- Facilidad de Pruebas CAT para verificar su correcto funcionamiento entre el registro de la Base de Datos, el Certificado Digital y la clave pública de un usuario.
- Conformidad por que cumple los requisitos obtenidos en el análisis de sistemas de información realizado en SITTEL.

- *Portabilidad.* El software y su tecnología tiene la posibilidad de ser portable e independiente frente al hardware (arquitectura de equipos) y software (sistema operativo, aplicaciones) sin afectar las mismas por que cumple con:
  - Adaptabilidad frente a diferentes tecnologías de software (Sistemas Operativos Linux, Unix y Microsoft) y Hardware para terminales (Computadoras genéricas, IBM, DELL).
  - Facilidad de instalación, por que el software no se instala, solo se configura en el servidor el cual funcionara.
  - Coexistencia con otras aplicaciones Web y no Web.
  - Recambiabilidad y actualización de módulos sin afectar su funcionamiento en línea.
  - Conformidad por que cumple los requisitos obtenidos en el análisis de sistemas de información realizado en SITTEL.

Con lo cual se **verifica** la subsección de Factores de Calidad del ISO 9126 para el software de firmas y certificados digitales a través de las comprobaciones de calidad de las métricas de calidad de la Norma Internacional.

6.2.3. Conclusiones

Se llega a la **conclusión** que habiéndose realizado el control de calidad y la revisión de las métricas para el Modelo McCall y la Norma Internacional ISO 9126 para la calidad de Software se **verificó** la calidad del software para las Firmas Digitales y Certificados Digitales, obteniéndose un software de mejor rendimiento y de acuerdo a las necesidades de la Superintendencia de Telecomunicaciones.

6.3. Comprobación de la Hipótesis del Proyecto de Grado

Las hipótesis desarrollada para el proyecto de "DESARROLLO DE UNA APLICACIÓN PARA ADMINISTRACIÓN DE FIRMAS Y CERTIFICADOS DIGITALES" en el subsección 1.5 se someten a

comprobación a continuación para determinar si son apoyadas o refutadas de acuerdo a lo que el investigador observa.

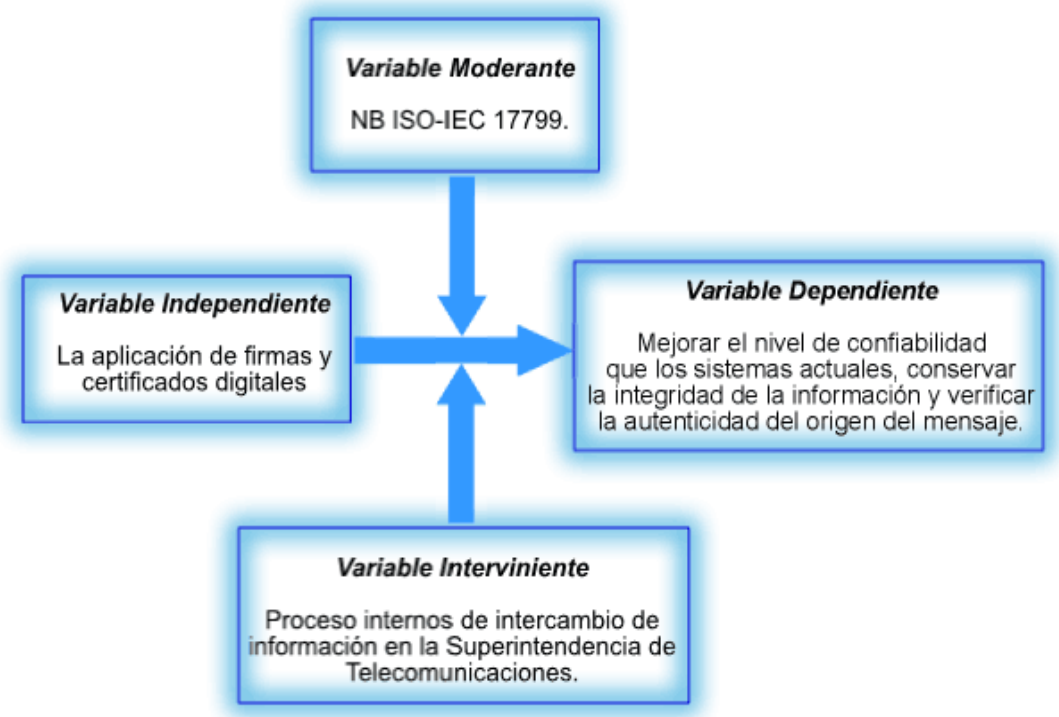
6.3.1. Hipótesis planteada

La hipótesis planteada en el capítulo 1 sección 1.5 es la siguiente:

La aplicación de firmas y certificados digitales acorde a la **NB ISO/IEC 17799** para los **procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones** permite tener un **mayor nivel de confiabilidad que los sistemas actuales** y **conserva la integridad de la información** como también **verifica la autenticidad del origen del mensaje**.

Se identificó las variables y sus relaciones identificadas a continuación en la figura 6.5.

Figura 6. 5: Relación entre las variables de la hipótesis



Fuente: Elaboración Propia

Para el desarrollo del método de validación se clasifica la hipótesis en:

- **Hipótesis Nula (Ho)**

  La aplicación de firmas y certificados digitales acorde a la NB ISO/IEC 17799 para los procesos internos de intercambio de información en la Superintendencia de

Telecomunicaciones **no** permite tener un mayor nivel de confiabilidad que los sistemas actuales y **no** conserva la integridad de la información como también **no** verifica la autenticidad del origen del mensaje.

- **Hipótesis Estadística (H1)**

  La aplicación de firmas y certificados digitales acorde a la NB ISO/IEC 17799 para los procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones permite tener un mayor nivel de confiabilidad que los sistemas actuales y conserva la integridad de la información como también verifica la autenticidad del origen del mensaje.

- **Hipótesis Alterna (H2)**

  La aplicación de firmas y certificados digitales acorde a la NB ISO/IEC 17799 para los procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones permite tener un nivel **similar** de confiabilidad que los sistemas actuales y **no** conserva la integridad de la información como también **no** verifica la autenticidad del origen del mensaje.

Formalmente las **hipótesis** se representan con la siguiente simbología:

$$H_O = \overline{X}_A < \overline{X_B}$$
$$H_1 = \overline{X}_A > \overline{X_B}$$
$$H_2 = \overline{X}_A = \overline{X_B}$$

Donde:

- $\overline{X}_A$ es el nivel de confiabilidad de los sistemas de comunicación después de implantar el sistema de Firmas y Certificados Digitales con un incremento en la conservación de la integridad de la información como también la verificación del autenticidad del origen del mensaje.
- $\overline{X}_B$ es el nivel de confiabilidad de los sistemas de comunicación medidos antes de implantar el Sistema de Firmas y Certificados Digitales sin la conservación de la integridad de la información como también la verificación del autenticidad del origen del mensaje.

Para la comprobación de la hipótesis en primer lugar se tomaron muestras de recursos antes y después de la implantación del sistema de seguridad que se detalla a continuación:

6.3.2. Nivel de Seguridad antes de la Implantación del Software

SITTEL no cuenta con ninguna herramienta de seguridad de información, por tanto se realizo la auditoria de sistemas de seguridad para verificar el riesgo por perdida de la integridad y autenticidad de la información, obteniéndose los siguientes resultados descritos en la tabla 6.5:

Tabla 6. 6: Tabla de Probabilidad de Riesgo antes de la Implantación del Software

						1-5	1-5	
N	**CR**	**Objetivo**	**Debilidad**	**Recomd.**	**Acción**	**Probabilidad de Riesgo (PR)**	**Impacto en SITTEL (IS)**	**R=PR*IS**
1	4	PS1	PS1	PS1	-	2	2	**4**
2	3	OS1	OS1	OS1	-	3	4	**12**
3	5	CCA2	CCA2	CCA2	-	2	2	**4**
4	**2**	**SP2**	**SP2**	**SP2**	**A3**	**3**	**5**	**15**
5	3	SP3	SP3	SP3	-	3	3	**9**
6	5	SFA3	SFA3	SFA3	-	3	2	**6**
7	4	CGO3	CGO3	CGO3	-	2	3	**6**
8	5	CGO6	CGO6	CGO6	-	2	2	**4**
9	5	CGO7	CGO7	CGO7	-	2	2	**4**
10	3	CA3	CA3	CA3	-	2	4	**8**
11	4	CA6	CA6	CA6	-	2	2	**4**
12	**1**	**DMS1**	**DMS1**	**DMS1**	**A1**	**5**	**4**	**20**
13	**1**	**DMS3**	**DMS3**	**DMS3**	**A2**	**5**	**5**	**25**
14	3	DMS4	DMS4	DMS4	-	5	3	**15**
15	4	GCN1	GCN1	GCN1	-	2	3	**6**
16	4	C3	C3	C3	-	0	3	**1**
							TOTAL	**137**

Fuente: Elaboración Propia

Tabla 6. 7; Tabla de Riesgos

IMPACTO	Riesgos 5	4	3	2	1
5	DMS3		SP2		
4	DMS1		OS1	SGO3-CA3	
3	DMS4		SP3	GCN1	
2			SFA3	PS1-CCA2-SGO6 SGO7-CA6	
1					C3

Fuente: Elaboración Propia

Con los resultados obtenidos en la auditoria de sistemas de seguridad realizados en la sección 5.1 de Auditoria a la Gestión de Seguridad de las Tecnologías de Información, se comparó la probabilidad de ocurrencia y el cumplimiento de objetivos respecto a la Norma Boliviana ISO/IEC 17799, concluyéndose en la tabla 6.6 de riesgos de mayor probabilidad contra la seguridad de la información de SITTEL.[46]

Donde:

PS1 SIGNIFICA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

OS1 SIGNIFICA INFRAESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN

CCA2 SIGNIFICA CLASIFICACIÓN DE LA INFORMACIÓN

SP2 SIGNIFICA CAPACITACIÓN DEL USUARIO

SP3 SIGNIFICA RESPUESTA A INCIDENTES Y ANOMALÍAS EN MATERIA DE SEGURIDAD

SFA3 SIGNIFICA CONTROLES GENERALES

GCO3 SIGNIFICA PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO

CGO6 SIGNIFICA GESTIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

CG7 SIGNIFICA INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE

CA3 SIGNIFICA RESPONSABILIDADES DE USUARIO

CA6 SIGNIFICA CONTROL DE ACCESO A LAS APLICACIONES

DMS1 SIGNIFICA REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS

DMS3 SIGNIFICA CONTROLES CRIPTOGRÁFICOS

DMS4 SIGNIFICA SEGURIDAD DE LOS ARCHIVOS DE SISTEMA

GCN1 SIGNIFICA ASPECTOS DE LA CONTINUIDAD DE LOS NEGOCIOS

C3 SIGNIFICA CONSIDERACIONES DE AUDITORIA DE SISTEMAS

Tabla 6. 8: Tabla de Objetivos

C	Importancia	Nivel	CR
Muy Alto	De 20 a 25	Muy Alto	DMS3
Alto	De 16 a 20	Alto	DMS1-SP2-DMS4-OS1
Medio	De 11 a 15	Medio	SP3-SGO3-CA3
Bajo	De 06 a 10	Bajo	SFA3-PS1-CCA2-SGO6-SGO7-CA6
Muy Bajo	De 01 a 05	Muy Bajo	C3

[46] El color rojo significa **Mayor Riesgo** y el Verde Claro el de **Menor Riesgo**.

Fuente: Elaboración Propia

En la tabla 6.7 se describen de manera esquemática los problemas con Mayor Riesgo de probabilidad de Ocurrencia e Impacto en SITTEL, quienes describen la necesidad de implementar una herramienta que coadyuve a la transferencia segura de información.

El riesgo en la seguridad de la información y con mayor probabilidad de ocurrencia fue:

- DMS3 – Controles criptográficos

Con la cual se determino que SITTEL necesita la implantación de Controles Criptográficos (cifrado de información, firmas digitales, certificados digitales y administración de claves) para asegurar la integridad de la información y la autenticidad del origen del mensaje.

6.3.3. Nivel de Seguridad después de la Implantación del Software

Se determino que para el cumplimiento de la hipótesis del proyecto de grado de "Administración de una Aplicación para Firmas y Certificados Digitales", deberá cumplir con el dominio de Desarrollo y Mantenimiento de Sistemas para los Controles criptográficos de la Norma Boliviana ISO/IEC 17799 en sus subdominios de controles criptográficos, firma digital, y administración de claves y firma digital desarrollados a continuación:

6.3.3.1. Controles criptográficos

Objetivo de la Norma sobre Controles Criptográficos: Proteger la confidencialidad, autenticidad o integridad de la información.

Se utilizaron sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

Por tanto deberá cumplir los siguientes puntos para probar que en SITTEL se mejoro el nivel de seguridad a través de la implantación del Sistema de Administración de Firmas y Certificados Digitales.

Para lo cual se realizó la revisión de los siguientes puntos:

a) La revisión de controles criptográficos con un enfoque gerencial en SITTEL en la colaboración del Jefe del Departamento de Tecnologías de Información y Comunicación a través de una encuesta sobre la seguridad de la información en SITTEL descrita en la subsección 5.1 de Auditoria de Sistemas.

b) Las funciones y responsabilidades de la seguridad de la información en SITTEL están a cargo del Analista de Sistemas[47], quien se ocupa de:

   1) La implementación de la política.

   2) La administración de las claves.

c) El nivel apropiado para la encriptación de la información en una red interna supera los 128 bits para un nivel adecuado de seguridad en la integridad de la información[48], para el nivel de encriptación de las firmas y certificados digitales se utiliza 128 bits.

d) Para la generación de Firmas Digitales se utilizan los estándares PGP por el nivel de seguridad que brinda (descrito en la sección 3.1 de Criptosistemas) y para la autentificación de las firmas digitales por Certificados Digitales se utiliza el estándar IUT X.509 S (estándar internacional para desarrollar Certificados Digitales).

e) SITTEL utiliza los siguientes modos de seguridad y los correspondientes criptosistemas descritos en la tabla 6.8 para sus sistemas de comunicación de información, los cuales no autentifican el origen de la información pero brindan encriptación de información en la intercomunicación de la información en la Superintendencia.

Tabla 6. 9: Tabla Seguridad adherida a sus Sistemas de Comunicación

Programa	Criptosistema o Método
NOVELL	SSL de 56 bits con DES/RC2/RC4
Dot Net Nuke	SSL con DES
Asp	Cifrado con DES

Fuente: Elaboración Propia

Con lo cual se **concluye** que se cumple con los requisitos para la verificación de controles criptográficos y la utilización de sistemas y técnicas esenciales para la protección de la información en estado de riesgo.

A continuación se desarrolla el segundo punto de controles criptográficos de la Norma Boliviana ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información.

[47] Información obtenida en la Encuesta realizada en SITTEL.
[48] Afirmación de Ing. Steven Clark – Microsoft Corporation

6.3.3.2. Firma digital

El sistema de Firmas Digitales comprobó los siguientes objetivos planteados por la NB ISO/IEC 17799:

- Se brinda mayor nivel de seguridad a las intercomunicaciones digitales, gracias a su implantación utilizando la técnica criptográfica PGP sobre la base de un par de claves relacionadas de manera única, donde una clave se utiliza para generar la firma digital (la clave privada) y la otra, para verificarla (la clave publica) conforme a la Norma Boliviana ISO/IEC 17799.
- Se dio recaudos para proteger la confidencialidad de la clave privada y pública mediante la encriptación del anillo de seguridad que almacena las claves, y la restricción de ingreso a la contraseña del usuario por parte del administrador a la Base de Datos de usuarios conforme a la Norma Boliviana ISO/IEC 17799.
- El nivel apropiado para la encriptación de la información en una red interna supera los 128 bits para un nivel adecuado de seguridad en la integridad de la información[49], para el nivel de encriptación de las firmas y certificados digitales se utiliza 128 bits.
- El software de Administración y Firmas Digitales tiene sustento jurídico en el Anteproyecto de Ley de Firmas Electrónicas desarrollado por SITTEL, ADSIB y PNUD.
- El sistema de firmas y certificados digitales cumple la función de brindar un servicio de no repudio conforme a la Norma Bolivia ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información que tiene SITTEL.

Con lo cual se **concluye** que se cumple con los requisitos para la verificación de firmas digitales, desarrollando un sistema para la "Administración de Firmas y Certificados Digitales" que brinda una mejor seguridad en la transferencia de información en SITTEL, además de trabajar sobre la Tecnología de 128 bits para un mayor nivel de seguridad en Asp.Net.

A continuación se desarrolla el tercer punto de Administración de Claves y Certificado Digital de la Norma Boliviana ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información.

[49] Afirmación de Ing. Steven Clark – Microsoft Corporation

6.3.3.3. Administración de Claves y Certificado Digital

La administración de claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. Cualquier compromiso o pérdida de claves criptográficas puede conducir a un compromiso de la confidencialidad, autenticidad y/o integridad de la información.

Para lo cual se implemento para la “Administración de Firmas y Certificados Digitales” en la Superintendencia de Telecomunicaciones. El sistema de administración de claves esta basado en un conjunto de normas, procedimientos y métodos seguros, que cumplen los siguientes requisitos en pro de su seguridad:

a) El sistema de Administración de Firmas y Certificados Digitales se encarga de firmas y encriptar la información, consecuentemente baja la información para que el usuario emisor adjunte el archivo firmado a un sistema de correo electrónico o aplicación de envió y recepción de información, pudiendo trabajar sobre diferentes plataformas, independiente del correo electrónico, a continuación se enlista un conjunto de herramientas donde se probo su funcionamiento (ver tabla 6.9).

Tabla 6. 10: Tabla de Comprobación de Envío y Recepción de Firma Digital

Correo	Adjunto y Envió el Archivo Firmado	Recepción y Comprobación de la Firma
Novell	Sí	Sí
Hotmail	Sí	Sí
Gmail	Sí	Sí
Yahoo	Sí	Sí

Fuente: Elaboración Propia

b) El sistema genera certificados digitales a partir de la clave pública y obtiene la información del usuario (ver sección 5.3 de Modelo Lineal Secuencial para la Firma y Certificado Digital).

c) Utiliza las claves del sistema de SITTEL y sus usuarios para facilitar su uso, y con el objetivo de que el usuario no necesite otras claves para su utilización (este punto no se puede comprobar por que no se pude mostrar los nombres de usuarios y sus contraseñas, las cuales conservan la privacidad de la información).

d) Según el funcionamiento de las Firmas y Certificados Digitales sobre PGP, se generan dos archivos denominados anillos (estructura almacenan las claves), de los cuales utiliza el PUBRING.PKR para las claves públicas y SECRING.SKR para las claves privadas (por seguridad no se dará la ubicación de las mismas), cada una de las claves genera una huella digital que identifica al usuario y tiene una correspondencia en una secuencia binaria, se utilizó este medio para proteger las claves de los usuarios y se determino que se obtendrá una copia mensual de respaldo para mayor seguridad.

e) Se determino que para tener un mayor nivel de seguridad, las claves de los usuarios caducarán cada 365 días, en el cual el sistema generara nuevas claves pública y privada para el usuario con la nueva contraseña ingresando a la opción de renovar o actualizar la firma digital del sistema, mostrando un formulario para el llenado de nuevos datos, de similar manera se realizara para la revocación o pérdida de claves.

f) En caso que una persona desee dejar de utilizar el sistema, el mismo podrá dar de baja a su usuario sin eliminar su contraseña, tendrá que elegir la opción de eliminar servicio de Firmas y Certificados Digitales, consecuentemente ingresar su usuario y contraseña.

g) Con el objetivo de que el sistema pueda ser auditado, se genera un log que registra las actividades que realiza el sistema, utiliza el tiempo, usuario, actividad.

h) Las claves tienen fechas de entrada en vigencia y de fin de vigencia, definidas por un lapso de un año, periodo definido por el nivel de riesgo que presenta SITTEL y la capacidad de descifrar la información dentro de SITTEL, al terminar el lapso el usuario tendrá que renovar su usuario y contraseña como indica el inciso e.

Con lo cual se **concluye** que se cumple con los requisitos para determinar el buen desarrollo del Sistema en su objetivo de Administración de Claves y Certificado Digital en la Superintendencia de Telecomunicaciones.

A continuación se desarrolla la Demostración de la Hipótesis a través del anterior análisis realizado en la Superintendencia de Telecomunicaciones con la Norma Boliviana ISO/IEC 17799.

6.3.3.4. Demostración de la Hipótesis

SITTEL cuenta con herramientas de brindan seguridad y control criptográfico sobre las intercomunicaciones, aseveración realizada por los resultados obtenidos en la auditoria de sistemas de seguridad por medio de la NB ISO/IEC 17799 para verificar el nuevo riesgo por perdida de la integridad y autenticidad de la información (ver tabla 6.9).

Tabla 6. 11: Tabla de Probabilidad de Riesgo despúes de la Implantación del Software

						1-5	1-5	
N	**CR**	**Objetivo**	**Debilidad**	**Recomd.**	**Acción**	**Probabilidad de Riesgo (PR)**	**Impacto en SITTEL (IS)**	**R=PR*IS**
1	4	PS1	PS1	PS1	-	1	2	**2**
2	3	OS1	OS1	OS1	-	3	4	**12**
3	5	CCA2	CCA2	CCA2	-	1	2	**2**
4	**2**	**SP2**	**SP2**	**SP2**	**A3**	**2**	**5**	**10**
5	3	SP3	SP3	SP3	-	3	3	**9**
6	5	SFA3	SFA3	SFA3	-	1	2	**3**
7	4	CGO3	CGO3	CGO3	-	2	3	**6**
8	5	CGO6	CGO6	CGO6	-	1	2	**2**
9	5	CGO7	CGO7	CGO7	-	2	2	**4**
10	3	CA3	CA3	CA3	-	1	4	**4**
11	4	CA6	CA6	CA6	-	2	2	**4**
12	**1**	**DMS1**	**DMS1**	**DMS1**	**A1**	**3**	**4**	**12**
13	**1**	**DMS3**	**DMS3**	**DMS3**	**A2**	**2**	**5**	**10**
14	3	DMS4	DMS4	DMS4	-	4	3	**12**
15	4	GCN1	GCN1	GCN1	-	2	3	**6**
16	4	C3	C3	C3	-	0	3	**0**
							TOTAL	**98**

Fuente: Elaboración Propia

Comparando los resultados obtenidos en la sección 5.1 de Auditoria a la Gestión de Seguridad de las Tecnologías de Información se observa que DMS3 y DMS1 bajó de 25 a 10 de riesgo y 20 a 8 de riesgo respectivamente, además disminuyo de 137 a 98 la probabilidad de riesgo en contra de la seguridad de la información, la disminución del riesgo se observa en forma más detallada en la tabla 6.10 de riesgos y en la tabla 6.11 de Objetivos.

Tabla 6. 12: Tabla de Riesgos

IMPACTO	Riesgos 5	4	3	2	1
5					
4			OS1		
3		DMS1	SP3		
2	SP2-DMS5		CGO3-GCN1	SGO7-CA6	PS1
1		CA3		CA2-SFA3-SGO6	C3

Fuente: Elaboración Propia

Tabla 6. 13: Tabla de Objetivos

C	Importancia	Nivel	CR
Muy Alto	De 20 a 25	Muy Alto	
Alto	De 16 a 20	Alto	SP2-DMS5-DMS1-OS1
Medio	De 11 a 15	Medio	SP3
Bajo	De 06 a 10	Bajo	CA3-CGO3-GCN1-SGO7-CA6
Muy Bajo	De 01 a 05	Muy Bajo	CA2-SFA3-SGO6-PS1-C3

Fuente: Elaboración Propia

Con la cual se determino que la implantación de Controles Criptográficos a través de las firmas y certificados digitales aseguran la integridad de la información y la autenticidad del origen del mensaje, y se concluye que el nuevo sistema implantado ofrece confidencialidad, integridad y autenticidad a la información en SITTEL, aceptándose la hipótesis de:

$$H_1 = \overline{X}_A > \overline{X}_B$$

- **Hipótesis Estadística (H1)**

  La aplicación de firmas y certificados digitales acorde a la NB ISO/IEC 17799 para los procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones permite tener un mayor nivel de confiabilidad que los sistemas actuales y conserva la integridad de la información como también verifica la autenticidad del origen del mensaje.

Por lo tanto se acepta la Hipótesis estadística H1.

Conclusión del Capítulo

El presente capítulo es parte importante para la culminación del presente trabajo propuesto que muestra el desarrollo y la comprobación de la hipótesis con el objetivo de probar todo lo planteado en formulación del capítulo 1.

Capítulo 7
Conclusiones y Recomendaciones

"… los argumentos como los hombres generalmente son pretenciosos."
Platón

Resumen

El presente capítulo contiene las conclusiones y recomendaciones pertinentes a la culminación del desarrollo del Sistema para la Administración de Firmas y Certificados Digitales implantados en la Superintendencia de Telecomunicaciones.

Conclusiones

A la finalización del presente trabajo de grado se han llegado a las siguientes conclusiones:

- Se realizó una auditoria de sistemas a SITTEL con la NB-ISO-IEC 17799 con el objetivo de obtener los niveles de seguridad de información antes y después de haber implementado el software, concluyendo que su mayor problema era la falta de herramientas criptográficas, la cual fue absuelta por el desarrollo del Administrador de Firmas y Certificados Digitales adecuadas a las necesites tecnológicas de SITTEL, cumpliéndose con los objetivos a) y e) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

- Se evito la pérdida de documentos físicos que son digitalizados y autentificados a cada usuario por firmas digitales a través de la implantación del Sistema de Administración de Firmas y Certificados Digitales, cumpliéndose con el objetivo b) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

- Se evaluó y aplicó el criptosistemas PGP que aseguran la integridad de la información y la autenticidad del origen del mensaje mediante el desarrollo de un administrador de firmas y certificados digitales, cumpliéndose con el objetivo d) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

- Se disminuyo el costo de mantenimiento de las firmas y certificados digitales con el desarrollo del software para administración de las mismas, además su implantación fue realizado sobre la plataforma Microsoft .Net y el sistema funciona independiente de la plataforma de software (Sistemas Operativos, Aplicaciones y Browser) y Hardware (ver capítulo 4. Factibilidad del Proyecto), cumpliéndose con el objetivo c) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

- La utilización del Sistema de Administración de Firmas y Certificados Digitales esta desarrollado bajo los estándares internacionales del ISO/IEC 17799 para los Sistemas de Gestión de Seguridad de la Información, es un sistema auditable por que genera log de seguridad y ofrece seguridad en la información que resguarda por métodos de encriptación (ver sección 5.1-5.2), cumpliéndose con el objetivo e) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

- Se contribuyó a la seguridad de la Información en SITTEL a través del desarrollo de firmas y certificados digitales que fueron evaluados por el ISO 9126[50] y las métricas de McCall, utilizando la NB ISO/IEC 177999 para afianzar la integridad de la información, autenticidad del origen del mensaje y se obtuvo un mayor nivel de confiabilidad que los sistemas actuales (ver sección 6.2-6.3), cumpliéndose con el objetivo e) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

- La utilización de Firmas y Certificados Digitales son parte de la implantación de PKI (Public Key Infrastructure – Infraestructura de Llaves Públicas), la cual permite a las partes realizar transacciones a través de la red para identificarse una a la otra proveyendo autenticidad en los certificados digitales y realizar comunicaciones seguras confiriendo confidencialidad a través del uso de la

[50] El producto resultante será evaluado contra los parámetros indicados por el estándar ISO/IEC 9126 (funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y transportabilidad) – **Ver Anexo D**.

encriptación, y autenticidad, integridad de datos y una base razonable para el no repudio mediante el uso de la firma digital y certificados digitales, cumpliéndose con el objetivo a) de la sección 1.4.2 de Objetivos Específicos del Capítulo de Generalidades.

Recomendaciones

A la finalización del presente trabajo de grado se espera que la Superintendencia de Telecomunicaciones tome en cuenta las siguientes recomendaciones:

- El presente trabajo demostró que el uso de firmas y certificados digitales en SITTEL mejoró su nivel de seguridad de la información.

- Siendo la Superintendencia de Telecomunicaciones el organismo que controla y protege las comunicaciones de los bolivianos, deberá tener entre sus objetivos implantar un sistema PKI (Infraestructura de Llave Pública) para el uso general de la sociedad, permitiendo autentificar a los usuarios por firma digitales en reemplazo de Carnets de Identidad, transacciones monetarias en tiendas y bancos, pago de impuestos, etc. Mediante Firmas y Certificados Digitales.

- Se recomienda realizar una auditoria de sistemas externa una vez al año y realizar una auditoria de sistemas interna dos veces al año y deberán contratar a un oficial de seguridad.

- Deberán implantar y Certificar a la Superintendencia de Telecomunicaciones con la Norma Boliviana ISO/IEC 17799 por el Departamento de Tecnologías de Información y Comunicación.

- El Sistema de Administración de Firmas y Certificados Digitales deberá evolucionar hacia una Infraestructura de Llaves Públicas (PKI) para el uso de la

Sociedad Boliviana y la evaluación de la Sociedad de la Información entre SITTEL, ADSIB y PNUD.

Bibliografía

AUTORES Y LIBROS

[PRESSMAN, ©2002]. PRESSMAN, Roger S. “Ingeniería de Software”, Editorial Mc Graw Hill, 5ta Edición, Madrid, España. ©2002.

[LUCENA LOPEZ, Criptografía y Seguridad en Computares]. LUCENA, Manuel. “Criptografía y Seguridad en Computadoras”, Departamento de Informática de la Escuela Politécnica Superior - Universidad de Jaén. ©2002.

[CABRERA, ©2001]. CABRERA, Federico. “Firmas Digitales”. ©2001. Disponible en Internet en: www.monografías.com

[ALCALDE, ©1997]. ALCALDE, Eduardo – GARCÍA, Miguel. “Informática Básica”, Editorial Mc Graw Hill, 2da Edición, Bogota, Colombia. ©1997.

[Kendall & Kendall, ©2001]. KENDALL, Kenneth – KENDALL, Julie. “Análisis y Diseño de Sistemas”, Prentice Hall Hispanoamericana, S.A. 3ra Edición, Ciudad de México, México. ©1997.

[JOYANES, ©1997]. JOYANES, Luís. “Fundamentos de Programación” Algoritmos y Estructura de Datos, Mc Graw Hill, 2da Edición, Bogota, Colombia. ©1997.

[TANENBAUM, ©1999]. TANENBAUM, Andrew. “Redes de Computadoras”, Prentice Hall Hispanoamericana, S.A. 3ra Edición, Ciudad de México, México. ©1999.

[SILBERSCHATZ, ©1994]. SILBERSCHATZ, Abraham – KORTH, Henry – SUDARSAHN. “Fundamentos de Bases de Datos”, Mc Graw Hill, 3ra Edición, Madrid, España. ©1994.

[www.microsoft.com] Microsoft Press. “Writing Secure Code”. ©2003.

[www.microsoft.com] Microsoft Press. “Building secure Microsoft ASP.NET Applications”. ©2004. Disponible en Internet en: http://www.microsoft.com/downloads/release.asp?ReleaseID=44047

[GARCÍA PELAYO, ©1999] GARCÍA PELAYO, Ramón – GROSS. “Diccionario Pequeño Larousse Ilustrado”, Librairie Lorousse, Francia, París. ©1964.

[SITTEL, ©1998-2001]. Superintendencia de Telecomunicaciones. “Regulación de las Telecomunicaciones en Bolivia 1998 - 2001”, La Paz, Bolivia. ©1998-2001. Disponible en Internet en: http://www.sittel.gov.bo

[SITTEL, ©1998-2001]. Superintendencia de Telecomunicaciones. “Telecomunicaciones: Un salto al futuro”, La Paz, Bolivia. ©2002. Disponible en Internet en: http://www.sittel.gov.bo

[URIONA ROSALES, ©2004]. URIONA ROSALES, Guido. Apuntes de la Materia de “Seguridad de Sistemas” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[ORTIZ LOAYZA, ©2004]. ORTIZ LOAYZA, Katherine Wendy. ”Diseño de un Sistema Inteligente de Seguridad para Computadoras Personales” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[ALCOCER MOLINA, 2004]. ALCOCER MOLINA, Rodney. ”Prototipo para Cursos de Post Grado Virtuales CASO: Maestría de Educación Superior de la EMI” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[SARMIENTO CALISAYA, ©2004]. SARMIENTO CALISAYA, Jenny Emerith. ”Modelo Computacional para Detectar el Segmento de una Falla de una Red” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[LOPEZ COLQUE, ©2004]. LOPEZ COLQUE, Leopoldo. ”Biblioteca Virtual EMI” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[GUTIERREZ, ©2004]. GUTIERREZ, Víctor Adrián. ”Diseño de un Sistema de Seguridad Informático CASO: CADE BOLIVIA S.A.” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[CARDENAS ZEBALLOS]. CARDENAS ZEBALLOS, Zelma Nancy. ”Sistema Experto Interactivo de Seguimiento del Desarrollo Cognitivo en Relación a la Motricidad para Niños en Edad Escolar” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[COAJERA VALERA, ©2004]. COAJERA VALERA, Hernán Gonzalo. ”Algoritmo de Encriptación de Datos Basado en Módulos de Interpolación” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[LOZA LUNA, ©2004]. LOZA LUNA, Carlos Renzo. ”Diseño de un Sistema Integrado de Seguridad y Control de Acceso Biométrico” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2004.

[SAKURA SATO, ©2004]. SAKURA SATO, Sergio Kenji. ”Diseño de un Algoritmo de Comprensión para Archivos de Sonido” – Escuela Militar de Ingeniería, La Paz,

Bolivia. ©2004.

[LOPEZ QUIROGA, ©2000]. LOPEZ QUIROGA, Coral. ”Sistema Centralizado de Información para el Registro y Seguimiento de Fallas de los Servicios y Telecomunicaciones de ENTEL S.A.” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2000.

[FLORES GUILLEN, ©2000]. FLORES GUILLEN, Víctor Osman. ”Emisión de Certificados de Nacimiento en la ciudad de La Paz con Tecnología VPN” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2000.

[VEIZAGA MACHICADO, ©2003]. VEIZAGA MACHICADO, Juan Manuel. ”Encriptador de Texto Aplicado a Autómatas Celulares Reversibles” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2001.

[MIER CORNEJO, ©2001]. MIER CORNEJO, Edwin. ”Método de Análisis de Sistemas para el Evaluación de Sistemas en Organizaciones Públicas” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©2001.

[CUELLAR, ©1999]. CUELLAR, Adrián. ”Neuro Identificador Funcional para Sistemas de Seguridad” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©1999.

[CUEVAS, ©1998]. CUEVAS, Alejandro. ”Medición de Comportamiento del Tráfico en Internet y sus Modelo mediante Características Fractales” – Escuela Militar de Ingeniería, La Paz, Bolivia. ©1998.

[NEILSON, www.monografías.com]. NEILSON, Jaime. “Comercio Electrónico”. ©2000. Disponible en la Web en: www.monografias.com.

[www.symantec.com]. SYMANTEC COMPANY. “Técnicas, Políticas y Herramientas de Auditoria de Seguridad”. ©2001. Disponible en la web: www.symantec.com.

[FERNÁNDEZ, ©2000]. FERNÁNDEZ, María Carmen. “Ciclo de Vida del Software”. ©2000. Disponible en la web en: www.monografias.com.

[COMPUTER SOCIETY, IEEE, ©1993]. COMPUTER SOCIETY, IEEE. “Definición de la Ingeniería de Software”. ©1993. Disponible en la web: www.computer.org.

[ENCICLOPEDIA LAROUSSE ILUSTRADA, ©1963]. ENCICLOPEDIA LAROUSSE ILUSTRADA. “DICCIONARIO”. ©1963.

[Advance Team, © 2004] ADVANCE TEAM, DALLAS, TEXAS, USA. Disponible en la

Web: www.advanceteam.com – www.atctraing.com

[CRIPTORED, ©2005] - RED TEMATICA IBEROAMERICANA DE CRIPTOGRAFIA Y SEGURIDAD DE LA INFORMACION. Disponible en la Web: http://www.criptored.upm.es/

[RSASECURITY, ©2005] – RSA Security Sign On-Manager. Disponible en la Web: http://www.rsasecurity.com/node.asp?id=2541

[REDIRIS, ©2005] - RED ESPAÑOLA DE I+D. Disponible en la Web. http://www.rediris.es/

[PGP, ©2005] – Encriptación para Datos, Privacidad para Clientes y Seguridad para empresas. Disponible en la Web: http://www.pgp.com/

[PGPI, ©2005] - The International PGP. Disponible en la Web: http://www.pgpi.org/

[GNUPGP, ©2005] – Organización de Software Libre Linux – PGP. Disponible en la Web: http://www.gnupgp.com/

[UIT. ©1998] - International Telecommunication Union o Unión Internacional de Telecomunicaciones (UIT). Disponible en la Web: www.itu.int/home/index-es.html

NORMAS APLICABLES A FIRMAS Y CERTIFICADOS DIGITALES

Organización Internacional de Estandarización (ISO)

NB-ISO-IEC 17799:2003

Tecnología de la Información – Código de práctica para la Gestión – Noviembre del 2003

ISO/IEC 15408-2:1999

Information Technology – Quality techniques – Digital Signatures with appendix – Part 2: Security functional components

ISO/IEC 14888-1:1998

Information Technology – Security techniques – Digital Signatures with appendix – Part 1: General

ISO/IEC 14888-1:1999

Information Technology – Security techniques – Digital Signatures with appendix – Part 2: Identify – mechanisms

ISO/IEC 14888-1:1998

Information Technology – Security techniques – Digital Signatures with appendix – Part 3: Certification – mechanisms

ISO/IEC 13888-1:1998

Information technology – Security techniques – Non-repudiation – Part 1: General

ISO/IEC 15945:2002

Information Technology – Security techniques – Specification of TTP services to support the application of digital signatures

ISO/IEC 15946-2:2002

Information Technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures

ISO/IEC 15946-4:2002

Information Technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital Signatures giving message recovery

Unión de Telecomunicaciones Internacional (ITU)

ITU-T X.509:

Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

ITU-T X.680:

Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation

ITU-T X.681:

Information technology – Abstract Syntax Notation One (ASN.1): Information object specification

ITU-T X.682:

Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification

ITU-T X.690:

Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

ITU-T X.691:

Information technology – ASN.1 encoding rules – Specification of Packed Encoding Rules (PER)

ITU-T X.693:

Information technology – ASN.1 encoding rules: XML encoding`rules (XER)

Organización en Estándares de Transmisión de Información por Internet

IETF RFC 3280:

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

IETF RFC 3647:

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

IETF RFC 3369:

Cryptographic Message Syntax (CMS)

IETF RFC 3370:

Cryptographic Message Syntax (CMS) Algorithms

IETF RFC 2797:

Certificate Management Messages over CMS

IETF RFC 2633:

S/MIME Version 3 Message Specification

IETF RFC 2632:

S/MIME Version 3 Certificate Handling

IETF RFC 2634:

Enhanced Security Services for S/MIME

COBIT

COBIT: Control Objectives for Information and Related Technology. 1998.

CURSOS, CONGRESOS Y POSTGRADOS

UNIVERSIDAD DEL SALVADOR, ARGENTINA – GEORGETOWN UNIVERSITY – ESTADOS UNIDOS. Postgrado en E-Business Management, “Firmas y Certificados Digitales, Marco Legal, Año 2001. Disponible en Internet en: http://appcpenn.org/International

CEPAL. Conferencia “Los caminos hacia una Sociedad de la Información en América Latina y el Caribe”. 2003 – http://www.alfa-redi.org

IBNOCAR: Seminario Internacional sobre “Gestión de la Seguridad de la Información en la empresa Norma ISO/IEC 17799” Expositor: Espeditto Pasarello. Santa Cruz – Bolivia. 25-26 de Noviembre de 2004.

Ilustre Colegio de Abogados. II Jornadas Internacionales de Informática y Derecho. Del 28 de febrero al 2 de marzo de 2005 – http://www.derechoteca.com/informatica

Microsoft Company. 1º Foro Latinoamericano de Seguridad Informática de Tecnologías de Microsoft. 2004 – http://www.microsft.com

EXPERTOS CONSULTADOS

Msc. Ing. Guido Rosales Uriona

CISA - CISM

Gerente General – YanapTi Consultores

Msc. Lic. Fernando Yañez Romero

Catedrático de la Carrera de Ingeniería de Sistema

Escuela Militar de Ingeniería

Msc. Ing. Carlos Moratto A.

Docente de la Materia de Ingeniería de Software

Escuela Militar de Ingeniería

Msc. Lic. Amparo Subieta

Jefe del Departamento de Tecnologías de Información y Comunicación

Superintendencia de Telecomunicaciones

Msc. Ing. Giovanni C. Gismondi P.

Analista de Tecnologías de Información

Superintendencia de Telecomunicaciones

Ing. Marcelo Lorente

Analista de Tecnologías de Información Web

Superintendencia de Telecomunicaciones

Ing. Roberto Baya

Administrador de la Base de Datos

Superintendencia de Telecomunicaciones

Lic. Claudio Arce

Administrador de la Base de Datos y Especialista en Lotus

Superintendencia de Telecomunicaciones

Dr. Ing. Expedito Pasarello

Coordinador de Tecnologías de la Información

Comité de Normalización de las Normas ISO/IEC 17799

Msc. Ing. Fernando Echevarria

Gerente B - SPA

Price Water House Coopers

Ing. Martín Otero

Asistente B - SPA

Price Water House Coopers

Msc. Ing. Cecilia Esther Uriona Lanza

Especialista en desarrollo de aplicaciones Web

SaiTec

Ing. Alejandro Gozalves

Experto Microsoft en Seguridad

Instituto COGNOS

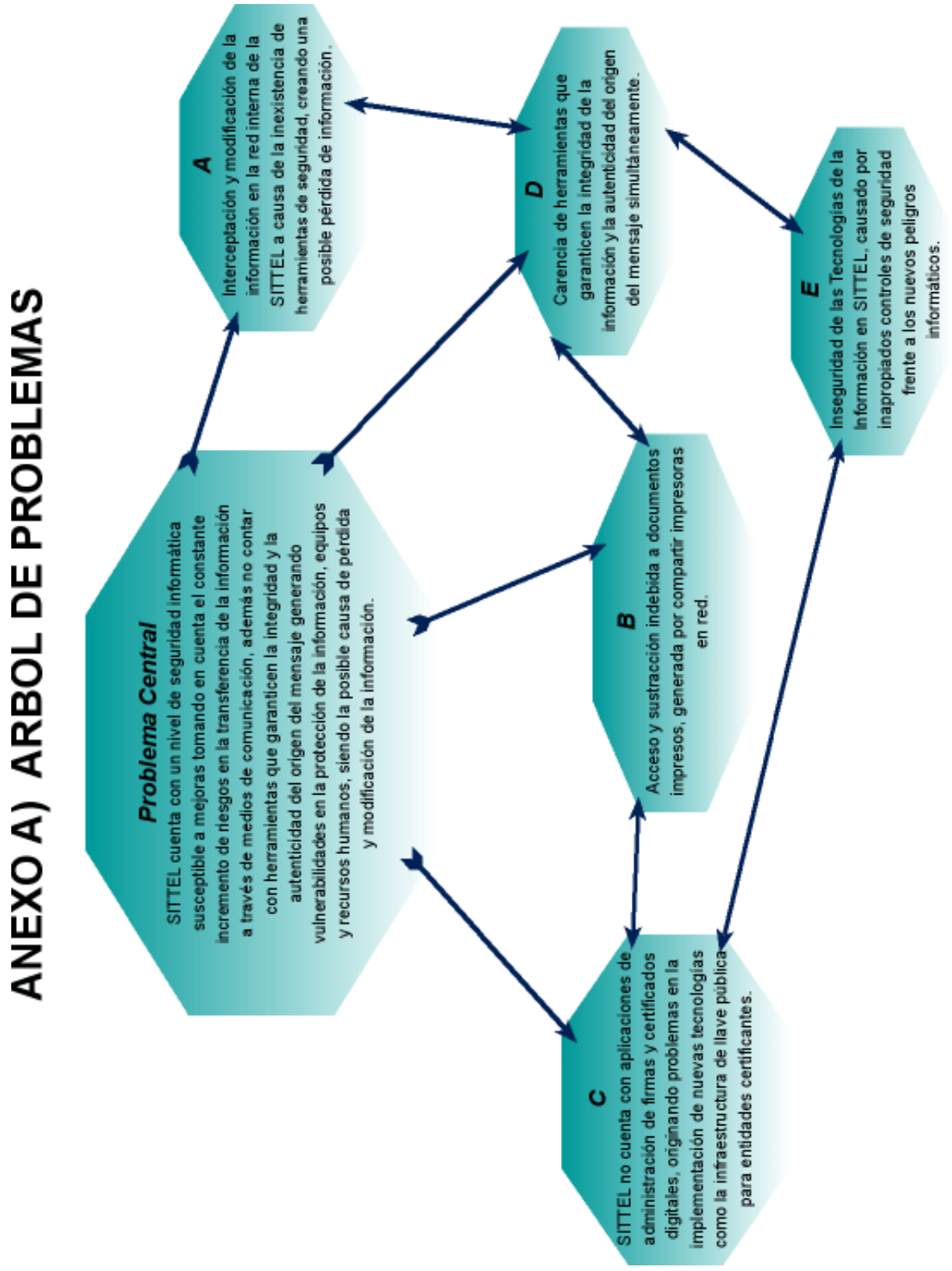
Ing. Esven Palma

Experto en Factibilidad de Proyectos

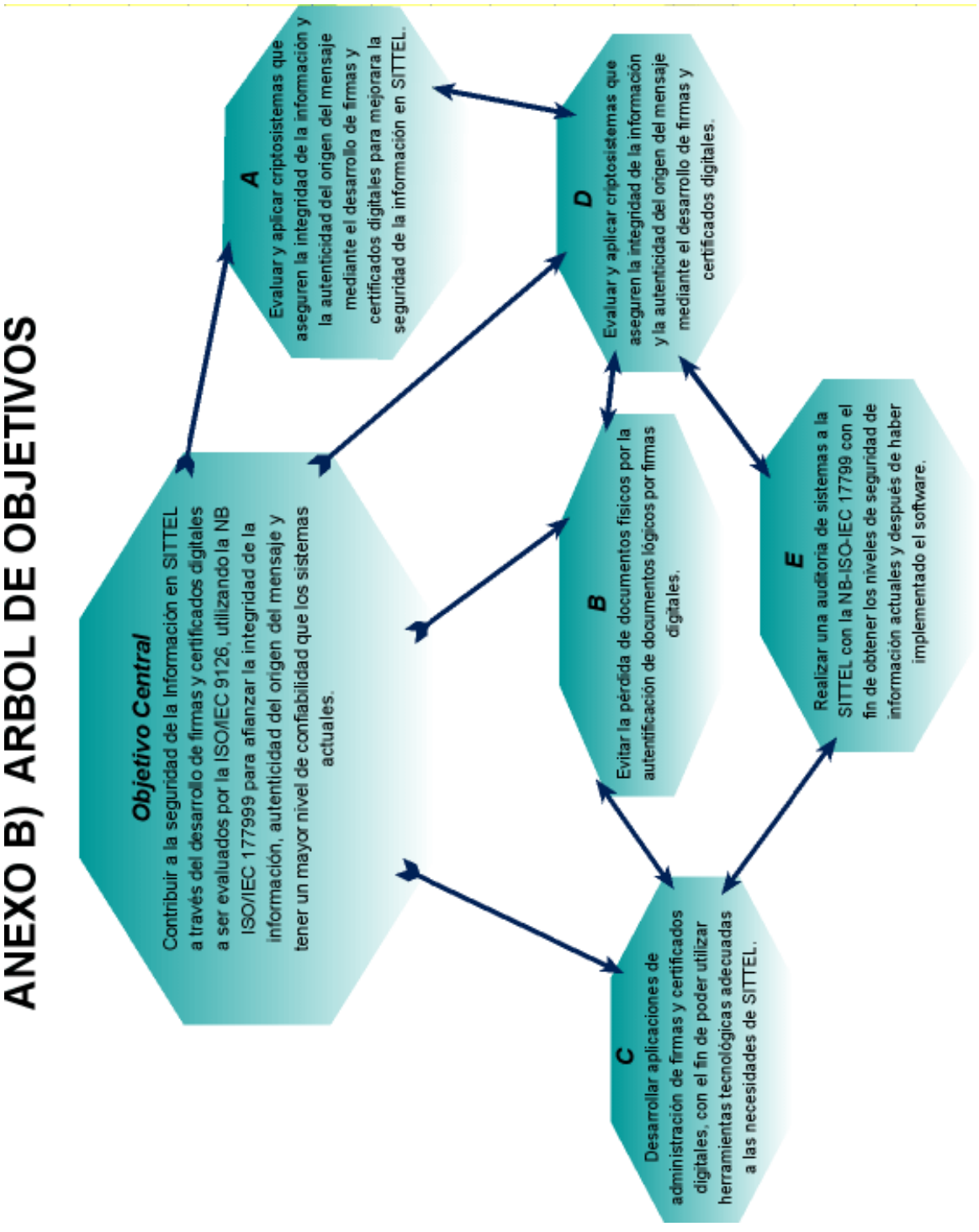
TOYOSA S.A.

ANEXOS

ANEXO A


ANEXO A) ARBOL DE PROBLEMAS
Problema Central
SITTEL cuenta con un nivel de seguridad informática susceptible a mejoras tomando en cuenta el constante incremento de riesgos en la transferencia de la información a través de medios de comunicación, además no contar con herramientas que garanticen la integridad y la autenticidad del origen del mensaje generando vulnerabilidades en la protección de la información, equipos y recursos humanos, siendo la posible causa de pérdida y modificación de la información.
A
Interceptación y modificación de la información en la red interna de la SITTEL a causa de la inexistencia de herramientas de seguridad, creando una posible pérdida de información.
B
Acceso y sustracción indebida a documentos impresos, generada por compartir impresoras en red.
C
SITTEL no cuenta con aplicaciones de administración de firmas y certificados digitales, originando problemas en la implementación de nuevas tecnologías como la infraestructura de llave pública para entidades certificantes.
D
Carencia de herramientas que garanticen la integridad de la información y la autenticidad del origen del mensaje simultáneamente.
E
Inseguridad de las Tecnologías de la Información en SITTEL, causado por inapropiados controles de seguridad frente a los nuevos peligros informáticos.

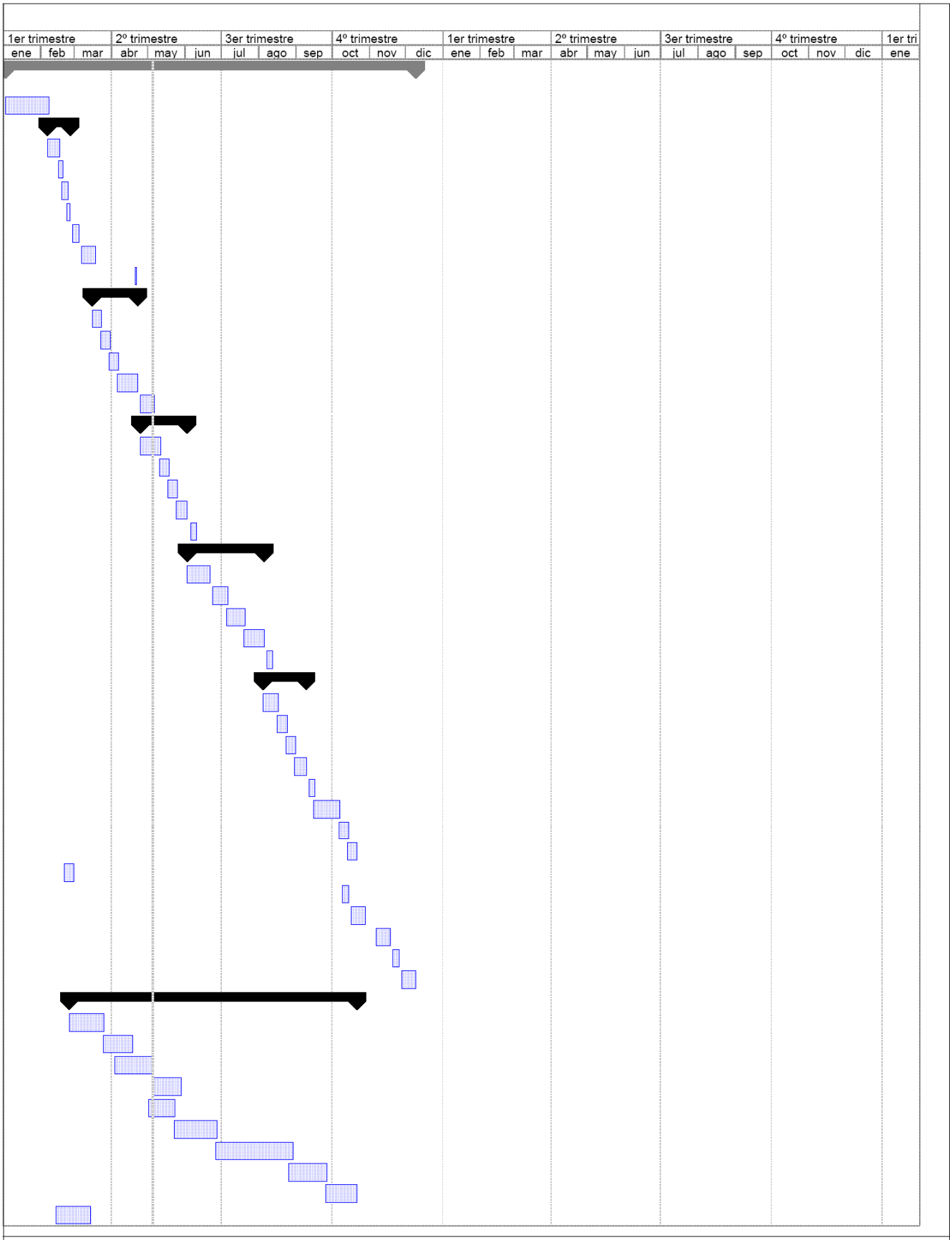
ANEXO B


ANEXO B) ARBOL DE OBJETIVOS
Objetivo Central
Contribuir a la seguridad de la Información en SITTEL a través del desarrollo de firmas y certificados digitales a ser evaluados por la ISO/IEC 9126, utilizando la NB ISO/IEC 177999 para afianzar la integridad de la información, autenticidad del origen del mensaje y tener un mayor nivel de confiabilidad que los sistemas actuales.
A
Evaluar y aplicar criptosistemas que aseguren la integridad de la información y la autenticidad del origen del mensaje mediante el desarrollo de firmas y certificados digitales para mejorara la seguridad de la información en SITTEL.
B
Evitar la pérdida de documentos físicos por la autentificación de documentos lógicos por firmas digitales.
C
Desarrollar aplicaciones de administración de firmas y certificados digitales, con el fin de poder utilizar herramientas tecnológicas adecuadas a las necesidades de SITTEL.
D
Evaluar y aplicar criptosistemas que aseguren la integridad de la información y la autenticidad del origen del mensaje mediante el desarrollo de firmas y certificados digitales.
E
Realizar una auditoria de sistemas a la SITTEL con la NB-ISO-IEC 17799 con el fin de obtener los niveles de seguridad de información actuales y después de haber implementado el software.

ANEXO C

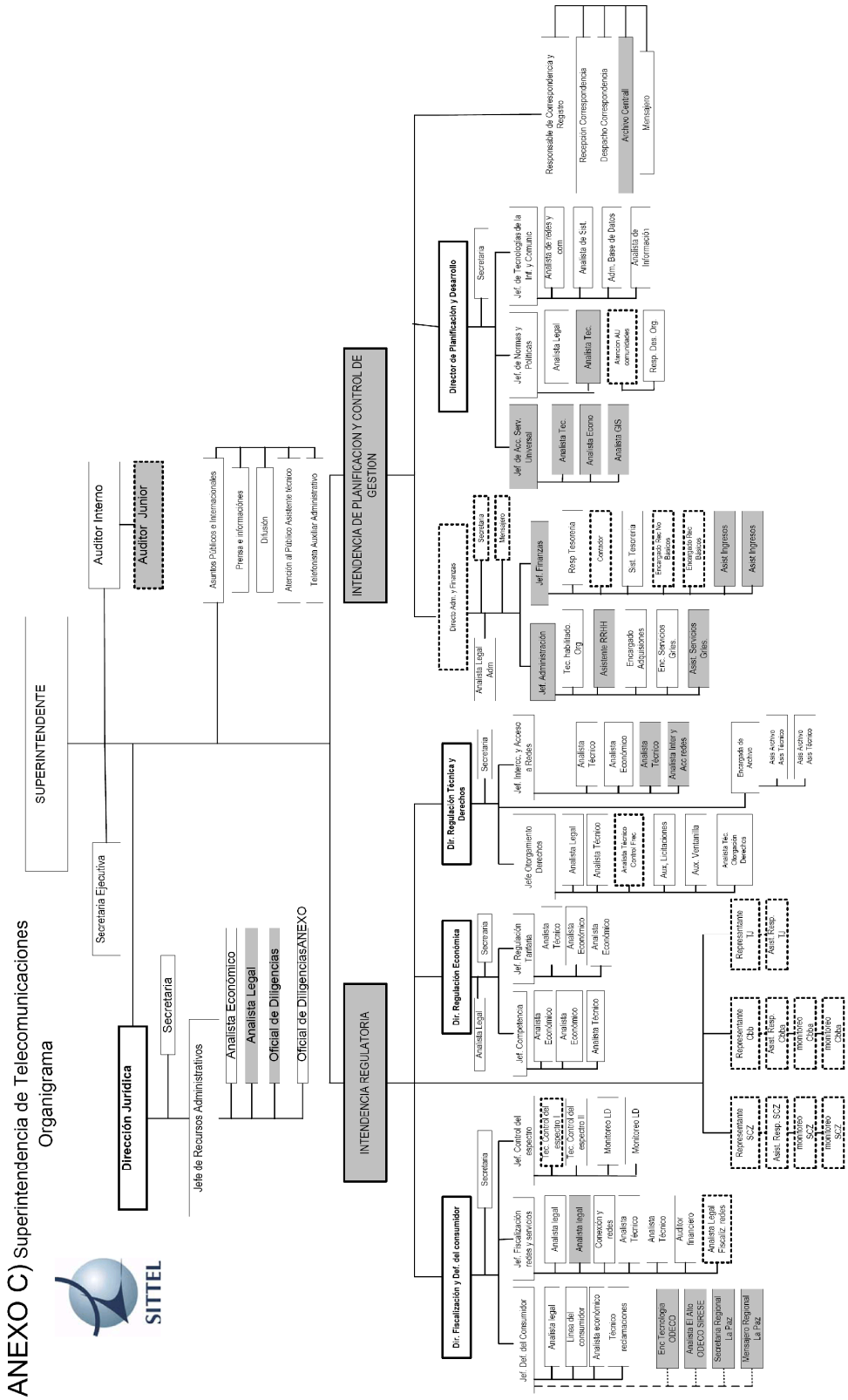
Cronograma de Actividades

Id	Nombre de tarea	Duración	Comienzo	Fin
0	**12. Cronograma**	**252 días**	**lun 05-01-03**	**vie 05-12-09**
1	Elección de Tema de Tesis	26 días	lun 05-01-03	lun 05-02-07
2	**Desarrollo de Perfil**	**16 días**	**lun 05-02-07**	**vie 05-02-25**
3	Presentación del 1º Borrador - Presentación hasta Justificación	8 días	lun 05-02-07	mié 05-02-16
4	Presentación del 2º Borrador - Presentación hasta Cronograma	4 días	mié 05-02-16	sáb 05-02-19
5	Presentación del 3º Borrador - Presentación hasta Glosario	4 días	sáb 05-02-19	mié 05-02-23
6	**Presentación del Perfil de Tesis y Documentación Completa**	**3 días**	**mié 05-02-23**	**vie 05-02-25**
7	**Revisión del Perfil del Trabajo de Grado (Elección del Tribunal)**	5 días	lun 05-02-28	vie 05-03-04
8	**Defensa del Perfil del Tribunal (1º Parcial)**	10 días	lun 05-03-07	vie 05-03-18
9	**Aprobación del Perfil del Decanato**	1 día	jue 05-04-21	jue 05-04-21
10	**Desarrollo del Marco Teórico**	**28 días**	**mié 05-03-16**	**vie 05-04-22**
11	Presentación del Marco Teórico (1º Borrador)	6 días	mié 05-03-16	mié 05-03-23
12	Presentación del Marco Teórico (2º Borrador)	6 días	mié 05-03-23	mié 05-03-30
13	Presentación del Marco Teórico (3º Borrador)	6 días	mié 05-03-30	mié 05-04-06
14	**Presentación del Marco Teórico**	13 días	mié 05-04-06	vie 05-04-22
15	**Defensa del Marco Teórico del Tribunal (2º Parcial)**	10 días	lun 05-04-25	vie 05-05-06
16	**Desarrollo del Marco Práctico - 1º Parte**	**31 días**	**lun 05-04-25**	**jue 05-06-02**
17	Presentación del Marco Práctico (1º Borrador)	14 días	lun 05-04-25	mié 05-05-11
18	Presentación del Marco Práctico (2º Borrador)	6 días	mié 05-05-11	mié 05-05-18
19	Presentación del Marco Práctico (3º Borrador)	6 días	mié 05-05-18	mié 05-05-25
20	**Presentación del Marco Práctico**	8 días	mié 05-05-25	jue 05-06-02
21	**Defensa del Marco Práctico del Tribunal (Final)**	5 días	lun 05-06-06	vie 05-06-10
22	**Desarrollo del Marco Práctico - 2º Parte**	**49 días**	**vie 05-06-03**	**vie 05-08-05**
23	Presentación del Marco Práctico (1º Borrador)	14 días	vie 05-06-03	mar 05-06-21
24	Presentación del Marco Práctico (2º Borrador)	11 días	vie 05-06-24	mié 05-07-06
25	Presentación del Marco Práctico (3º Borrador)	11 días	mié 05-07-06	mié 05-07-20
26	**Presentación del Marco Práctico**	13 días	mié 05-07-20	vie 05-08-05
27	**Revisión por Tirbunal ante Docente y Tutor (1º Parcial)**	5 días	lun 05-08-08	vie 05-08-12
28	**Desarrollo del Estudios Complementarios y Conclusiones**	**26 días**	**vie 05-08-05**	**vie 05-09-09**
29	Presentación de Conclusiones (1º Borrador)	9 días	vie 05-08-05	mié 05-08-17
30	Presentación de Conclusiones (2º Borrador)	6 días	mié 05-08-17	mié 05-08-24
31	Presentación de Conclusiones (3º Borrador)	6 días	mié 05-08-24	mié 05-08-31
32	**Presentación del Marco Práctico**	8 días	mié 05-08-31	vie 05-09-09
33	**Revisión con Tribunal (2º Parcial)**	5 días	lun 05-09-12	vie 05-09-16
34	**Presentación Borrador**	16 días	vie 05-09-16	vie 05-10-07
35	Revisión Previa ante el Tribunal (1º Borrador)	6 días	vie 05-10-07	vie 05-10-14
36	Revisión Previa ante el Tribunal (2º Borrador)	6 días	vie 05-10-14	vie 05-10-21
37	Revisión Previa ante el Tribunal (3º Borrador)	6 días	lun 05-02-21	lun 05-02-28
38	**Revisión Tribunal**	5 días	lun 05-10-10	vie 05-10-14
39	**Defensa ante Tribunal Completa**	10 días	lun 05-10-17	vie 05-10-28
40	**Correlación de Errores y Presentación en Limpio**	10 días	lun 05-11-07	vie 05-11-18
41	**Semana de Examenes Finales**	5 días	lun 05-11-21	vie 05-11-25
42	**Exposición y Defensa Final del Trabajo de Grado**	10 días	lun 05-11-28	vie 05-12-09
43	**Software: Firmas y Certificados Digitales**	**177 días**	**vie 05-02-25**	**vie 05-10-21**
44	Obtención de Información	21 días	vie 05-02-25	vie 05-03-25
45	Análisis de la Información	17 días	vie 05-03-25	lun 05-04-18
46	Auditoria de Sistemas	25 días	lun 05-04-04	jue 05-05-05
47	Análisis del Encriptador a utilizarse	18 días	vie 05-05-06	sáb 05-05-28
48	Análisis del Sistema y Determinación de Requerimientos	17 días	lun 05-05-02	lun 05-05-23
49	Diseño del Software que contiene Subsistemas que explican el funcio	29 días	lun 05-05-23	lun 05-06-27
50	Desarrollo del Sistema	47 días	lun 05-06-27	lun 05-08-29
51	Prueba del Sistema	22 días	vie 05-08-26	lun 05-09-26
52	Implantación, Evaluación y Determinación de Mejoras en la Seguridad	20 días	lun 05-09-26	vie 05-10-21
53	**Análisis del Anteproyecto de Ley de Firmas y Certificados Digitales**	22 días	lun 05-02-14	lun 05-03-14


1er trimestre
2º trimestre
3er trimestre
4º trimestre
1er trimestre
2º trimestre
3er trimestre
4º trimestre
1er tri
ene
feb
mar
abr
may
jun
jul
ago
sep
oct
nov
dic
ene
feb
mar
abr
may
jun
jul
ago
sep
oct
nov
dic
ene

ANEXO D

Organigrama de la SITTEL



ANEXO E

Acreditación de Sistemas – CALIDAD

REQUERIMIENTO		**CÓDIGO MESA DE AYUDA:**	
Descripción del Sistema:			
Propósito del Sistema:			
Fecha Solicitada.		**Criticidad:**	

Responsabilidad	**Nombre**	**Fecha Designación**	**Firma**
Funcionalidad			
Fiabilidad			
Usabilidad			
Eficiencia			
Mantenibilidad			
Portabilidad			
Documentos			

FUNCIONALIDAD				
ACTIVIDADES	**RESULTADOS (Referencia a documentación de respaldo)**	**APROBACIÓN DEL EVALUADOR**		
		SI	**NO**	**OBSERVACIONES**
Conveniencia, Exactitud, Interoperatividad, Conformidad, Seguridad		☐	☐	

FIABILIDAD				
ACTIVIDADES	**RESULTADOS (Referencia a documentación de respaldo)**	**APROBACIÓN JEFE DE TECNOLOGÍA**		
		SI	**NO**	**OBSERVACIONES**
Madurez, Tolerancia a Fallos, Recuperabilidad, Conformidad		☐	☐	

USABILIDAD				
ACTIVIDADES	**RESULTADOS (Referencia a documentación de respaldo)**	**APROBACIÓN JEFE DE TECNOLOGÍA**		
		SI	**NO**	**OBSERVACIONES**
Comprensibilidad, Facilidad de aprendizaje, Operabilidad, Conformidad, Atractividad		☐	☐	

ANEXO F

SITTEL

1. Reforma Estructural en 1980

En los años 80, el esquema presentado en la Figura E1 comenzó a mostrar sus debilidades. Se hizo clara la percepción del fracaso de la concepción del Estado empresario. En el caso particular de las telecomunicaciones, si bien ENTEL estatal logró importantes ganancias en eficiencia interna -inclusive superiores a los niveles iniciales de eficiencia posteriores a su privatización- y , en general, la calidad de sus servicios era buena fue necesario dotarle de mecanismos más ágiles de gestión acordes con los de las empresas privadas.

Figura E1: Reforma Estructural

Fuente: Elaboración Propia

El monopolio privado de la televisión local, responsable del suministros del servicio básico, enfrento graves problemas, que se manifestaron en hechos concretos, como el pobre desarrollo de la red, baja productividad, ingresos inadecuados, tarifas subvencionadas fijadas por los municipios y un catálogo de servicios muy reducido.

Estos elementos y la toma de conciencia de la importancia de decisiva del sector para el desarrollo de la economía impulsaron al país a tomar acciones, lo que contribuyó a que las telecomunicaciones se convirtieran en la punta de lanza del proceso de reforma que involucró a todo el Estado y la Privatización de ENTEL, desarrollando las actuales leyes

de comunicaciones que sirven para su regulación, principalmente la introducción de Internet como el medio de comunicación en el Siglo XI. [SITTEL, ©2000]

2. Características de SITTEL

a. Independencia

Figura E2: Independencia

Fuente: Elaboración Propia

Del marco regulatorio boliviano se establece que SITTEL tiene un alto grado de independencia, que se traduce en: (Ver Figura E2)

- Una relación equidistante con las firmas reguladas, consumidores y con otros intereses privados.
- Independencia de las autoridades políticas gubernamentales.

SITTEL es elegido por el Presidente de la República de una terna propuesta por el Senado, por un período fijo de cinco años, no pudiendo ser reelegido sino pasado un tiempo igual al que ejerció su mandato. Durante este tiempo no puede ser removido por ninguna autoridad, incluido el Presidente. La destitución sólo es posible en virtud de una sentencia ejecutoriada, por delitos cometidos en el ejercicio de sus funciones.

Las actividades de SITTEL se financian mediante una tasa de regulación que pagan los operadores de telecomunicaciones. Esta tasa se aplica a personas individuales o colectivas, independientemente de la cantidad de concesiones, licencias o registros de que sea titular, hasta un uno por ciento anual de los ingresos brutos de operación del año anterior.

a. Transparencia

b. Rendición de cuentas - Responsabilidad

c. **Grado de Predicibilidad de las Acciones del Cuerpo Regulatorio**

d. Claridad en las Responsabilidades y Papel del Órgano Regulador

ANEXO G

IBNORCA

1. Origen y Evolución de las Normas

A medida que el hombre acrecienta su dominio en el aprovechamiento de lo que ofrece la naturaleza, va creando y mejorando los productos que utiliza, satisfaciendo un mayor numero de necesidades, acondicionándolos, cada ves mas, a especificaciones del material, forma, tamaño, peso, etc., según el uso a que los destine. Y es así que, en la misma medida que se va civilizando, moldea sus actividades según Normas para vestirse, construir sus chozas, cazar, domesticar animales, cultivar la tierra, etc.

En los países industrializados el surgimiento de la producción en serie, marco el principio de la normalización técnica como se conoce hoy día. Inicialmente, el primer piano de la normalización lo ocupaban las tareas de nacionalización y clasificación. La elaboración de normas la ejecutaban particulares y compañías, no era dirigida por instituciones externas (Nacionales o Internacionales).

En las décadas siguientes, la normalización en muchos países industrializados, se fomento con un esfuerzo exhaustivo y principalmente privado de cooperación tecnológica. Las estructuras y los procesos de normalización, fueron iniciados por la industria privada "desde abajo y desde adentro", los conocimientos técnicos necesarios proceden de forma exclusiva del sector privado y el apoyo financiero para la normalización en los países industrializados, esta sustentados en gran medida por la industria privada.

Sin embargo, no hay un país industrializado en el que la normalización este totalmente privatizada, debido a que el Estado debe contribuir día a día con el financiamiento de las organizaciones para normas, y su interés legitimo en la normalización debe estar reforzado en los contratos o acuerdos con la organización nacional de normas, o incorporado en leyes; relacionadas a aspectos tales como:

- Salud
- Seguridad en el trabajo
- Protección al consumidor
- Protección del medio ambiente
- Competencia leal
- Política de Comercio Internacional

En contraste con los países industrializados, la normalización en países en vías de desarrollo, es normalmente un proceso que funciona "desde afuera y desde arriba". Por regla general, las organizaciones nacionales de normas en los países en vías de desarrollo se remontan a las iniciativas de los respectivos poderes coloniales, o se han construido con un considerable apoyo extranjero o internacional con un "Know-How" externo. El lento desarrollo, casi orgánico, de estas instituciones, para ajustarse a los requisitos específicos del país en cuestión, no ha tenido lugar, o si es así, solo de alcance limitado.

La industria local apenas, o nunca, ha estado implicada en el desarrollo y expansión de las estructuras de normalización. La razón principal de esto ha sido la falta de conocimiento de los beneficios económicos de la normalización, lo que ha llevado a un amplio desinterés en las actividades de normalización.

De acuerdo a la Organización Internacional de Normalización ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION) con sede en Ginebra - Suiza: "La normalización es el proceso de formular y aplicar reglas para un enfoque metódico de una actividad especifica, establecida con la cooperación y el consenso de las partes interesadas para conseguir un beneficio a la comunidad y en particular para la promoción de una optima economía integral, teniendo debidamente en cuenta las condiciones funcionales y requisitos de seguridad".

La normalización esta basada en los resultados consolidados de la ciencia, tecnología y experiencia, no determina solo las bases para el desarrollo presente, sino también para el futuro debiendo avanzar a la par del progreso.

2. Beneficios de la Normalización

a) En el campo de la producción:

- Facilita el planeamiento de la producción
- Mejora los procesos de fabricación
- Facilita la producción en serie
- Uniformiza la mano de obra
- Disminuye las existencias almacenadas
- Disminuye costos de adquisición, fabricación, mantenimiento de equipo y embalaje

- Incrementa la producción

b) En el campo de la comercialización y el consume:

- Facilita el acceso a datos técnicos, anteriormente disperses o inciertos
- Facilita la selección del producto mas adecuado a las necesidades
- Agiliza la formulación de pedidos
- Disminuye los precios
- Reduce los plazos de entrega
- Permite la evaluación de la conformidad
- Disminuye los litigios

c) En el campo de la macroeconomía:

- Mejora la producción en cantidad, calidad y regularidad
- Pone orden en las actividades económicas
- Mejora la relación entre la oferta y la demanda
- Permite la estructuración progresiva de un catalogo de productos nacionales
- Promociona las ventas en el mercado internacional
- Acelera el desarrollo socio-económico

3. Norma Técnica

a. Concepto

Una norma técnica es un documento establecido por consenso y aprobado por un organismo autorizado, que proporciona para uso común y repetido reglas directivas o características especiales de los productos, procesos y servicios, a fin de garantizar un orden optimo de un contexto dado.

Contar con una norma técnica se traduce en la necesidad de contar con un instrumento imprescindible para que los productos puedan ingresar a los mercados de consumo nacional e internacional, es decir, la norma crea las condiciones necesarias para el intercambio comercial abierto, colocando a los fabricantes y consumidores en una situación siempre favorable.

Una norma facilita información sobre el producto o servicio utilizado, porque con este documento los productores disponen de los reglamentos nacionales e internacionales para la elaboración, etiquetado, indicación del lugar de origen, conformación, etc.

Las normas deben ser utilizadas de acuerdo a las necesidades tanto de los exportadores como de los importadores, los primeros porque deben conocer los niveles de cumplimiento que se les exige y los segundos porque deben conocer lo que están importando.

Por ultimo una norma procura armonizar las definiciones o conceptos adoptados por el momento por los productores y comercializadores para facilitar el intercambio, proteger la salud, ayuda a la ética de preselección del producto y asegura que se apliquen prácticas comerciales equitativas en la industria y el comercio. [IBNORCA, ©2002]

ANEXO H

Entidades Reguladoras en Firmas y Certificados Digitales en el Mundo

	País	Entidad Reguladora
	Alemania	Regulatory Authority for Telecommunications and Posts
	Australia	Australian Government's strategy for the use of Public Key Infrastructure (PKI) - Gatekeeper
	Austria	Supervisory Authority for Electronic Signatures
	Bélgica	Centre d' Information sur la Signature Electronique
	Brasil	ICP-Brasil - Infra-estrutura de Chaves Públicas Brasileira Instituto Nacional de Tecnologia da Informação Autoridade Certificadora Raiz da ICP
	Canadá	Government of Canada Public Key Infrastructure
	Chile	Entidad Acreditadora de Firma Electrónica
	Colombia	Colombia: Superintendencia de Industria y Comercio
	EEUU	Federal Public Key Infrastructure Steering Committee NIST PKI Program Federal Bridge Certification Authority (FBCA)
	Eslovenia	Government Centre for Informatics
	España	Fábrica Nacional de Moneda y Timbre - Proyecto CERES Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información
	Finlandia	Finnish Communications Regulatory Authority
	Francia	Le site du programme d'action de l'Etat pour la société de l'information Serveur Thématique sur la Sécurité des Systèmes dInformation
	Hong Kong	Electronic Service Delivery Infrastructure
	India	Controller of Certifying Authorities
	Italia	CNIPA:Centro Nazionale per Informatica nella Pubblica Amministrazione
	Luxemburgo	Office Luxembourgeois d'Accreditation et de Surveillance
	Noruega	Norwegian Post and Telecommunication Authority
	Nueva Zelanda	Secure Electronic Environment PKI
	Panamá	Proyecto Firma Digital y Comercio Electrónico (SENACYT)
	Perú	INDECOPI - Acreditación de entidades de certificación
	Reino Unido	The National Technical Authority for Information Authority Government Gateway
	República de Corea	Korea Certification Authority Central
	Singapur	Controller of Certification Authorities
	Suecia	Swedish Board for Accreditation and Conformity Assessment
	Venezuela	Superintendencia de Servicios de Certificación Electrónica

ANEXO I

Sondeo del Mercado de Hardware

Práctica 28. Sondeo de Mercado de Ordenadores Pentium VI integrada

Ubicación	US$*	Bs.
1. J&J – Eloy Salmón # 1579	500.00	4050.00
2. Huyustus # 798	**390.00**	**3159.00**
3. Power Point – C. Socabaya # 388	610.00	4941.00

*Cambio de US$ 1.00 a Bs. 8.10

La Paz, 12 de diciembre de 2012

Señor
Marcelo Palma

Presente.-

REF.: CONTRATO POR LA COMPRA Y ENSAMBLADO DE UNA COMPUTADORA PERSONAL

Estimado Magda:

Mediante la presente deseamos manifestarle nuestra complacencia por ser parte de nuestra distinguida clientela, como también para hacerle llegar el contrato referente a la entrega de su nuevo equipo.

Como se acordó el día sábado 8 de enero, se adjunta el recibo por concepto de la compra, ensamblado, curso de utilización de 2 horas y mantenimiento por un año de una computadora con las siguientes partes:

AMD 2.8 Ghz Pc Chip S/V/R/F

- Tarjeta Madre Pc Chip S/V/R/F Integrada
- Microprocesador AMD de 2.8 Ghz
- Memoria DDR 256 MB de 333 Mhz
- Disco Duro de 80 GB
- FAX MODEM 56 KB
- Tarjeta de Red 10/1000
- Tarjeta de Video ATI de 32 Mb
- Lector de CD – Marca LG 52X
- Quemador de CD – Marca Liteon 52X
- Disquetera 1.44 Mitsumi
- Monitor de 15 Pulgadas

- Case System – Color Azul
- Parlantes System
- Teclado System
- Mouse Óptico System
- Pad Mouse
- Cortapicos
- Protector de Pantalla

Por el valor de $us. 390.00

Por causas inexistencia de partes en el mercado el ensamblo del equipo fue modificado a:

AMD 3.2 Ghz Pc Chip S/V/R/F

- Tarjeta Madre Pc Chip S/V/R/F Integrada
- Microprocesador AMD de 3.2 Ghz
- Memoria DDR 256 MB de 333 Mhz
- Disco Duro de 80 GB
- FAX MODEM 56 KB
- Tarjeta de Red 10/1000
- Tarjeta de Video ATI de 32 Mb
- Lector de CD – Marca LG 52X
- Quemador de CD – Marca Liteon 52X
- Disquetera 1.44 Mitsumi
- Monitor de 15 Pulgadas ESN
- Case System – Color Azul
- Parlantes System
- Teclado System
- Mouse Óptico System
- Pad Mouse
- Cortapicos
- Protector de Pantalla

Por el valor de $us. 450.00

Puntos relevantes en el contrato:

1. **De la garantía:**

    - La garantía empieza desde el primer día de ser entregado el equipo al comprador y termina pasado el tiempo de un año.
    - Mantenimiento de la computadora por el lapso de la garantía, que consta de la reinstalación del Software, mantenimiento del Hardware y cambio de partes del Hardware, previa entrega de las mismas por la empresa o encargado, este será revisado a domicilio durante los 3

primeros meses y después tendrá que ser traído a nuestras oficinas.
- En caso de fallas en el Hardware, se hará una notificación a la empresa SaiTec, la cual hará la revisión correspondiente del equipo siendo posible cambiar alguna parte en caso de falla o defecto únicamente durante los tres meses desde su entrega.

2. Fallas en el Hardware:

- La garantía y cambio de partes por fallas en el Hardware se podrá hacer en un lapso de 3 meses desde la entrega del equipo al comprador, previa revisión correspondiente del equipo por personal de la empresa SaiTec.

3. De la Perdida de la garantía:

- Se colocará un precinto de garantía después de indicar las partes del equipo con el contrato, el cual evitará que cualquier persona ajena a la empresa extraiga o cambie alguna parte del computador.
- **Si el precinto es retirado, descolado o cortado, la garantía de la computadora quedara anulada.**

4. Del Curso de Utilización:

- Dicho curso tendrá que ser reservado con anterioridad y consistirá en el manejo, instalación y configuración Básica de la Computadora y Software a utilizar.

Me despido agradeciendo su preferencia. Reciba usted las seguridades de mi mayor consideración.

Marcelo Palma	**Ing. Elizabeth Ríos**
CLIENTE	**NETBIOS**

ANEXO J

Modelo COCOMO

Bohem platea tres jerarquías de modelos de estimación de software. Los modelos de esta jerarquía son:

- El modelo 1 o básico calcula el esfuerzo y coste en función del tamaño del programa, expresado en LDC (Líneas de Código)
- El modelo 2 o intermedio calcula el esfuerzo en función del tamaño del programa y de un conjunto de "conductores de costes" o "atributos", que incluyen la evaluación subjetiva del producto, del hardware, del personal, de los atributos del proyecto.
- El modelo 3 o avanzado que incorpora las características del modelo intermedio y evalúa el impacto de los conductores de coste en cada fase (análisis, diseño, etc.).

Los modelos de COCOMO están definidos para tres tipos de proyectos de software:

Modo Orgánico: Proyectos de software relativamente pequeño, sencillos en los que trabajan pequeños equipos, con buena experiencia en la aplicación sobre un conjunto de requisitos poco rígidos.

Modo Semiacoplado: Proyectos de software intermedios en tamaño y complejidad.

Modo Empotrado: Proyectos de software que deben ser desarrollados en un conjunto de hardware, software y restricciones operativas muy restringidas.[51]

Obtenido el tipo de modo a continuación se describen los valores constantes que se asignan a cada modo.

Los coeficientes a_b, c_b y los exponentes b_b y d_b se detallan a continuación:

Tabla. Coeficientes del Modelo COCOMO II

Proyecto de Software	a_b	c_b	b_b	d_b
Orgánico	2.40	1.005	2.50	0.38

[51] PRESSMAN Roger S., Ingeniería de Software, quinta edición, Pág. 82, Mc Graw-Hill, México

Semi – Acoplado	3.00	1.120	2.50	0.35
Empotrado	3.60	1.200	2.50	0.32

Fuente: Elaboración Propia

Las ecuaciones del COCOMO II son las siguientes:

$$E = a_b * (KLDC) \exp(b_b) \quad \text{Ec(2)}$$

$$D = c_b * (E) \exp(d_b) \quad \text{Ec(3)}$$

$$\text{Costo de desarrollo de Software} = E * \text{Costo Relativo} \quad \text{Ec(4)}$$

Donde: E = El esfuerzo aplicado en personas/mes

KLDC = Es el número de líneas de código dividido entre 1000

D = Es el tiempo de desarrollo en meses

ANEXO K

Ecuación de Putnam

La ecuación de PUTNAM sirve para hallar el tamaño del Software.

$$L = C_K * K^{\frac{1}{3}} * td^{\frac{4}{3}} \qquad Ec.(1)$$

Donde:

- C_K es una constante (2000, 8000, 11000) dependiendo de las características del sistemas, donde:
  - C_K = 2000, para un entorno pobre de desarrollo de software, si la metodología, documentación y revisiones pobres, modo de ejecución no interactivo.
  - C_K = 8000, para un buen entorno de desarrollo, buena metodología, documentación y buena revisión, modo de ejecución interactivo.
  - C_K = 11000, para entorno excelente, con herramientas y técnicas automatizadas.
- C_K K es el esfuerzo.
- td es el tiempo de desarrollo en años.
- L son las líneas de código.

ANEXO L

Detalle de Recomendaciones

I. FINALIDAD

La aplicación de firmas y certificados digitales acorde a la **NB ISO/IEC 17799** para los **procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones** permite tener un **mayor nivel de confiabilidad que los sistemas actuales** y **conserva la integridad de la información** como también **verifica la autenticidad del origen del mensaje**.

II. OBJETIVO

Contribuir a la seguridad de la Información en SITTEL a través del desarrollo de firmas y certificados digitales a ser evaluados por la ISO/IEC 9126[52], utilizando la NB ISO/IEC 177999 para afianzar la integridad de la información, autenticidad del origen del mensaje y tener un mayor nivel de confiabilidad que los sistemas actuales.

III. CAPACIDAD DE PRODUCCIÓN NORMAL

Producir un CD con el programa tarda, no más de 10 minutos, en 8 horas de trabajo se tendrá 48, en un mes se trendría Cd's 1000.00 y en 10 meses CD's 10000.00, además la pagina web podrá vender a través de una central de E-Commerce.

Venta mínima para cubrir gastos son CD's 5000.00 a un precio de 89.90

IV. COSTO TOTAL

DETALLE		BASE AÑO	AÑO UNO	AÑO DOS	AÑO TRES
1.	**ORIGEN**	**133235.58**	**1034536.56**	**1121322.89**	**1210571.62**
1.1	Saldo de Caja de Ejercicio Anterior	0.00	46536.56	261762.89	351011.62
1.2	Aporte de Capital	133235.58	0.00	0.00	0.00
1.3	Obligaciones con Banco o deudas contraídas por Préstamo	0.00	0.00	0.00	0.00
1.4	Ventas	0.00	859560.00	859560.00	859560.00
2	**USOS**	**86699.02**	**772773.67**	**770311.27**	**767851.87**
2.1	Equipos	9857.70	0.00	0.00	0.00

[52] El producto resultante será evaluado contra los parámetros indicados por el estándar ISO/IEC 9126 (funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y transportabilidad) – **Ver Anexo D**.

2.2	Muebles	10270.80	0.00	0.00	0.00
2.3	Otros Activos o Inversiones	0.00	0.00	0.00	0.00
2.4	Inversión Diferida	51180.52	0.00	0.00	0.00
2.5	Alquileres Anticipados o Anticréticos	15390.00	61560.00	59097.60	56635.20
2.6	Costo Fijo con Factura	0.00	0.00	0.00	0.00
2.7	Costo Fijo sin Factura	0.00	418121.32	418121.32	418121.32
2.8	Casto Variable con Factura	0.00	19965.20	19965.20	19965.20
2.9	Casto Variable sin Factura	0.00	0.00	0.00	0.00
2.10	Impuesto de Valor Agregado	0.00	131423.30	131423.30	131423.30
2.11	Impuesto a Transacciones	0.00	29640.00	29640.00	29640.00
2.12	Impuestos a Utilidad	0.00	112063.85	112063.85	112063.85
2.13	Otros Egresos	0.00	0.00	0.00	0.00
3	**Saldo de la Caja de Ejercicio**	**46536.56**	**261762.89**	**351011.62**	**442719.75**

V. COSTO UNITARIO

$$CU = CMF + CMV = 44.00 + 3.04 = 47.04$$

Cada unidad del producto a desarrollarse tiene un costo de Bs. 47.04

VI. UMBRAL DE RENTABILIDAD

$$UR \Rightarrow Y = CT$$

$$\text{Pr}ecio\ x\ \#\ de\ Contratos = CF + CV$$

$$CV = CMV\ x\ \#\ de\ Contratos$$

$$\text{Pr}ecio * N^{\circ}\ de\ Contratos = CF + CMV * N^{\circ}\ de\ Contratos$$

$$\text{Pr}ecion * N^{\circ}\ de\ Contratos - CMV * N^{\circ}\ de\ Contratos = CF$$

$$N^{\circ}\ de\ Contratos\ (\text{Pr}ecio - CMV) = CF$$

$$N^{\circ}\ de\ Contratos = \frac{CF}{\text{Pr}ecio - CMV}$$

$$N^{\circ}\ de\ Contratos = \frac{469633.23}{98.80 - 4.70} = 4990.80$$

Con vender 4991 unidades, menos de la mitad calculada (10000 unidades) cobramos el costo por demás.

VII. TOTAL DE INVERSIÓN

Cod.	Detalle	Ref.	Importe
1	**Inversión Fija:**	**(1)**	**81688.50**
1.1	Inmueble	(1.1)	61560.00
1.2	Equipos	(1.2)	9857.70
1.3	Maquinarias	(1.3)	0.00
1.4	Herramientas	(1.4)	0.00
1.5	Muebles	(1.5)	10270.80
1.6	Vehículos	(1.6)	0.00
1.7	Otros	(1.7)	0.00
2	**Inversión Diferida:**	**(2)**	**51180.52**
2.1	Gasto de Organización	(2.1)	3435.00
2.2	Gasto de Ejecución del Proyecto	(2.2)	47565.52
2.3	Gasto de Investigación del Mercado	(2.3)	180.00
2.4	Otros	(2.4)	0.00
3	**Capital de Explotación:**	**(3)**	**66705.91**
3.1	Fondo Anticrético o fondo de alquiles anticipados	(3.1)	15390.00
3.2	Fondo lanzamiento de producto	(3.2)	1848.50
3.3	Fondo de inventario, suministros o elementos	(3.3)	21750.00
3.4	Otros fondos	(3.4)	0.00
3.5	Caja	(3.5)	27717.41
		TOTAL	**199574.93**

VIII. TIR ECONÓMICO

TIR = 11.444408

TIR = 1144.4408 % > 10.00 %, por lo tanto el proyecto es factible

IX. TIR FINANCIERO

TIR = 689.4843

X. APALANCAMIENTO

$$Apalancamiento = TIR\,Financiero - TIR\,Económico$$

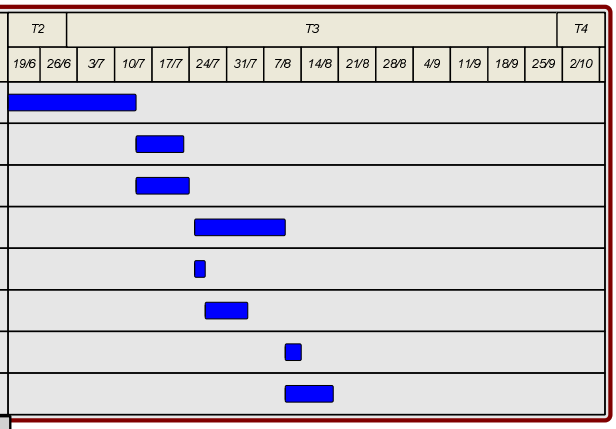
$$Apalancamiento = 689.4843 - 1144.4408$$

$$Apalancamiento = -454.9565$$

XI. TIEMPO DE EJECUCIÓN DEL PROYECTO

TIEMPO ÓPTIMO

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	A	20/06/2005	13/07/2005	21d
2	B	14/07/2005	22/07/2005	8d
3	C	14/07/2005	23/07/2005	9d
4	D	25/07/2005	10/08/2005	15d
5	E	25/07/2005	26/07/2005	2d
6	F	27/07/2005	03/08/2005	7d
7	G	11/08/2005	13/08/2005	3d
8	H	11/08/2005	19/08/2005	8d
			TOTAL	**53**



TIEMPO PESIMISTA

ANEXO M

Tecnología Cliente-Servidor con Asp

Introducción

Desde hace algún tiempo, Microsoft está llevando adelante una estrategia para construir una nueva tecnología tendiente a crear aplicaciones web distribuidas y que aprovechen al máximo las posibilidades que ofrece Internet. Esta tecnología, que lleva el nombre de .NET, y que incluye un nuevo lenguaje denominado C#, una nueva versión de Visual Basic, con el nombre de Visual Basic.Net y otra serie de tecnologías, entre las que se encuentra: ASP.NET, que viene a reemplazar a las Active Server Pages (ASP), logrando el desarrollo de aplicaciones web más dinámicas, con un código más claro y limpio, por ende **reusable**,multiplataforma y definitivamente más simple, ya que el entorno ASP.NET permite la creación automática de alguna de las tarea más comunes para un creador web, cómo los formularios o la validación de los datos.

El .NET Framework

Los Ingenieros de Microsoft se han preocupado por brindarle a los desarrolladores un entorno de desarrollo que le permita disponer de una gran serie de herramientas y tecnologías tendientes a facilitar el desarrollo de aplicaciones web potentes y distribuidas, creando un ambiente multiplataforma, altamente deseado por todos los desarrolladores.

El .NET Framework es un marco de trabajo multilenguaje, que le permite al desarrollador crear Aplicaciones y Servicios Web con las herramientas básicas para escribir el código.

De forma simple, el .NET Framework está formado por el **Common Languaje Runtime** o **CLR**, la **Base Class Library**, que funciona como una gran librería de clases unificada, que contiene todas las clases que funcionan dentro del entorno .NET y finalmente la nueva versión de ASP, denominada ASP.NET.

De ASP a ASP+

A pesar de ser una tecnología relativamente nueva, las Active Server Pages han logrado crear un estándar en cuanto a la creación de páginas web dinámicas. Antes de la aparición de las páginas ASP, los desarrolladores debían utilizar la tecnología CGI para comunicarse con el servidor. Si bien CGI ha sido implementado por una gran cantidad de desarrolladores, la utilización de páginas ASP, resulta más sencillo y brinda un mayor rendimiento y seguridad.

Sin embargo, Microsoft ha pasado los últimos 3 años, desarrollando la nueva versión de ASP, que venga a solucionar pricipalemnte los siguientes problemas de las páginas ASP:

Mantenimiento

Las aplicaciones Cliente/Servidor en ASP son difíciles de mantener. El código ASP mezclado con la interfaz de usuario hace que muchas veces se pierda demasiado tiempo actualizando toda la aplicación, no pudiendo trabajar simplemente con el núcleo del código. ASP+ viene a solucionar este déficit, al permitir separar interfaz de código.

Código...Código..Código...

La mayoría de todo lo que funciona en una página web debe ser creado por el desarrollador. Cada formulario que ingresa datos a una base de datos conlleva varias líneas de código, obligando al desarrollador a generar desde cero cada aplicación. El rico entorno de .NET Framework, brinda una extensa cantidad de controles predefinidos, que permiten crear aplicaciones potentes, simplemente escribiendo una pocas líneas de código.

Limitación de Lenguajes

ASP.NET incorpora soporte nativo para C#, Visual Basic y JScript. Logrando así dejar atrás las limitaciones ASP que sólo permitía código en VBScript y JScript.

Principales características de ASP.NET

Eficiencia

Desde el principio, uno de los objetivos más importantes del diseño de .NET ha sido su gran rendimiento y nivelación. Para que .NET tenga éxito, las empresas deben estar capacitadas para migrar sus aplicaciones y no sufrir de un rendimiento deficiente debido a la forma en que CLR ejecuta el código. Para asegurarse un óptimo rendimiento, el CLR compila, en algún punto, todos los códigos de aplicaciones en códigos naturales de máquina.

Esta conversión puede hacerse, o bien en el momento en que se ejecuta la aplicación (método por método), o cuando se instala la aplicación por primera vez. El proceso de compilación hará uso automáticamente de todas las características del microprocesador, disponibles en diferentes plataformas, algo que las aplicaciones tradicionales de Windows nunca podrían hacer, a menos que usted cargase distintos binarios para distintas plataformas.

Soporte de Lenguajes

Esta es una de las novedades más importantes que vienen de la mano de ASP.NET. La posibilidad de escribir código en diferentes lenguajes es un alivio para los desarrolladores que en numerosas ocasiones, veían acotadas sus aplicaciones web, al estar obligados a trabajar con VBScript o JScript. ASP.NET soporta la programación en lenguajes potentes cómo, VisualBasic.Net (VB) y C#, el nuevo lenguaje creado por Microsoft con la intención de aprovechar la potencia del C++ y combinarlo con las facilidades que brinda a la programación en Internet un lenguaje como Java.

Contenido y Código, por separado

Muchos desarrolladores de sitios web han tenido que lidiar con el inconveniente de tener que crear la interfaz de usuario y el código ASP todo junto. Esta mezcla de imágenes, botones y tablas en código HTML con pedazos de código en VBScript o Jscript llegaba a ser algo muy molesto para el desarrollador. ASP.NET viene a solucionar este problema, utilizando un criterio similar al que utiliza Visual Basic, es decir, separar la interfaz de usuario con el código.

Compatibilidad con Navegadores ASP.NET permite crear un página web que funcionará correctamente en todos los navegadores. Esta mejora está dada especialmente por los controles de servidor incluidos en ASP.NET. Cuando una control es procesado, este automáticamente chequea el tipo de navegador que lo está ejecutando, generando una página adecuada para ese navegador.

Código Compilado

ASP.NET ya no interpreta el código como la hace la versión anterior de ASP. Dentro del entorno NGWS (New Generation Windows Services) el código es compilado **just-in-time**, logrando un enorme aumento en el rendimiento, a través de soporte nativo y servicios de caché. Controles de Servidor Uno de los aspectos más importantes dentro del .NET Framework es su librería de clases.

Esta librería es común en toda la plataforma .NET, lo que le brinda al programador una herramienta ideal para crear aplicaciones multiplataforma, con un considerable ahorro de líneas de código. Los controles de servidor están divididos en dos categorías: Controles Web y Controles HTML.

Posiblemente sean los Controles Web, lo que atractivos para el desarrollador, ya que permiten crear automáticamente controles que realicen tareas importantes en el servidor

como validar la entrada de formularios, verificar las capacidades de los navegadores o implementar un sistema de banners rotativos.

Los nuevos Controles Web Forms

ASP.NET adopta el modo de Visual Basic a la hora de utilizar controles. Esto permite separar el código de la interfaz del usuario de forma sencilla y clara. En este pequeño ejemplo, se ve la utilización de la sentencia **runat="server**" que le indica al servidor ASP.NET que debe procesar el control de servidor, que es en este caso es un Botón.

```
<html>
<script language="VB" runat="server">
Public Sub btn_Click(Sender As Object, E As EventArgs)
 Response.Write(“Su Nombre es: “ & Name.Text)
 End Sub

</script> <body> <form method="post" runat="server">
 Name: <asp:Button text="OK" OnClick="btn_Click" runat="server">
</form>
</body>
</html>
```

El atributo Text se utiliza, como sucede en Visual Basic, para establecer el texto que se mostrará en el botón. Esto es consistente con los otros controles.

El atributo OnClick finalmente identifica el evento que se ejecutará cuando se haga clic en el botón. Debido a que es un control del servidor, este procedimiento se ejecuta en el servidor.

Tipos de Controles

Controles del Servidor HTML, que son los equivalentes del servidor de los elementos HTML.

Controles de Formulario Web, que planifican aproximadamente elementos HTML individuales.

Controles de Lista, que planifican grupos de elementos de HTML, que producen grillas o un diseño similar.

Controles Ricos, que producen ricos contenidos y encapsulan funcionalidad compleja, y producirá HTML puro o HTML y script. Un buen ejemplo de esto es el control Calendario, que provee al usuario un calendario de una sola línea de código.

Controles de Validación, que son no-visibles, pero permiten el fácil uso de la validación del formulario por parte del servidor y del cliente.

Controles Móviles, que producen HTML o WML dependiendo del dispositivo con el que se accede a la página.

Bibliografía

http://www.gamarod.com.ar/articulos/introduccion_a_aspnet.asp

ANEXO N

ANTEPROYECTO DE LEY

ANTEPROYECTO

LEY DE COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS

Versión elaborada por el Ministerio de Servicios y Obras Públicas, Superintendencia de Telecomunicaciones, Superintendencia de Bancos y Entidades Financieras, Banco Central de Bolivia y la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

(Trascrito por el Viceministerio de Justicia, del ejemplar entregado por el Dr. Diego Arce representante de SITTEL el 1o de diciembre de 2004)

ANTEPROYECTO

LEY SOBRE COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS

ANTEPROYECTO

LEY SOBRE COMUNICACIÓN ELECTRÓNICA DE DATOS, CONTRATACIÓN ELECTRÓNICA Y FIRMAS ELECTRÓNICAS

TÍTULO I DISPOSICIONES GENERALES

CAPITULO I. OBJETO Y ÁMBITO DE APLICACIÓN.

Artículo 1 (Objeto)

II. La presente Ley tiene por objeto regular la comunicación electrónica de datos, otorgando y reconociendo eficacia y valor jurídico a: los mensajes de datos, documentos electrónicos; la firma electrónica; la contratación electrónica. Así como a los diversos actos atribuibles a personas naturales o jurídicas, publicas o privadas realizadas por medios electrónicos.

III. Asimismo regula los servicios de certificación de información, la prestación de otros servicios electrónicos a través de redes de información, incluida la contratación electrónica así como la protección a los usuarios de estos sistemas.

Articulo 2 (Ámbito de aplicación)

I. Los principios y normas establecidas en esta Ley se aplicarán a los actos jurídicos que produzcan efectos de datos y que, den origen a documentos electrónicos, o a contratos, operaciones, servicios u otro tipo de actos. La presente Ley será además aplicable a todo tipo de información en forma de mensajes de datos y documentos electrónicos, salvo que se encuentre prohibido expresamente por Ley.

Las disposiciones contenidas en esta ley no alteran, sino complementan las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos que se efectúen por medios electrónicos; así como tampoco altera las normas relativas al tipo de instrumentos en que los actos jurídicos deben constar.

2.3.9. Firmas Electrónicas y Certificados Digitales.

2.3.10. Capítulo I. Firma Electrónica

Artículo 35. (Definiciones)

I. La firma electrónica es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un mensaje de datos, utilizada como método de identificación del firmante, con la intención de vincularse con el contenido de dicho documento.

II. La firma electrónica avanzada o firma digital es la firma electrónica que cumple con los siguientes requisitos.

a) Estar vinculada exclusivamente a su titular

b) Permite verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos de comprobación establecidos por la Ley y los reglamentos,

c) Que el método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual generado y/o comunicado, y;

d) Que los datos de creación de la firma estén, al momento de la firma bajo el control exclusivo del signatario.

e) Que en caso de que uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, sea posible detectar cualquier alteración de esa información hecha después del momento de la firma.

III. Los procedimientos de firma y verificación a ser utilizados para lates fines serán los determinados por reglamento en consonancia con estándares tecnológicos internacionales vigentes.

Artículo 36 (Efectos)

I. La firma electrónica avanzada tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos.

II. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica avanzada en relación a los datos a los que esta asociada por el mero hecho de presentarse en forma electrónica, debiendo valorarse de acuerdo a los criterios de la sana critica.

III. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre si, se tendrá en cuenta lo estipulado entre ellas.

Artículo 37 (Presunciones)

La firma electrónica avanzada que cumpla con los recaudos y exigencias que esta Ley y su reglamentación disponen, genera las siguientes presunciones, salvo prueba en contrario:

a) Que toda firma electrónica avanzada pertenece al titular de la misma

b) Que el documento electrónico no ha sido modificado desde el momento de su firma electrónica avanzada, si el resultado del procedimiento de verificación así lo indica.

Artículo 38 (Obligaciones del titular)

El titular de la firma electrónica deberá cumplir con las obligaciones derivadas del uso de la firma electrónica, actuando con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada, debiendo cumplir las obligaciones establecidas en la presente Ley y sus reglamentos.

Artículo 39 (Extinción)

I. La facultad de firmar electrónicamente mediante el empleo de determinados dispositivos o datos de creación de firma se extinguirá por las causales establecidas en el reglamento.

II. La extinción de la facultad mencionada en el párrafo anterior no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Artículo 40 (Administraciones Públicas)

I.- Esta ley se aplicará al uso de la firma electrónica en el seno de las Entidades de la Administración Pública, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre si o con los particulares.

II.- Entidades de la Administración Pública, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en sus procedimientos.

III.- La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a al seguridad pública o a al defensa nacional se regirá por normativa especifica.

2.3.11. Capítulo II. Certificados Electrónicos

2.3.11.1. Sección 1. Disposiciones Generales

Artículo 41 (Plazo de validez y extinción)

I.- Salvo acuerdo contractual, el plazo de validez de los certificados electrónicos será el establecido en el reglamento respectivo.

II. Las causales y efectos de la extinción, suspensión temporal y revocatoria de los certificados de firma electrónica se determinarán en el reglamento respectivo.

Artículo 42 (Certificados emitidos por entidades extranjeras)

I.- Los certificados electrónicos emitidos por entidades de certificación extranjera, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el territorio nacional de acuerdo a reglamento.

II. Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en Bolivia se someterán a lo previsto en esta Ley y su reglamento.

Artículo 43 (Libre convenio)

No obstante lo dispuesto en este Titulo, las partes involucradas en el intercambio electrónico de datos podrán convenir sus propios estándares y formatos para tal efecto,

los que serán válidos para todos los efectos legales a que haya lugar entre ellas exclusivamente.

Artículo 44 (Armonización)

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

2.3.11.2. Sección 2. Entidades de Certificación

Artículo 45 (Definición)

Son Entidades de Certificación, las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con a firma electrónica, debiendo ser previamente autorizadas por la Superintendencia de Telecomunicaciones, según lo dispuesto en esta Ley y el reglamento correspondiente.

Artículo 46 (Funciones)

I. Las entidades de certificación, de acuerdo a la presente Ley y sus reglamentos, podrán restar los servicios siguientes:

a) Emitir, suspender o revocar certificados en relación con las firmas electrónicas de personas físicas y jurídicas;

b) Prestar cualquier otro servicio que se les asigne mediante reglamento u otros servicios que no estén expresamente prohibidos por normas pertinentes.

II. Las entidades de certificación podrán prestar servicios de sellado de tiempo. Este servicio deberá, ser acreditado técnicamente por la Superintendencia de Telecomunicaciones.

Artículo 47 (Obligaciones)

Son obligaciones de las entidades de certificación:

a) Encontrarse legalmente constituidas y estar autorizadas por la Superintendencia de Telecomunicaciones.

b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios.

c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio.

d) Cumplir las demás obligaciones establecidas en la presente Ley y sus reglamentos.

Artículo 48 (Responsabilidades)

I. Las entidades de certificación serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley y sus reglamentos o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley. Serán también responsables por el uso indebido de los certificados electrónicos que emitan, cuando éstos no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación.

II. A los efectos de este artículo los contratos que suscriba una Entidad de Certificación con los usuarios deberán incluir una cláusula de responsabilidad.

III. Cuando la garantía constituida por las entidades de certificación no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con todo su patrimonio.

Artículo 49 (Cesación de actividades)

La entidad de certificación, deberán notificar a la Superintendencia de Telecomunicaciones por lo menos con noventa días de anticipación la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

2.3.11.3. Sección 3. Regulación de las Entidades de Certificación

Artículo 50 (Superintendencia de Telecomunicaciones)

Para efectos de esta Ley, la Superintendencia de Telecomunicaciones, será el organismo encargado de la regulación, fiscalización y control de las entidades de certificación, de acuerdo a las facultades y atribuciones establecidas en el reglamento respectivo.

Artículo 51 (Autoridad normalizadora)

La Superintendencia de Telecomunicaciones actuará como autoridad normalizadota competente y podrá adaptar, reconocer y aprobar los estándares, formatos, instrucciones y códigos calificadores para los documentos electrónicos destinados al intercambio electrónico de datos (EDI), de conformidad con las normas que rigen a dicho organismo, de manera que sean uniformes y compatibles entre sí.

Artículo 52 (Tasa de regulación)

Las actividades regulatorias de la Superintendencia de Telecomunicaciones establecidas en la presente Ley y sus reglamentos, serán cubiertas mediante tasas de regulación a ser pagadas por las entidades de certificación. Los montos y formas de pago de estas serán establecidas mediante reglamento, no pudiendo en ningún caso fijarse una tasa superior al uno por ciento (1%) de sus ingresos brutos de operación del año anterior. [ADSIB, ©2004]

ANEXO O

Controles Criptográficos

Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información. Deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

Política de utilización de controles criptográficos.

Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que tipo de control debe aplicarse y conque propósito, y los procesos de la empresa.

Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, y para evitar un uso inadecuado o incorrecto. Al desarrollar una política se debe considerar lo siguiente:

f) el enfoque gerencial respecto del uso de controles criptográficos en toda la organización, con inclusión de los principios generales según los cuales debe protegerse la información de la empresa;
g) el enfoque respecto de la administración de claves, con inclusión de los métodos para administrar la recuperación de la información cifrada en caso de perdida, compromiso o daño de las claves;
h) funciones y responsabilidades, por ej. quien es responsable de:
    3) la implementación de la política;
    4) la administración de las claves;
i) como se determinara el nivel apropiado de protección criptográfica;
j) los estándares que han de adoptarse para la eficaz implementación en toda la organización (que solución se aplica para cada uno de los procesos de negocio).

Cifrado

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se debe tener en cuenta para la protección de información sensible o critica.

Mediante una evaluación de riesgos se debe identificar el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la política de la organización en materia criptográfica, se deben considerar las normas y restricciones nacionales que podrían aplicarse al uso de técnicas criptográficas, en diferentes partes del mundo, y las cuestiones relativas al flujo de información cifrada a través de las fronteras. Asimismo, se deben considerar los controles aplicables a la exportación e importación de tecnología criptográfica (ver también 12.1.6).

Se debe procurar asesoramiento especializado para identificar el nivel apropiado de protección, a fin de seleccionar productos adecuados que suministren la protección requerida, y la implementación de un sistema seguro de administración de claves (ver también 10.3.5). Asimismo,

podría resultar necesario obtener asesoramiento jurídico con respecto a las leyes y normas que podrían aplicarse al uso del cifrado que intenta realizar la organización.

Firma digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Por ejemplo, puede utilizarse en comercio electrónico donde existe la necesidad de verificar quien firma un documento electrónico y comprobar si el contenido del documento firmado ha sido modificado.

Las firmas digitales pueden aplicarse a cualquier tipo de documento que se procese electrónicamente, por ej., pueden utilizarse para firmar pagos, transferencias de fondos, contratos y convenios electrónicos. Pueden implementarse utilizando una técnica criptográfica sobre la base de un par de claves relacionadas de manera única, donde una clave se utiliza para crear una firma (la clave privada) y la otra, para verificarla (la clave publica).

Se den tomar recaudos para proteger la confidencialidad de la clave privada.

Esta clave debe mantenerse en secreto dado que una persona que tenga acceso a esta clave puede firmar documentos, por ej.: pagos y contratos, falsificando así la firma del propietario de la clave.

Asimismo, es importante proteger la integridad de la clave publica. Esta protección se provee mediante el uso de un certificado de clave publica (ver 10.3.5).

Es necesario considerar el tipo y la calidad del algoritmo de firma utilizado y la longitud de las claves a utilizar. Las claves criptográficas aplicadas a firmas digitales deben ser distintas de las que se utilizan para el cifrado (ver 10.3.2).

Al utilizar firmas digitales, se debe considerar la legislación pertinente que describa las condiciones bajo las cuales una firma digital es legalmente vinculante. Por ejemplo, en el caso del comercio electrónico es importante conocer la situación jurídica de las firmas digitales. Podría ser necesario establecer contratos de cumplimiento obligatorio u otros acuerdos para respaldar el uso de las mismas, cuando el marco legal es inadecuado. Se debe obtener asesoramiento legal con respecto a las leyes y normas que podrían aplicarse al uso de firmas digitales que pretende realizar la organización.

Servicios de No Repudio

Los servicios de no repudio deben utilizarse cuando es necesario resolver disputas acerca de la ocurrencia o no ocurrencia de un evento o acción, por ej. una disputa que involucre el uso de una firma digital en un contrato o pago electrónico. Pueden ayudar a sentar evidencia para probar que un evento o acción determinados han tenido lugar, por ej. cuando se objeta haber enviado una instrucción firmada digitalmente a través del correo electrónico. Estos servicios están basados en el uso de técnicas de encriptación y firma digital (ver también 10,3,2 y 10.3.3).

Administración de claves

PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

La administración de claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. Cualquier compromiso o pérdida de claves criptográficas puede conducir a un compromiso de la confidencialidad, autenticidad y/o integridad de la información. Se debe implementar un sistema de administración para respaldar el uso por parte de la organización, de los dos tipos de técnicas criptográficas, los cuales son:

a) técnicas de clave secreta, cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla. Esta clave tiene que mantenerse en secreto dado que una persona que tenga acceso a la misma podrá descifrar toda la información cifrada con dicha clave, o introducir información no autorizada;
b) técnicas de clave publica, cuando cada usuario tiene un par de claves: una clave publica (que puede ser revelada a cualquier persona) y una clave privada (que debe mantenerse en secreto). Las técnicas de clave publica pueden utilizarse para el cifrado (ver 10.3.2) y para generar firmas digitales (ver 10.3.3).

Todas las claves deben ser protegidas contra modificación y destrucción, y las claves secretas y privadas necesitan protección contra divulgación no autorizada.
Las técnicas criptográficas también pueden aplicarse con este propósito. Se debe proveer de protección física al equipamiento utilizado para generar, almacenar y archivar claves.

Normas, procedimientos y métodos

Un sistema de administración de claves debe estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

i) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;
j) generar y obtener certificados de clave publica;
k) distribuir claves a los usuarios que corresponda, incluyendo como deben activarse las claves cuando se reciben;
l) almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados;
m) cambiar o actualizar claves incluyendo reglas sobre cuando y como deben cambiarse las claves;
n) ocuparse de las claves comprometidas;
o) revocar claves incluyendo como deben retirarse o desactivarse las mismas, por ej. cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deben archivarse);
p) recuperar claves perdidas o alteradas como parte de la administración de la continuidad del negocio, por ej. la recuperación de la información cifrada;
q) archivar claves, por ej. , para la información archivada o resguardada;
r) destruir claves;
s) registrar (logging) y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves deben tener fechas de entrada en vigencia y de fin de vigencia, definidas de manera que solo puedan ser utilizadas por un periodo limitado de tiempo. Este periodo debe definirse según el riesgo percibido y las circunstancias bajo las cuales se aplica el control criptográfico.

Podría resultar necesario considerar procedimientos para administrar requerimientos legales de acceso a claves criptográficas, por ej. puede resultar necesario poner a disposición la información cifrada en una forma clara, como evidencia en un caso judicial.

Además de la administración segura de las claves secretas y privadas, también debe tenerse en cuenta la protección de las claves publicas. Existe la amenaza de que una persona falsifique una firma digital reemplazando la clave publica de un usuario con su propia clave. Este problema es abordado mediante el uso de un certificado de clave publica. Estos certificados deben generarse en una forma que vincule de manera única la información relativa al propietario del par de claves publica/privada con la clave publica. En consecuencia es importante que el proceso de administración que genera estos certificados sea confiable. Normalmente, este proceso es llevado a cabo por una autoridad de certificación, la cual debe residir en una organización reconocida, con adecuados controles y procedimientos implementados, para ofrecer el nivel de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicios o contratos con proveedores externos de servicios criptográficos, por ej. con una autoridad de certificación, deben comprender los tópicos de responsabilidad legal, confiabilidad del servicio y tiempos de respuesta para la prestación de los mismos (ver 4.2.2).

ANEXO P

CUESTIONARIO CON LAS RESPUESTAS CORRECTAS PARA LA AUDITORIA DE SISTEMA EN AL SUPERINTENDENCIA DE TELECOMUNICACIONES

Tabla: Cuestionario con Respuestas Correctas

COD	Pregunta	Respuesta
SP1	¿SITTEL tiene un plan de contingencias?	Sí
SP2	¿Quién es el encargado de actualizar el plan de contingencia?	Analista de Sistema
SP3	¿Cada cuanto se brinda a los empleados un curso de seguridad o actualización de la misma?	Un tiempo no mayor a 6 meses
SP4	¿Su documentación de Seguridad de Sistemas prohíbe la utilización de software malicioso y virus?	Sí
OS1	¿Tienen un responsable en Seguridad de la Información?	Sí
OS2	¿Quién es el responsable en Seguridad de la Información?	Analista de Sistema i
OS3	¿Tuvo incidentes en seguridad de la Información en SITTEL?	No
OS4	¿Puede mencionar algún incidente reciente?	Ninguno
OS5	¿Quién aprueba las principales iniciativas para incrementar la seguridad de la información?	Jefe del Dpto. de Sistemas
CCA1	¿Se clasifico la información por prioridades, necesidades y el grado de protección?	Sí
CCA2	¿Si la respuesta CCA1 es positiva, donde esta descrita la clasificación?	En el plan de contingencias
CCA3	¿Quién es el responsable de publicar información por medios escritos y por su página Web?	Actualizador de la Página Web
CCA4	¿Se tiene procedimientos para el manejo adecuado de la información?	Sí
CCA5	¿Qué procedimiento se maneja para el envió de información por correo electrónico?	Encriptado de la información y Log para el respaldo del envió
SP1	Los empleados de SITTEL reciben alguna capacitación respecto a las amenazas e incumbencias en materia de seguridad de la información.	Si
SP2	¿Qué responsabilidades legales se enseñan a los empleados?	Costo de perdida de la información y protección de Recursos Tecnológicos
SP3	En caso de incidentes con la seguridad de la información, cual es el procedimiento formal de comunicación	Jefe del Dpto. de Sistemas
SP4	¿Existe procedimientos de feedback para garantizar la notificación de los resultados en incidentes con los empleados?	Si
SP5	¿Se registraron los incidentes en algún documento?	En una base de datos
SFA1	¿Se tiene políticas de escritorios y pantallas	Si

	limpias?	
SFA2	¿Existe procedimientos para el manejo de información sensible o confidencial?	Si
SFA3	¿Las terminales (PC, impresoras y otros) son controladas por cerraduras de seguridad cuando no están en uso?	Si
SFA4	¿Existe procedimientos para el ingreso y salida de equipos?	Si
SFA5	¿Dónde se encuentran los procedimientos de retiro de bienes para empleados de SITTEL?	En el plan de contingencias y Base de datos
GCO1	¿Se tiene documentación sobre tipo de cuentas de usuario y cuentas de usuarios de los empleados de SITTEL?	Si
GCO2	¿Quién esta encargado de instalar y desinstalar software en las máquinas de SITTEL?	Analista de Red
GCO3	¿Se tienen cerrados los puertos de transferencia de archivos con redes externas?	Si
CGO4	¿Qué medios de almacenamiento masivo son utilizados en SITTEL?	Discos Magnéticos
CGO5	¿Quién es el encargado de manejar los medios de almacenamiento masivo en SITTEL?	Analista de Sistemas
CGO6	¿Existe procedimientos de eliminación de medios informáticos?	Si
CGO7	¿El ambiente donde es almacenado los medios de información concuerda con las especificaciones de los fabricantes o proveedores?	Si
CGO8	¿Se utiliza log's de auditoria en SITTEL?	Si
CGO9	¿La información que es transmitida por que sistema de encriptación es protegida?	RSA y PGP
CGO10	¿Qué nivel de confianza recíproca recibe el usuario y SITTEL con respecto a la identidad alegada por cada uno de ellos?	Autenticidad por algún sistema de seguridad como ser certificados digitales personales
CGO11	¿Existe control de acceso de usuarios remotos a las cuentas de correo electrónico?	Si
CGO12	¿Se hace uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos?	Si
CA1	¿Cuándo se crea un nuevo usuario, se notifica al usuario que debe mantener su contraseña en secreto?	Si
CA2	¿Cada cuanto tiempo el sistema pide actualizar la contraseña?	Mensualmente
CA3	¿Qué características tiene la contraseña de ingreso a una computadora personal en SITTEL?	Mínimo 6 letras Actualizable mensualmente
CA4	¿En caso de máquinas o bases de datos compartidas, que precauciones se toman?	Password
CA5	¿SITTEL que medios de seguridad física tiene en sus instalaciones?	Identificación por Tarjetas Magnéticas Restricción a sectores por sistemas de seguridad física

CA6	¿Existe documentación respecto a la sensibilidad de los sistemas de aplicación?	Si
CA7	¿Cuándo una aplicación sensible a ejecutarse en un ambiente compartido, que procedimiento de seguridad se aplica?	Passowrd
CA8	¿Quién otorga privilegios a los usuarios para el acceso a las bases de datos compartidas en SITTEL?	Analista de Sistemas
DMS1	¿Existe procedimientos para el diseño y desarrollo de Sistemas?	Si
DMS2	¿Qué sistemas de validación de datos de entrada se manejan en SITTEL?	Control de calidad realizado por el Dpto. de Sistemas
DMS3	¿Qué sistemas y técnicas criptográficas son utilizadas para proteger la información que se considera en estado de riesgo y para la cual otros sistemas no suministran una adecuada protección?	RSA y PGP
DMS4	¿Existe políticas sobre el uso de controles criptográficos para la protección de la información de SITTEL?	Si
DMS5	¿Cómo determino usted el nivel apropiado de protección criptográfico?	Por medio de aplicaciones de seguridad
DMS6	¿Qué normas de seguridad implemento para el proceso del negocio de SITTEL?	En el plan de contingencias
DMS7	¿Qué sistemas utiliza para asegurar la autenticidad e integridad de la información?	Firmas digitales, autentificación de usuarios, etc.
DMS8	¿Qué recaudos se toman para proteger las claves de los usuarios en SITTEL?	Imposibilidad de ingreso a la base de datos por password
DMS9	¿Existe en SITTEL políticas de No Repudio?	Si
DMS10	¿Qué procedimiento de control de acceso a los sistemas de aplicación en operación se tiene?	Respaldo de operaciones y acciones
DMS11	¿Existe procedimientos para la instalación de un servidor de datos en SITTEL?	Si
GCN1	¿Se tiene un plan de Gestión de Continuidad de Negocios?	Si
GCN2	¿Quién es el encargado de actualizar el plan de Continuidad de Negocios?	Jefe de Dpto. de Sistemas y el Analista de Sistemas
CGN3	¿Se tiene estimado la perdida económica por una interrupción por fallas de equipos, inundaciones e incendios en SITTEL?	Si
CG4	¿Se probo los planes de Continuidad de Negocios?	Si
C1	¿Se hicieron auditorias de sistemas?	Si, internas por TIC's
C2	¿SITTEL tiene un auditor interno?	Si
C3	¿Quién es el auditor de sistemas en el Dpto. de TIC?	Analista de Sistemas

Fuente: Elaboración Propia

GLOSARIO

Administrador (SYSOP, ROOT): Persona que se encarga del mantenimiento de un sistema informático, generalmente tienen control total sobre el sistema.

BackDoor: Puerta trasera, mecanismo en el software que permite entrar evitando el método normal.

BackOffice: Paquete de software para Windows NT que provee conectividad y servicios de Internet.

Bombas Lógicas: Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruir o modificara la información, o provocara el cuelgue del sistema.

Boeing: Uso de aparatos electrónicos o eléctricos (Boxes) para hacer phreacking.

BUG: (AGUJERO, HOLE) - Defecto del software que permite a los hackers introducirse en ordenadores ajenos.

Caballo de Troya: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (formatear el disco duro, modificar un fichero, sacar un mensaje, etc.). En una de las formas de los virus.

Carding: Uso ilegitimo de las tarjetas de crédito, o sus números, pertenecientes a otras personas. Se relaciona mucho con el hacking, porque para conseguir números de tarjetas de créditos, una de las mejores maneras es el hacking.

Contraseña: Clave secreta de un usuario que da el acceso a programas y hardware.

Cortafuego: (FIREWALL, BASTION) - Sistema avanzado de seguridad que impide a personas no acreditadas el acceso al sistema.

Crackeador: Programa utilizado para sacar los password encriptados de los archivos de passwords. Bien desencriptándolos, cuando se puede, o bien probando múltiples combinaciones hasta que encuentra la correcta.

Cracker: Persona que elimina las protecciones lógicas y a veces físicas del software. Hacker malvado. Hacker que emplea la fuerza bruta, o métodos que dañan el sistema que intenta hackear.

Cracking: Se llama a la acción de violar o romper la seguridad de un sistema operativo o programa.

Caber Punk: Es un tipo de ideología o de sub-cultura. Se basa en el culto a la tecnología, a la ciencia, y el odio a cualquier forma de poder organizado. Igual que en el caso de la anarkia, se usa en muchas ocasiones con criterios equivocados, produciendo una mala imagen de este grupo. También tiene una importante relación con el mundo hacker.

Fichero de Password: Fichero en el que el sistema guarda sus claves de acceso.

FingerPrinting: Técnica utilizada por Hackers y Crackers para obtener mayor cantidad de información sobre un determinado sistema operativo y servicios en ejecución de una computadora personal o servidor.

Firewall: Programa que permite el filtrado de paquetes y servicios a una red.

GUI: (Graphic User Interface) Interfaz de Usuario Gráfica.

Hacker por Fuerza Bruta: No significa nada bestia, ni que necesite mucha fuerza, implemente es un hacking que necesita mucho esfuerzo, mucho tiempo de proceso o de intentos. Como es probar distintos passwords hasta encontrar el acertado, usar un crackeador, desencriptar un fichero encriptádo, sacar las claves de un archivo de passwords usando las palabras de un diccionario, etc.

Hacker: Persona que hace hacking. Persona muy hábil con los ordenadores. Pirata informático, en cualquiera de sus muchos significados.

Hacking: Penetrar en sistemas informáticos ajenos sin su consentimiento, tanto "virtualmente" como físicamente. (Ej. Entrar en una oficina y robar unos manuales). Cualquier acción encaminada a conseguir lo primero; como son la ingeniería social, el trashing, etc.

Hexadecimal: Número en un sistema con base en 16.

Ingeniería Social: Convencer a un internauta, por diversos medios, para que facilite información útil para hackear, o para que haga algo que nos beneficie (no solo al hackear).

Intervención de Líneas de Datos (SPOOFING); Similar al Intervención de líneas telefónicas, en este caso el objetivo son los sistemas de transmisión de datos (Cable telefónico usado por módem, cableado de una red local,

fibra óptica, TV por cable) con el fin de monitorizar la información que pasa por ese punto y obtener información del sistema.

Internet: Red privada conectada a Internet, pero generalmente aislada de esta por un cortafuegos. Red privada que usa los mismo protocolos de comunicación que Internet (TCP/IP) y que puede estar aislada o conectada a Internet.

Intranet: Red interna o también llamada corporativa, separada de Internet pero con similares servicios a los mismos usuarios.

IP: (Internet Protocol) Protocolo de Internet

IPCE: (Intern Process Comunication Environment) Procesos Internos del Ambiente de Comunicación.

ISN: (Initial Sequence Number) Número de Secuencia Inicial. Son aquellos números que se generan en la secuencia inicial cuando el servidor responde a las solicitudes de conexión.

Log: Archivo que recoge un registro de tus actividades en el sistema, almacena información sobre tu acceso al sistema.

Login: Procedimiento de entrar en un sistema.

Patch (Parche): Modificación de un programa anterior, con la intención de solucionar un bug, o para crackearlo.

PBX o **PABX** - Centrales telefónicas privadas, generalmente de empresas.

Phreaking: Uso del teléfono, o de las redes y servicios telefónicos, gratis o con un coste menor del normal. Debido al uso intensivo del teléfono por parte de los hackers, es bastante normal que usen el phreackin para ahorrar. Modificación o intervención de las líneas telefónicas, con otros fines distintos del llamar gratis.

Pirata Informático: Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc. Persona que elimina las protecciones software. Más conocido como cracker. Delincuente informático.

Proxy: Un servidor Proxy es el que comunica la estación del usuario con el Internet y esta asociado al Gateway y en algunos casos al Firewall.

Puertas Falsas: Es una practica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas. Aquellos que programaban en C sabrán de lo que hablo.

RFC: (Request For Comment) Petición de Respuesta.

Router: Encaminador, dispositivo que conecta dos redes de área local o entre el Internet e Intranet.

Script: Seria el equivalente en UNIX, de los bat's del MS-DOS, aunque mucho mas potentes y con mas opciones, siendo casi un pequeño lenguaje de programación.

SMTP: (Simple Mail Transfer Protocol) Protocolo de Transferencia de Correo Simple.

Simulación de Identidad: Básicamente en usar un terminal de un sistema en nombre de otro usuario bien por que se conoce su clave, por que abandono el terminal pero no lo desconecto y ocupamos su lugar. El término también es aplicable al uso de Tarjetas de Crédito o documentos falsos a nombre de otra persona.

Simulación de Ordenador: Se define como el uso de la computadora para simular previamente una situación y de esta forma determinar las acciones a probar. En el contexto del hacking se refiere a la simulación en la computadora propia del sistema a atacar con el fin de elaborar estrategias de acción.

Sniffer: Programa encargado de interceptar la información que circula por la red.

Tracear: Seguir la pista a través de la red a una información o a una persona.

Trashing (Recogida de basura): Rebuscar en la basura, para encontrar algo que pueda ser útil a la hora de hackear. Conexiones y es Protocolo abierto en el que el usuario (programador) define su propio tipo de paquete.

Troyano: Programa que aparenta dar un servicio confiable, pero que en realidad atenta contra la seguridad de la información de quien lo utiliza.

UPS: (Unit Power Suply) Unidad de Fuente de Poder.

Virus: Programa que tiene el comportamiento de los virus biológicos, se reproducen de igual forma y atacan hasta el punto de dejar inutilizable a la computadora.

WAN: (Wide Area Network) Red de Área Amplia.

X25: Es un tipo de línea de comunicaciones, como lo es la línea telefónica normal (RTC) o la RDSI. Generalmente se usa para transmisiones de datos. Redes de este estilo son IBERPAC, TYMNET, etc.